Zero Trust Hospital

An Architect's Approach to Achieving Zero Trust in a Clinical Setting

zscaler™
Healthcare Solutions

AUTHORS

Steven Z Hajny
Ryan Ulrick
Dave Steinke
Derek Brodeur

Zero Trust Hospital

An Architect's Approach to Achieving Zero Trust in a Clinical Setting

AUTHORS
Steven Z Hajny
Ryan Ulrick
Dave Steinke
Derek Brodeur

Healthcare Solutions

Published February, 2025
First Edition
ISBN Number: 979-8-9924738-3-4

Table of Contents

CHAPTER 1

Introduction to the Zero Trust Hospital

The Zero Trust Hospital is designed to create a framework that a healthcare provider can follow to achieve better cyberthreat protection, data protection, user experience and patient care. While this may not encompass all use cases or fine details of implementing this strategy, it should serve as a great starting point for a cybersecurity team who is unfamiliar with where to begin when it comes to implementing a zero trust model. Readers will be led through the landscape of threats observed in the healthcare industry, the catalyst for change, and the phased approach that Zscaler sees customers take to reduce complexity and become more risk averse.

Introduction to Digital Transformation in Healthcare

The healthcare industry is poised at the precipice of a significant digital transformation, reshaping patient care, operational efficiencies, and the overall healthcare experience. This transformation is powered by the integration of technologies such as AI with electronic health records (EHRs), telemedicine, mobile health applications, and wearable technology. These innovations offer unprecedented opportunities for enhancing patient outcomes, improving data accessibility, and streamlining healthcare delivery. For instance, the adoption of EHR systems has become widespread, with a reported increase from 22% in 2009 to 78% in 2021 among office-based physicians in the United States, according to the Office of the National Coordinator for Health Information Technology. Telemedicine has also seen explosive growth, especially catalyzed by the COVID-19 pandemic, with the CDC reporting an 85.9% increase in telehealth visits from 2019 to 2021.

The Contradiction: Digital Innovation vs. Cyber Vulnerability

While digital transformation in healthcare promises numerous benefits, it also introduces significant cybersecurity risks. The reliance on digital technologies and the vast amounts of sensitive data being generated, processed, transmitted, and stored online have made healthcare organizations prime targets for cybercriminals. Cyberthreats in healthcare are diverse and sophisticated, ranging from ransomware attacks that can lock access to vital patient data and disrupt hospital operations, to sophisticated phishing schemes designed to steal sensitive information. The 2024 Cybersecurity Incident and Breach Trends Report from the Health Information Sharing and

Analysis Center (H-ISAC) highlighted a surge in social engineering attacks, ransomware, and supply chain attacks, indicating the evolving nature of threats facing the healthcare sector. A total of 459 ransomware events occurred globally in the healthcare sector during 2023 with 379 of those events occurring in America's healthcare sector. A striking example of these vulnerabilities was the WannaCry ransomware attack in 2017, which affected over 200,000 computers across 150 countries, including the UK's National Health Service (NHS). The attack caused widespread disruption to healthcare services, highlighting the potential consequences of cybersecurity failures in a healthcare context.

The High Valuation of Healthcare Data by Cybercriminals

Healthcare data is a goldmine for cybercriminals due to its comprehensive, sensitive, and immutable nature. Unlike other types of personal information that can be changed (such as credit card numbers), health information is inherently permanent. This permanence adds to its value on the dark web, where it can be sold for a premium. According to a report by Trustwave, healthcare records can fetch up to $250 each on the dark market, significantly more than credit card information. Cybercriminals exploit healthcare data for various nefarious purposes, including identity theft, insurance fraud, and even targeted phishing attacks. The detailed personal and health information contained in medical records allows criminals to craft highly convincing scams, making this data particularly lucrative.

Healthcare records are **47x** more valuable on the Dark Web than payment card records.

PAYMENT CARD

$5.40
per record

HEALTHCARE

$250.00
per record

Types of Data at Risk

Personal Health Information (PHI)

PHI encompasses a wide range of data, from basic personal identifiers like names and addresses to more sensitive information such as medical histories, test results, and prescription information. The Health Insurance Portability and Accountability Act (HIPAA) in the United States sets strict regulations for the handling of PHI, underscoring its sensitivity and importance.

Payment Information

Healthcare providers process vast amounts of payment information, including credit card numbers, insurance details, and billing addresses. This information is highly sought after by cybercriminals for financial fraud and identity theft.

Research Data

Healthcare research data, including clinical trial information and proprietary pharmaceutical research, represents a significant intellectual and economic asset. Breaches involving this type of data can lead to substantial financial losses and competitive disadvantage.

The Broader Impact of Data Breaches

The consequences of healthcare data breaches extend far beyond the immediate financial costs associated with containment, remediation, and regulatory fines. The IBM Security Cost of a Data Breach Report 2023 highlighted the healthcare sector as having the highest average cost of a data breach, reaching $10.93 million. However, the impacts are multifaceted:

Erosion of Patient Trust and Increased Patient Mortality

Trust is foundational to the patient–provider relationship. A data breach can severely damage this trust, leading to patients being reluctant to share necessary information for their care or even switching providers.

A study done in 2023 by Proofpoint showed that IT professionals stated that due to cyberattacks, fatalities increased by 28% for ransomware, 12% for BECs, 21% for supply chain attacks and 29% for cloud compromises.

Operational Continuity

Cyberattacks, particularly ransomware, can cripple hospital IT systems, disrupting patient care services. The WannaCry attack's impact on the NHS, where thousands of appointments and surgeries were canceled, exemplifies the potential for disruption.

Long-Term Reputational Damage

The reputation of a healthcare provider is critical to its success and ability to attract and retain patients. Data breaches can tarnish a provider's reputation, leading to a long-term decrease in patient numbers and revenue.

Regulatory and Legal Repercussions

Healthcare providers are subject to stringent regulatory requirements for data protection, such as HIPAA in the United States and the General Data Protection Regulation (GDPR) in the European Union. Breaches can result in hefty fines and legal actions, further compounding financial losses.

Impact on Research and Development

For healthcare research institutions, a breach can result in the loss of intellectual property, setting back medical advances and eroding competitive edges.

The Escalation of Cyberattacks on Healthcare

Recent years have witnessed a noticeable uptick in cyberattacks targeting healthcare institutions worldwide. According to the 2021 Cybersecurity Breach Report by the Department of Health and Human Services' Office for Civil Rights, there was a significant rise in reported healthcare breaches, with over 600 major breaches affecting 500 or more individuals in a single year, marking a 55% increase from the previous year. Ransomware attacks, in particular, have become a grave concern. The American Hospital Association (AHA) has reported a dramatic escalation in ransomware incidents, with attacks more than doubling in frequency from 2019 to 2020. This surge reflects not only the increasing sophistication of cybercriminals but also the high value of healthcare data and the critical nature of healthcare services, which can pressure organizations into paying ransoms to regain access to their systems and data.

The Sophistication of Cyberthreats

Advanced Methods: Supply Chain Attacks and State-Sponsored Hacking

The cybersecurity landscape has seen a marked shift towards more sophisticated and insidious methods of attack. Supply chain attacks, where attackers target less secure elements in the supply chain to compromise their primary target, have become increasingly prevalent. A notable example is the SolarWinds Orion breach in December 2020, which, while not healthcare-specific, underscores the potential for such attacks to infiltrate healthcare organizations through third-party vendors and software. State-sponsored hacking represents another significant threat, with various nations deploying cyber espionage tactics to steal intellectual property, including COVID-19 research data. For instance, in July 2020, the United States, United Kingdom, and Canada issued a joint advisory accusing Russian state-sponsored actors of targeting healthcare organizations involved in coronavirus vaccine development.

Social Engineering: The Human Element

Cybercriminals continue to target the human element as the easiest way to infiltrate organizations, making employees the most vulnerable layer in security. According to KnowBe4's 2023 Phishing by Industry Benchmark Report, which analyzed over 12.5 million users across 35,600 organizations, phishing susceptibility remains a significant risk. The report spans 19 industries and 7 regions, with findings based on over 32.1 million simulated phishing tests.

Key statistics show that prior to any training, 33.2% of employees are likely to fall for a phishing email. However, after completing KnowBe4 training, this rate drops significantly. Within 90 days, only 18.5% of users fail phishing tests, and after a year of ongoing training, just 5.4% of employees remain vulnerable. On average, organizations improved their resilience to phishing attacks by 82% after a year on the platform.

The report highlights the importance of building a strong security culture that goes beyond training. Employees must consistently understand and embrace their role in defending against cyberattacks, both professionally and personally. Only a continuous, well-structured security awareness program, coupled with frequent simulated phishing tests, can foster the necessary behavior changes to reduce risk.

The COVID-19 Pandemic: A Catalyst for Digital Healthcare

The pandemic has undoubtedly accelerated the adoption of digital healthcare services, from telehealth consultations to remote patient monitoring, enhancing access to care during lockdowns and social distancing measures. However, this rapid digitalization has also expanded the attack surface for cybercriminals. The FBI reported a 300% increase in reported cybercrimes since the beginning of the pandemic, with healthcare organizations increasingly targeted due to the critical nature of their services and the sensitivity of the data they handle.

Emerging Technologies: IoT and Telehealth Security Challenges

The integration of IoT devices in healthcare, such as wearable health monitors and connected medical devices, introduces new vulnerabilities. These devices often lack robust security features, making them easy targets for cyberattacks.

In 2018, the Department of Homeland Security issued an alert about a set of vulnerabilities, known as URGENT/11, which could potentially compromise millions of IoT devices, including medical devices.

Telehealth platforms, while essential for maintaining care continuity during the pandemic, have also presented significant security challenges. The rush to implement these solutions often led to the use of platforms that were not fully compliant with healthcare regulations or did not have adequate security measures in place. The Health and Human Services' Office for Civil Rights reported a significant increase in breaches related to unauthorized access/disclosure incidents, many of which can be attributed to the rapid adoption of telehealth services.

Universal Health Services (UHS) Ransomware Attack (2020)

Examination of the Attack Timeline and Response

In September 2020, Universal Health Services, one of the largest healthcare providers in the U.S., experienced a massive ransomware attack that disabled systems across approximately 400 facilities. The attack, attributed to the Ryuk ransomware, led to widespread disruption of healthcare services, including patient record access, medication orders, and emergency services.

UHS' response included taking all systems offline to contain the spread, working with cybersecurity experts to investigate the breach, and gradually restoring systems from backups. The organization was lauded for its transparency and communication efforts throughout the incident.

Lessons Learned for the Healthcare Industry

The UHS incident underscored the critical need for robust incident response plans and the value of maintaining up-to-date backups. It also highlighted the importance of staff training, as employees had to revert to manual processes during the system downtime. For the healthcare industry, the UHS attack reinforced the necessity of a multi-layered cybersecurity strategy that includes endpoint protection, employee education, and regular system backups.

Scripps Health Ransomware Attack (2021)

Case Study: Execution and Impacts

In May 2021, Scripps Health, a major healthcare system in San Diego, fell victim to a ransomware attack that led to a significant disruption of its IT systems. The attack resulted in the cancellation of appointments, diversion of emergency patients, and a return to paper records. Scripps Health's communication systems, including email and patient portals, were also affected, complicating communication with patients and between staff.

The immediate financial impact of the Scripps Health attack was profound, with the organization reporting an estimated loss of $112.7 million due to the incident. This included both direct costs related to the cybersecurity response and indirect costs from lost revenue.

Cybersecurity Measures Adopted Post-Attack

In response to the attack, Scripps Health accelerated its cybersecurity initiatives, investing in advanced monitoring tools, enhancing endpoint security, and expanding its cybersecurity training for staff. The organization also focused on improving its incident response framework to ensure quicker detection and containment of future threats.

Change Healthcare Ransomware Attack (2024)

THE MECHANISM AND VULNERABILITIES EXPLOITED

The Change Healthcare ransomware attack occurred on February 21, 2024, when the ALPHV/BlackCat ransomware group breached the company's systems, exploiting the lack of multifactor authentication (MFA) on one of Change Healthcare's critical remote access servers. This oversight allowed hackers to infiltrate the network, where they accessed and exfiltrated up to 6 terabytes of sensitive data, including personal information, medical records, insurance data, and payment details. Despite being a subsidiary of UnitedHealth Group with HITRUST certification, Change Healthcare's outdated legacy systems made them vulnerable to this attack.

AFTERMATH AND IMPACT ON HEALTHCARE PROVIDERS

The breach caused widespread disruptions across the U.S. healthcare system, impacting hospitals, medical offices, and pharmacies. The attack led to delays in insurance claims processing, reimbursement issues, and disrupted patient care, with approximately 94% of hospitals experiencing financial repercussions. Change Healthcare temporarily took systems offline, leading to a backlog of unpaid claims that threatened cash flow for smaller healthcare providers. It's estimated that about one-third of Americans had their sensitive health information exposed, including Social Security numbers, medical records, and other personal data.

THE RESPONSE AND CONSEQUENCES

UnitedHealth Group paid a ransom of $22 million in Bitcoin to the attackers. Despite this, the company couldn't guarantee that further data wouldn't be leaked. The breach prompted multiple investigations, with the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) initiating an investigation into Change Healthcare's HIPAA compliance. Legislators and federal agencies are pushing for stricter regulations on healthcare data protection, emphasizing the need for robust security measures like MFA and stronger cybersecurity frameworks.

LESSONS AND RECOMMENDATIONS

The Change Healthcare incident serves as a wake-up call for the healthcare industry to strengthen security measures. Recommendations include implementing comprehensive cybersecurity protocols such as regular patch management, strong access controls, multifactor authentication, end-to-end encryption, and proactive risk management strategies. The attack demonstrated that even large, well-established healthcare organizations are vulnerable to cyberthreats, underscoring the need for ongoing vigilance and compliance with HIPAA and HITRUST standards.

Balancing Security with Access

Perhaps the most critical challenge in healthcare cybersecurity is striking the right balance between securing sensitive data and ensuring healthcare providers have quick, unhindered access to patient information. Delays in accessing critical patient data can have life-or-death consequences in emergency situations. Achieving this balance requires a nuanced approach to cybersecurity, with strategies that include role-based access controls, the use of secure but user-friendly authentication methods, and the deployment of advanced encryption technologies. Moreover, embracing a zero trust architecture, where trust is never assumed and verification is required from everyone attempting to access resources in the network, can provide a robust framework for securing sensitive data while facilitating necessary access. As healthcare organizations navigate the complexities of the digital age, the adoption of a zero trust security model represents a fundamental shift in the approach to protecting sensitive patient data and critical IT infrastructure.

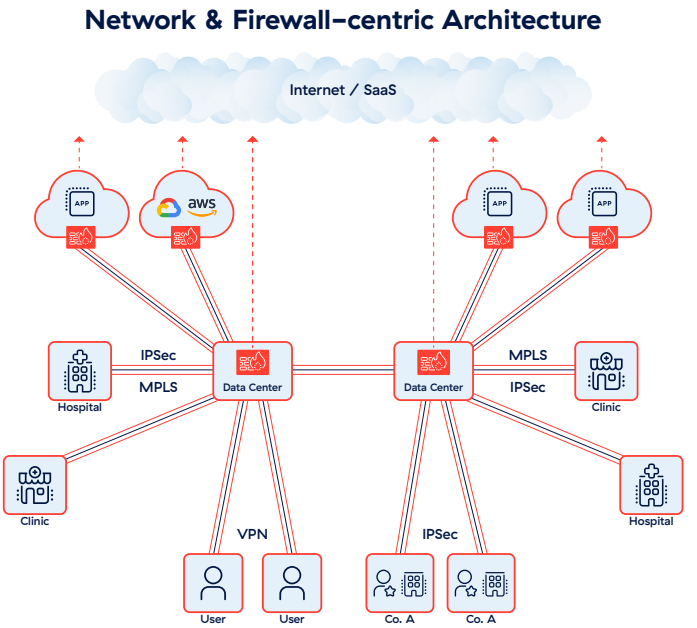
Foundational Overview of the Zero Trust Model

The zero trust model is a strategic approach to cybersecurity that operates on the principle of "never trust, always verify." Unlike conventional security models that implicitly trust users and devices within an organization's network, zero trust assumes that threats can originate from anywhere, both outside and inside the network. Therefore, every attempt to access the network's resources is treated as a potential threat that must be authenticated, authorized, and continuously validated for security compliance before access is granted.

CORE PRINCIPLES OF ZERO TRUST

- **Least-privileged access:** Ensuring users have only the access necessary to perform their job functions, reducing the attack surface.
- **Microsegmentation:** Dividing the network into secure zones to contain breaches and limit lateral movement by attackers.
- **Multifactor authentication (MFA):** Requiring more than one piece of evidence to authenticate a user, significantly enhancing security.
- **Continuous monitoring and validation:** Regularly verifying the security posture of devices and users to ensure they meet the organization's security standards.

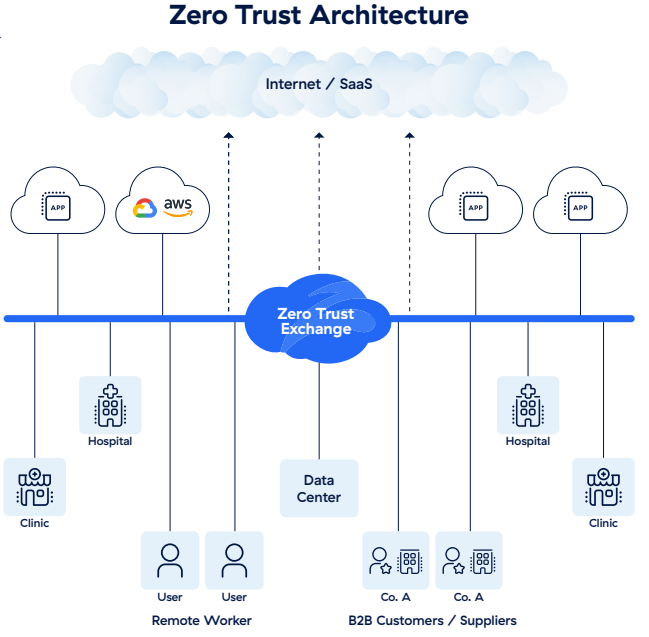
Traditional Perimeter–Based Security vs. Zero Trust



A trusted network connects users, sites and apps
Secure the network for threat and data protection

Rigid, Complex and a Security Risk
Barrier to Transformation

TWO OPPOSING



Business policies determine who can access
what over any network, the network is transport

Agile, Simple and Secure
Enables Transformation

Traditional perimeter-based security models, often likened to a "castle-and-moat" approach, focus on fortifying the network's outer defenses to keep attackers out. Once inside the network, users and devices are generally trusted by default. This model has become increasingly ineffective as organizations adopt cloud services, mobile computing, and remote work, which blur the boundaries of the traditional network perimeter. In contrast, the zero trust model recognizes that threats can originate from any location—external or internal—and that trust should not be assumed based on the network's location. This approach offers a more dynamic and flexible framework for securing modern digital environments, where the traditional network perimeter no longer exists.

The Relevance of Zero Trust in Healthcare

The healthcare industry faces specific cybersecurity challenges that make the zero trust model particularly relevant:

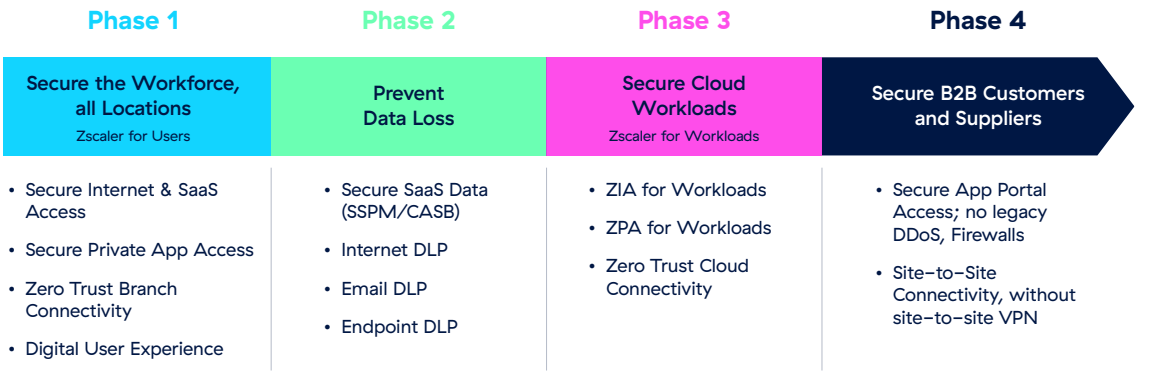
- **Highly sensitive data:** Healthcare organizations manage vast amounts of sensitive patient data, making them prime targets for cyberattacks. Zero trust's principle of least privilege minimizes the risk of data breaches by ensuring that only authorized users can access specific data.

- **Regulatory compliance:** Healthcare providers must comply with stringent data protection regulations, such as HIPAA and GDPR. The continuous monitoring and validation aspects of zero trust can help organizations meet these regulatory requirements by ensuring that data access is securely controlled and audited.

- **Complex ecosystems:** Healthcare IT environments are complex, with a mix of legacy systems, IoT devices, and cloud services. The microsegmentation of zero trust allows for the creation of secure zones, making it easier to secure this diverse ecosystem.

- **Insider threats:** Given the high value of healthcare data, insider threats are a significant concern. Zero trust's "never trust, always verify" approach mitigates this risk by treating all users as potential threats until their identity and permissions are verified.

Implementing a zero trust architecture in healthcare requires a strategic, phased approach, starting with securing your workforce, identifying and securing your sensitive data, securing your workloads, securing your B2B, and gradually applying zero trust principles across the network.



While the transition to zero trust can be challenging, especially in complex healthcare environments, the benefits of enhanced security, compliance, and patient trust make it a compelling strategy for healthcare CISOs and cybersecurity professionals.

"What used to take weeks to accomplish with on-premises ... can now be achieved in a matter of hours using Zscaler. We can secure our data in the cloud at a speed that would not have been possible using traditional legacy systems."

MANI MASOOD | Head of Information Security, AMN Healthcare

CHAPTER 2

Protect Your Workforce

We start with securing the workforce as the first phase in the journey to achieving the Zero Trust Hospital. Your workforce is the foundation to achieving your health systems goals, however a large number of threats come from phishing a user and using their system to laterally move through the environment and ultimately doing data exfiltration.

The Role of Identity and Context in Zero Trust

In a zero trust environment, identity is not just about a username or an email address; it's a comprehensive profile that includes roles, attributes, and behavior patterns of a user. Context brings in additional parameters like device health, location, time of access, and the sensitivity of the accessed data. This amalgamation of identity and context ensures that access to resources is granted not just because someone knows the right password but because they are the right person, in the right location, trying to access the right resource for the right reasons.

Identity providers (IdPs) are central to managing this identity information. They serve as a repository and management system for user identities, facilitating the authentication and authorization processes. IdPs like Okta, Microsoft Azure AD, and Google Identity provide the foundation for zero trust by ensuring that identities are securely managed and accessible across various applications and services. A system that automates auditing of identity is equally as important to tie into your IdP that way if an account is given too many permissions or has had access changes that could compromise a system it is known and premeditated by the automation.

The Importance of Security Assertion Markup Language (SAML) in Zero Trust

SAML plays a crucial role by enabling secure, single sign-on (SSO) access to cloud applications without requiring users to manage multiple passwords. SAML allows security assertions, including authentication and authorization decisions, to be exchanged between an IdP and a service provider (SP). In a zero trust architecture, SAML ensures that every application access request is authenticated and authorized, aligning with the principle of least-privileged access.

Multifactor Authentication (MFA)

MFA is non-negotiable in a Zero Trust Hospital. It adds an extra layer of security by requiring users to provide two or more verification factors to gain access to resources, thereby reducing the likelihood of unauthorized access. MFA can include something you know (a password), something you have (a smartphone or token), and something you are (biometrics). In the context of identity and zero trust, MFA ensures that even if one factor is compromised, unauthorized users still cannot access sensitive resources.

System for Cross-Domain Identity Management (SCIM) vs. SAML Auto Provisioning: Enhancing Security with Identity Management

While SAML is pivotal for authentication and SSO, SCIM focuses on the automated management of user identities. SCIM is a standard for automating the exchange of user identity information between identity domains or IT systems. It simplifies the task of user management in multi-application environments, such as provisioning, deprovisioning, and group memberships.

The security benefits of using SCIM over SAML for auto-provisioning are significant:

- **Automated user life cycle management:** SCIM automates the provisioning and deprovisioning process, ensuring that users' access rights are accurately reflected across all systems in real-time. This reduces the risk of former employees retaining access to corporate resources—a common security loophole.

- **Consistent identity information:** By standardizing how identity information is exchanged, SCIM ensures that identity attributes remain consistent across different systems. This consistency is critical in enforcing access policies based on user attributes.

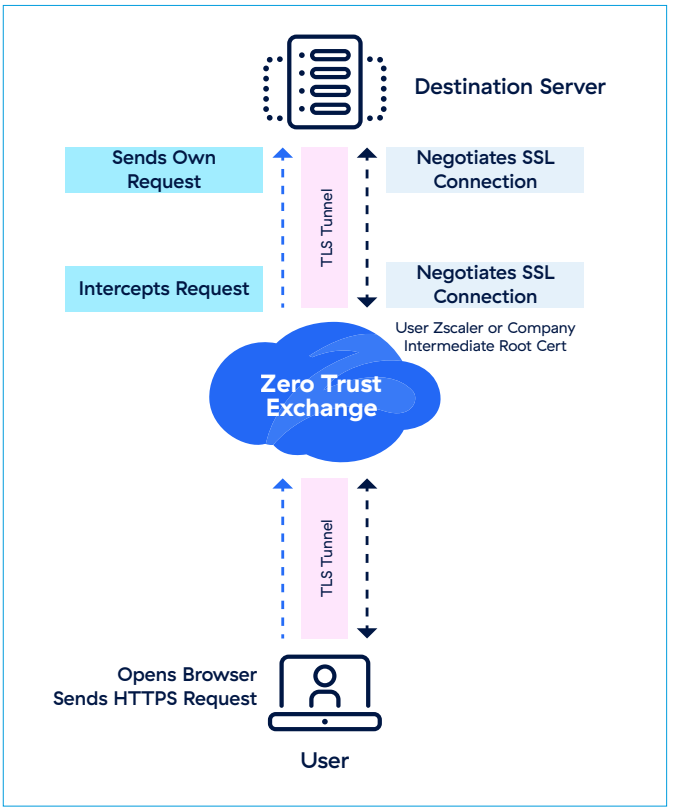
- **Efficiency and reduced error:** Manual provisioning is prone to errors, which can lead to security vulnerabilities. SCIM reduces these errors by automating the identity management process, thereby enhancing security posture.

You should not use SCIM and auto-provisioning together for the same domain as it can cause issues. SCIM is preferred per best practices. Identity however, is the first step to achieving identity and context; the next important part is how that context turns into policy. This is where utilizing an agent-based approach comes into play.

Proxy Architecture Overview

A proxy architecture in the context of cybersecurity serves as an intermediary between users and the services or resources they wish to access. This setup is particularly relevant in environments adopting a zero trust security model where the traditional assumption that users within a network perimeter can be trusted is replaced with a "never trust, always verify" approach. In such a model, the proxy architecture plays a crucial role in ensuring that all access requests are authenticated, authorized, and encrypted, regardless of their origin before getting to the destination.

How Proxy Architecture Works



Proxy architectures can be implemented in various forms, including forward proxies, reverse proxies, and transparent proxies, each serving different purposes. A forward proxy acts on behalf of clients, requesting resources from the internet or other networks. In contrast, a reverse proxy receives requests from the internet and forwards them to internal servers, acting as a shield for those servers. Transparent proxies, on the other hand, intercept all network traffic between users and the internet without requiring any configuration on the user's part.

In a zero trust environment, proxies are often deployed as security gateways that enforce access controls and security policies. When a user attempts to access a resource, the request is routed through the proxy, which then performs several security checks, including authentication of the user's identity, validation of their access rights, and inspection of the request for malicious content. Only after passing these checks is the request allowed to proceed to the intended resource, and even then, the communication is often monitored and logged for ongoing security analysis.

Benefits of Cloud-Based Proxy Architecture in a Zero Trust Environment

Enhanced security: By intercepting all access requests, a cloud proxy architecture ensures that no direct connections are established between users and resources until those requests are verified. This setup significantly reduces the attack surface, as malicious actors cannot directly target backend systems or exploit unsecured direct connections.

Centralized access control: Cloud Proxy architectures enable centralized management of security policies and access controls. This centralization simplifies the enforcement of complex security policies.

Improved user experience: While enhancing security, proxy architectures can also streamline the user experience by providing a single access point for multiple services and resources. This can reduce the need for multiple logins and direct interactions with different security systems, making access more seamless for legitimate users.

Visibility and logging: Proxy architectures offer comprehensive visibility into all traffic entering or leaving the network. This visibility is crucial for detecting potential threats, monitoring for anomalous behavior, and conducting forensic analysis in the event of a security incident.

Scalability and flexibility: Cloud-based Proxies easily scale to accommodate growing traffic demands or to extend protection to new resources and services. They also support a range of security technologies such as SSL/TLS decryption, deep packet inspection, and advanced threat protection, allowing organizations to adapt their security posture as threats evolve. This allows for legacy security stack consolidation.

In conclusion, the proxy architecture is a vital component of a zero trust environment, offering enhanced security, centralized control, and improved visibility. By verifying and controlling access at the perimeter, proxies help to minimize risks and protect against modern cyberthreats, making them an indispensable tool in the arsenal of zero trust security strategies.

Traffic Forwarding Mechanisms in a Zero Trust Architecture

In a healthcare environment, securing both user traffic and workloads (i.e., application or server traffic) is critical to maintaining a robust zero trust architecture. Forwarding mechanisms play a crucial role in ensuring that traffic from all endpoints, whether user devices or workloads, is routed through secure inspection points for policy enforcement. These mechanisms can be implemented in various ways, such as using GRE/IPsec tunnels, agent-based solutions, agentless connectors, or cloud-based forwarding methods.

Let's explore these forwarding methods, along with their pros and cons, to understand how they can be applied effectively in a healthcare environment.

1. GRE Tunnels

Overview: GRE (Generic routing encapsulation) tunnels allow network traffic from an entire site or branch to be forwarded to a central inspection point or security proxy. This method is widely used for forwarding traffic from on-premises networks, including workloads hosted in data centers.

PROS:

- **Scalability:** Suitable for large-scale environments, as a single tunnel can handle traffic from multiple users and workloads.
- **Simplicity:** Easy to implement in environments with existing networking infrastructure.
- **Centralized security:** Ensures all traffic from a network site is subject to consistent security policies and inspection.

CONS:

- **No granularity:** Lacks application-level control, meaning all traffic is treated equally regardless of the source or application.
- **Increased bandwidth usage:** Can lead to higher bandwidth consumption since all traffic, even local traffic, is routed through the tunnel.
- **Requires network changes:** May require adjustments to existing network configurations, which can be complex in some healthcare settings.

2. IPsec Tunnels

Overview: IPsec (Internet Protocol Security) tunnels provide encrypted connections between on-premises networks or cloud workloads and the central zero trust inspection point. This method ensures data confidentiality and integrity, making it ideal for protecting sensitive healthcare data.

PROS:

- **High security:** Offers strong encryption, protecting data in transit, which is crucial for compliance with healthcare regulations.
- **Flexible deployment:** Can be used for connecting remote sites, cloud workloads, or third-party partners securely.
- **Reliability:** Provides robust connectivity and secure communication between endpoints.

CONS:

- **Complex configuration:** Requires more configuration and management than GRE tunnels, which can be a challenge for healthcare organizations with limited networking expertise.
- **Performance impact:** The encryption process can introduce latency, which might affect the performance of time-sensitive healthcare applications.
- **Scalability:** May not be as easily scalable as other methods when dealing with a large number of remote sites or workloads.

3. Agent-Based Forwarding

Overview: Agent-based forwarding involves installing software agents on endpoints, such as user devices or virtual machines, which route traffic through a central inspection point. This method supports detailed traffic management and policy enforcement, even for remote or roaming devices.

PROS:

- **Granular control:** Offers detailed control over traffic, enabling policy enforcement based on user identity, application, and device posture.
- **Consistent security:** Ensures that security policies are enforced regardless of the device's location, whether inside or outside the healthcare network.
- **Real-time posture assessment:** Allows for continuous monitoring of device compliance, ensuring that only secure devices access sensitive workloads.

CONS:

- **Deployment and maintenance:** Requires installation and ongoing maintenance on each endpoint, which can be challenging in large, diverse environments.
- **Compatibility issues:** Not all devices or workloads support agent installation, limiting applicability in some scenarios.

4. Agentless Connectors

Overview: Agentless connectors forward traffic from endpoints that cannot support an agent, such as IoT devices, legacy systems, or certain workloads. These connectors are deployed within the network to capture and forward traffic to the central inspection point.

PROS:

- **No endpoint installation:** Ideal for devices that cannot run agents, such as medical IoT devices or legacy systems.
- **Centralized management:** Provides a way to enforce security policies without modifying endpoint configurations.
- **Quick deployment:** Faster to implement since no software installation is required on individual devices.

CONS:

- **Limited visibility:** May not provide the same level of granular visibility or control as agent-based solutions.
- **Network complexity:** Requires network changes to route traffic through the connector, which can be complex in large healthcare environments.
- **Potential bottlenecks:** As all traffic is funneled through the connector, it could become a single point of failure or cause latency issues.

5. Cloud-Based Forwarding (Service Mesh for Workloads)

Overview: Cloud-based forwarding uses a service mesh or virtual network overlay to route traffic between cloud workloads through a central policy enforcement point. This is particularly relevant for workloads hosted in cloud environments, ensuring that traffic between cloud services adheres to zero trust principles.

PROS:

- **Scalability:** Easily scales with cloud workloads, making it ideal for dynamic healthcare applications and services.
- **Application-level control:** Provides granular control over traffic between workloads, allowing for fine-tuned policy enforcement.
- **Minimal on-premises changes:** Reduces the need for network adjustments in cloud environments, making it easier to deploy in hybrid setups.

CONS:

- **Complex configuration:** Can be complicated to set up, especially in multicloud or hybrid environments where workloads span different platforms.
- **Potential latency:** Traffic inspection can introduce latency, affecting the performance of cloud-based healthcare applications.
- **Cost:** May incur additional costs, especially with high traffic volumes or complex configurations.

6. PAC File Utilization

Overview: PAC (Proxy auto-configuration) files are scripting files used to define how traffic should be routed from endpoints to a proxy or central inspection point based on specific criteria such as destination URLs, IP ranges, or application types. In a zero trust architecture, PAC files enable flexible, granular control over traffic forwarding, making them a valuable tool for selectively enforcing policies in both user and workload environments.

PROS:

- **Granular control:** Allows precise traffic routing decisions based on a wide range of criteria, enabling fine-tuned policy enforcement for different applications and destinations.
- **Performance optimization:** By bypassing certain trusted or latency-sensitive traffic, PAC files help reduce unnecessary inspection, improving performance for critical healthcare applications.
- **Flexibility:** Can adapt to changing network environments and security requirements quickly, allowing organizations to update routing policies without requiring software or network changes.
- **Compatibility:** Works alongside various forwarding mechanisms (e.g., agent-based, agentless, GRE/IPsec tunnels), making PAC files versatile in different healthcare infrastructure setups.

CONS:

- **Configuration complexity:** As PAC files grow in size and logic, they can become complex to manage, requiring careful configuration to avoid errors.
- **Maintenance requirement:** Regular updates and maintenance are needed to ensure PAC files stay current with network changes and evolving security policies.
- **Potential security gaps:** Misconfigured PAC files can introduce security vulnerabilities or allow unauthorized traffic bypasses, posing a risk if not managed correctly.
- **Limited visibility:** PAC files may not provide detailed visibility into bypassed traffic, potentially reducing the ability to monitor or audit certain activities comprehensively.

Combining PAC Files with Other Forwarding Mechanisms

PAC files are often used in conjunction with other forwarding mechanisms to enhance the efficiency and flexibility of a zero trust architecture.

- **Agent-based solutions:** PAC files can be used by agents to determine which traffic should be forwarded through the zero trust inspection point and which can be bypassed, optimizing device performance.
- **GRE/IPsec tunnels:** PAC files provide an additional layer of control, allowing selective bypass of certain traffic even within tunnel-based environments, ensuring only relevant traffic is inspected.
- **Agentless connectors:** PAC files ensure that traffic from non-agent-supported devices is still efficiently routed or bypassed as needed, maintaining consistent policy enforcement.

Common PAC File Bypass Examples in Healthcare

1. **Local network resources:** PAC files can be configured to bypass traffic for local resources such as printers, file servers, or other internal healthcare systems to avoid unnecessary routing through the central inspection point.

javascript

```
if (isInNet(host, “192.168.1.0”, “255.255.255.0”)) return “DIRECT”;
```

2. **Trusted SaaS applications:** Certain pre-vetted cloud-based healthcare applications (e.g., telehealth platforms or cloud-based Electronic Health Record (EHR) systems) might be allowed to bypass zero trust inspection for improved performance, ensuring seamless access for clinicians.

javascript
```
if (shExpMatch(url, "*://*.trustedtelehealth.com/*")) return "DIRECT";
```

3. **Latency-sensitive applications:** For applications requiring real-time communication, such as video conferencing (e.g., Zoom) used for remote consultations or medical training, PAC files can be configured to bypass inspection to reduce latency.

javascript
```
if (shExpMatch(url, "*://*.zoom.us/*")) return "DIRECT";
```

Conclusion

Each forwarding mechanism has its advantages and disadvantages when applied to a healthcare environment.

- **GRE and IPsec tunnels** are effective for centralizing security for entire networks but may lack granularity or introduce complexity.
- **Agent-based solutions** provide detailed control and visibility but require more maintenance and resources.
- **Agentless connectors** are essential for environments with non-agent-compatible devices but may limit visibility and control.
- **Cloud-based forwarding** is ideal for modern, cloud native workloads but can be complex and potentially costly.

Healthcare security architects should evaluate their specific needs, considering factors such as network architecture, device diversity, application requirements, and regulatory compliance, to select the most appropriate traffic forwarding mechanisms for their zero trust architecture. This hybrid approach ensures comprehensive security across both user and workload traffic, helping maintain a secure, compliant environment for sensitive healthcare data.

Securing Your Workforce: Internet Access

Securing internet access is the first step in protecting your workforce because it serves as the primary gateway through which threats can enter and sensitive data can leave your organization. In a proxy architecture, all internet-bound traffic is funneled through a central inspection point, ensuring that every request is evaluated against security policies before being allowed. This approach provides visibility into user activity, blocks malicious content, and enforces compliance with corporate policies, significantly reducing the risk of cyberattacks such as phishing, malware, or data breaches.

By securing internet access, you create a strong foundation for a zero trust model, where trust is never assumed, and every connection is continuously verified. This centralized control allows your organization to maintain consistent security policies regardless of where employees are working, whether they're on-site, remote, or on mobile devices. As a result, securing internet access not only protects against external threats but also ensures that your workforce operates within a safe and controlled environment, minimizing vulnerabilities from the very first point of connection.

Device Access/Policy

Below is an outline of a policy framework that incorporates conditional access policies, along with measures like browser isolation, to safeguard against unauthorized access and data exfiltration.

Device Management and Conditional Access Policy

Policy objective: Ensure that all devices, regardless of type or operating system, adhere to the organization's security standards before granting access to network resources, internet, or SaaS applications.

1. Device enrollment and compliance

- **Enrollment:** All devices must be enrolled with the organization's device management system, providing essential details like device type, OS, owner, and compliance status.

- **Security checks:** Regularly verify that each device meets the organization's security requirements, including updated operating systems, security patches, and other critical settings.
- **Access denial for non-compliant devices:** If devices do not meet the compliance requirements deny access to organizational resources containing sensitive information.

2. Conditional access based on security posture

- **Basic compliance requirements:** Define basic compliance checks for all devices, such as having a firewall enabled, up-to-date antivirus software, and encryption of stored data.
- **Access denial for non-compliant devices:** Devices that do not meet the basic compliance requirements will be denied access to the internet and SaaS resources. Users will be notified of the specific compliance failures and guided on how to rectify them.

3. Partial compliance and browser isolation

- **Browser isolation for partially compliant devices:** If a device meets some but not all compliance requirements (e.g., has an antivirus but the firewall is disabled), it may be granted limited access through browser isolation. This ensures that users can access web-based applications without exposing the network to potential threats.
- **Purpose of browser isolation:** Browser isolation runs web sessions in a remote, controlled environment, preventing any downloaded content from reaching the user's device directly. This mitigates the risk of malware infection and data exfiltration.

4. Full compliance and unrestricted access

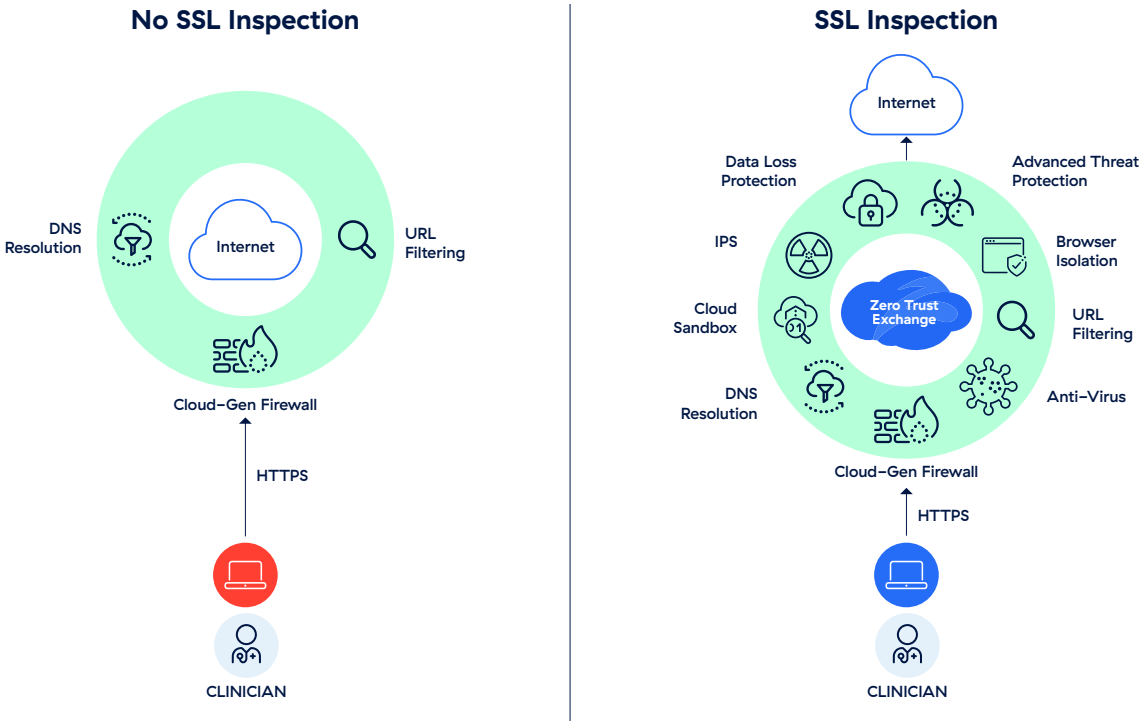
- **Criteria for full compliance:** A device is considered fully compliant when it meets all predefined security criteria, including but not limited to an active firewall, functional antivirus, and updated software.
- **Unrestricted access for compliant devices:** Fully compliant devices are granted unrestricted access to the internet and SaaS applications, following user policy guidelines that govern acceptable use, data protection standards, and monitoring for abnormal activities.

5. Continuous monitoring and adaptation

- **Ongoing compliance verification:** Devices' compliance statuses are continuously monitored, with real-time assessments that can adjust access permissions as the security posture of a device changes.
- **User education and support:** Provide users with clear guidelines on maintaining device compliance and offer coaching t for resolving security issues that may restrict access.

SSL Inspection

Now that users are accessing the internet through a proxy architecture we need to develop a policy for encrypted threats. SSL (secure sockets layer) inspection is a crucial, foundational feature within a zero trust model, offering the ability to decrypt, inspect, and re-encrypt SSL-encrypted traffic at scale. This capability is essential for identifying and mitigating hidden threats within encrypted traffic, such as malware, ransomware, and phishing attempts. 95% of all web traffic is encrypted. 85.9% of threats are delivered via encrypted channels according to a ThreatLabz report. Implementing SSL inspection requires a balanced approach to maintain privacy, compliance, and performance. Here are best practices for SSL inspection policies, tailored for healthcare providers.



Categories and Websites Not to Inspect

1. **Health information sites:** Websites categorized under Health and Medicine should generally be exempt from SSL inspection due to the sensitive nature of the information. Inspecting traffic to these sites could potentially compromise patient confidentiality and violate regulations like HIPAA.

2. **Financial services:** SSL inspection should not be applied to sites categorized under Financial Services. This ensures that sensitive financial transactions and personal financial information are kept secure and private.

3. **Other exemptions:** Categories such as political organizations, religious institutions, and specific legal or HR resources might also be exempt to respect privacy and comply with regulations or organizational policies.

Websites and Categories to Inspect

1. **Webmail and cloud storage:** Webmail and cloud storage sites should be subjected to SSL inspection to prevent data exfiltration and protect against malware that might be uploaded to or downloaded from these services.

2. **Social media:** Given its frequent misuse for phishing and distribution of malware, social media traffic should be inspected.

3. **General browsing:** Websites categorized under General News, Entertainment, and any uncategorized websites should be inspected to prevent access to malicious sites and content that could compromise the healthcare provider's network.

While you may have policies against certain website categories such as cloud storage you should still enforce inspection on these categories as exceptions often happen.

Best Practices for Implementing SSL Inspection

1. **Inform and educate:** Ensure that all staff members are aware of the SSL inspection policies, including which types of traffic will be inspected and the rationale behind these decisions, emphasizing the role of these policies in protecting patient data and healthcare operations.

2. **Regularly update exemption lists:** Keep the lists of exempted categories and websites up to date based on the evolving web landscape, regulatory changes, and organizational needs.

3. **Monitor performance and adjust accordingly:** Continuously monitor the impact of SSL inspection on network performance. Adjust policies as needed to maintain an optimal balance between security and performance, ensuring that critical healthcare applications and services run efficiently.

4. **Ensure compliance with privacy regulations:** Work closely with legal and compliance teams to ensure that SSL inspection policies adhere to all applicable privacy regulations and standards, protecting patient information and the healthcare provider's reputation.

By following these best practices, healthcare providers can effectively utilize SSL inspection to enhance their cybersecurity posture while maintaining the trust of their patients and staff.

Implementing SSL inspection within a zero trust framework for a healthcare provider demands a strategic approach that balances security needs with privacy concerns, regulatory compliance, and network performance.

EXAMPLE POLICIES:

Rule Name	Criteria	Action	Description
ZTH_Recommended Exemptions	URL CATEGORIES Health and Finance	**Do not inspect** – Bypass Other Policies – Block No Server Name Indication (SNI): Disabled	Recommended Exemptions Rule
Exclude Apps – SSL Certificate Pinning	URL CATEGORIES SSLPinnedApplications	**Do not inspect** Evaluate Other Policies – Show End User Notifications: Disabled – Untrusted Server Certificates: Block – OCSP Revocation Check: Enabled – Block No Server Name Indication (SNI): Disabled – Minimum TLS Version: TLS 1.1	Exclude apps which require SSL Certificate Pinning
ZTH_SSL_Inspect_ Catch_All	Any	**Inspect** – Untrusted Server Certificates: Block – OCSP Revocation Check: Enabled – Block No Server Name Indication (SNI): Disabled – Block Undecryptable Traffic: Enabled – Minimum Client TLS Version: TLS 1.2 – Minimum Server TLS Version: TLS 1.2	Default catch–all for SSL Inspection

DNS Security, Firewall Rules, and Advanced Threat Protection

Now that we have done SSL inspection to stop advanced threats we can take our first step into modernizing our security stack. The use of Cloud Firewall plays a good first step in establishing a comprehensive security posture. Here, we explore the best practices for utilizing Cloud Firewall, along with DNS security enhancements, to ensure the highest level of protection for healthcare providers.

Cloud Firewall: Best Practices

Block High-Risk Protocols

Certain protocols are commonly exploited for cyberattacks due to their vulnerabilities or the nature of the data they transmit. Your zero trust enforcement engine allows organizations to block or tightly control the use of such protocols. Healthcare providers should consider blocking protocols known for transmitting unencrypted data, such as Telnet, and ensure that secure shell (SSH) and file transfer protocol secure (FTPS) are used in their place for encrypted data transmission. They should also consider blocking QUIC which is another protocol that security solutions cannot inspect.

EXAMPLE POLICIES:

Rule Name	Criteria	Action	Description
ZTH_BlockICMPQUIC	NETWORK SERVICES QUIC	Block/ICMP	This is an example firewall rule for blocking QUIC protocol on the tenant level
ZTH_Allow_Web	NETWORK SERVICES HTTP; HTTPS	Allow	Allows only Web traffic
ZTH_Allow_NTP_Windows	DESTINATION ADDRESSES time.windows.com NETWORK APPLICATIONS NTP NETWORK SERVICES NTP	Allow	Allows access to NTP to Windows
Default	Default Firewall Filtering Rule	Block/Drop	Default Block Rule

DNS (Domain Name Services) Security Best Practices

1. **Block malicious and suspicious domains**
   Integrating a zero trust enforcement engine with DNS security allows healthcare organizations to block access to malicious and suspicious domains automatically. By leveraging real-time threat intelligence feeds a zero trust enforcement engine can prevent users from accessing domains known for phishing, malware distribution, or command and control (C&C) activities, thus significantly reducing the risk of infection and data breaches.

2. **Use DNS encryption**
   To protect the integrity of DNS queries and prevent interception or manipulation, healthcare organizations should implement DNS over HTTPS (DoH) or DNS over TLS (DoT) using a zero trust enforcement engine. Encrypting DNS traffic ensures that external parties cannot easily spy on or redirect internet traffic, enhancing privacy and security.

3. **Monitor and analyze DNS traffic**
   Continuous monitoring and analysis of DNS traffic can provide insights into network activity and potential security threats. A zero trust enforcement engine's analytics capabilities enable healthcare organizations to identify unusual patterns, such as a spike in DNS requests to known malicious domains, indicating a possible compromise or attack in progress.

EXAMPLE POLICIES:

Rule Name	Criteria	Action	Description
ZTH_Critical risk DNS categories	REQUEST CATEGORIES Phishing; Botnet Callback; Malicious Content; Spyware/Adware; Domain Generation Algorithm (DGA) Domains RESPONSE CATEGORIES Phishing; Botnet Callback; Malicious Content; Spyware/Adware; Domain Generation Algorithm (DGA) Domains	Block	Blocks "Critical risk DNS categories"
ZTH_Critical risk DNS tunnels	DNS TUNNELS & NETWORK APPS BaiduYunDns; DnsTunMaliciousRsvd; Genesis Missionary Baptist Church; Hoff; KrO; LearnZolaSuite; MailShell; Song Mountain FineArt; TGIN; Three Minute Website; ToadTexture; Truckinsurance; WeaverPublishing	Block	Blocks "Critical risk DNS tunnels"
Rule Name	**Criteria**	**Action**	**Description**
ZTH_High risk DNS categories	REQUEST CATEGORIES Other Security; Newly Registered and Observed Domains; Newly Revived Domains RESPONSE CATEGORIES Other Security; Newly Registered and Observed Domains; Newly Revived Domains	Block	Blocks "High risk DNS categories"

ZTH_High risk DNS tunnels	DNS TUNNELS & NETWORK APPS DnsTunUnknownRsvd; DnsTunCatSocial; DnsTunCatIM; DnsTunCatP2P; DnsTunCatStreaming; DnsTunCatWebSearch; DnsTunCatMalware; DnsTunCatImgHost; DnsTunCatEnterprise; DnsTunCatBusiness; DnsTunCatMappStore; DnsTunCatGaming; DnsTunCatNetMgmt; DnsTunCatAuth; DnsTunCatTunneling; DnsTunCatFileTransfer; DnsTunCatDatabase; DnsTunCatConf; DnsTunCatRemote; DnsTunCatMobile; DnsTunCatAds	**Block**	Blocks “High risk DNS tunnels”
ZTH_Unknown DNS Traffic	PROTOCOL Any	**Block**	Applies “Block” action on suspected malformed traffic, non-standard DNS traffic, or even non-DNS traffic attempting to conceal itself as DNS traffic

Advanced Threat Protection

Advanced threat protection (ATP) is designed to protect users against a wide range of cyberthreats, including ransomware, zero-day threats, and unknown malware. When deploying ATP the solution should come equipped with default settings designed to offer robust protection from the get-go. These defaults should include always-on ransomware protection, zero-day threat prevention, C&C protection, blocking anonymizers (i.e., TOR), and blocking p2p such as Bittorrent. ATP solutions offer a significant customization capabilities to tailor the protection features to the specific needs of a healthcare organization. The policy configuration allows for the adjustment of rules, actions, and notifications across different threat categories and scenarios.

URL Filtering/Cloud App Controls

Now that we have the foundational building blocks of the Zero Trust Hospital with SSL Inspection and Advanced threat protection, it is time to move onto URL categories and cloud app controls. URL filtering is usually easier to enforce, blocking access to gambling and adult websites, for example. You can also enforce via URL filters such as end user notification pages with caution messages, overrides, and isolation, for example. Nuances usually come from some of the other categories such as webmail, file transfer sites, generative AI sites, media streaming websites, and social networks. Cloud app controls can allow specific actions on a granular level for a particular website or category. For example, you could allow YouTube as a URL category, but enforce Restricted Mode through cloud app controls.

EXAMPLE POLICIES: URL FILTERING

Rule Name	Criteria	Action	Description
ZTH_Block_Legal_Liability_Class	**PROTOCOL** WebSocket SSL; WebSocket; DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FTP; HTTPS; HTTP; SSLTunnel **REQUEST METHOD** OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER **URL CATEGORIES** Other Adult Material; Adult Themes Lingerie/Bikini; Nudity; Pornography; Body Art; Adult; Sex Education; K–12 Sex Education; Other Drugs; Gambling; Other Illegal or Questionable; Copyright Infringement; Computer Hacking; Questionable; Profanity; Mature Humor; Anonymizer; Militancy/Hate and Extremism; Tasteless; Violence; Weapons/Bombs; Social Networking Adult; Marijuana	**Block With Override** **Override Users: IT Staff**	Commonly blocked URL SuperCategories under Legal Liability Class
ZTH_Block_Security_Globally	**PROTOCOL** WebSocket SSL; WebSocket; DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FTP; HTTPS; HTTP; SSLTunnel **REQUEST METHOD** OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER **URL CATEGORIES** Other Security; Spyware/Adware; Custom Encrypted Content; Dynamic DNS Host; Newly Revived Domains	**Block**	Block the URL Category “Spyware/ Adware”
ZTH_Block_FileHost_Webmail_Globally	**PROTOCOL** WebSocket SSL; WebSocket; DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FTP; HTTPS; HTTP; SSLTunnel **REQUEST METHOD** OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER **URL CATEGORIES** FileHost; Webmail	**Block**	The rule blocks URL Categories FileHost & Webmail globally; Cloud App Control rules handle any exceptions to this rule

EXAMPLE POLICIES: CLOUD APP CONTROLS

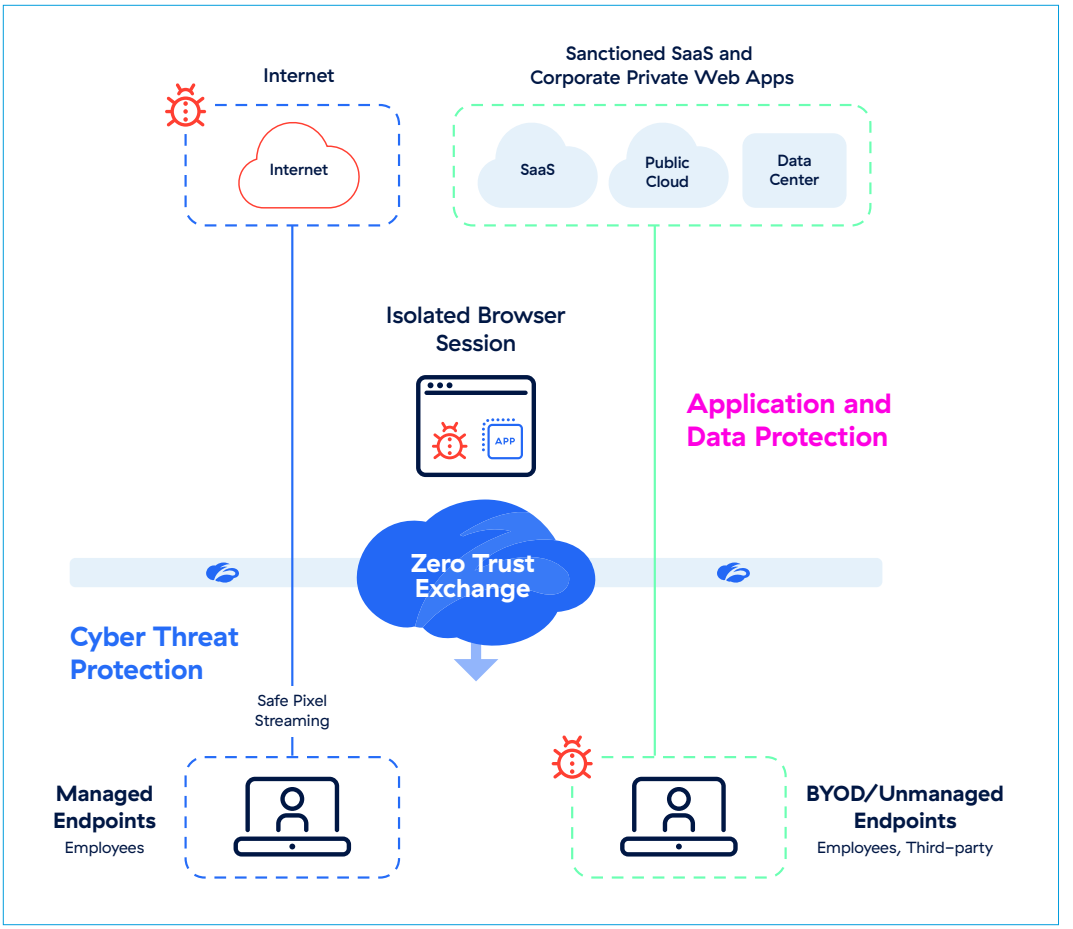
Rule Name	Criteria	Action	Description
ZTH_Block_Any_DNS_Over_HTTPS	APPLICATIONS Any	**Block Application Access**	Block all Cloud Apps under the category "DNS Over HTTPS Service"
ZTH_Isolate_GDrive_Globally	APPLICATIONS GDrive USER AGENT Opera; Firefox; Microsoft Internet Explorer; Microsoft Edge; Chrome; Safari; MS Chromium Edge	Isolate Viewing Mail Isolation Profile IsoProfile_PersonalMailStorage_Global	Isolate GDrive
ZTH_Block_Any_File_Sharing	APPLICATIONS Any	**Block Application Access**	Global block rule for all Cloud Apps classified as "File-Sharing"
ZTH_Allow_Zendesk_Chat	APPLICATIONS Zendesk Chat	**Block File Transfers** **Allow Chatting**	Allow known Customer Support Chat
ZTH_Block_Any_Instant_Messaging	APPLICATIONS Any	**Block Chatting, File Transfers**	Global block rule for all classified as "Instant Messaging"
ZTH_Allow_LinkedIn_Globally	APPLICATIONS LinkedIn	**Allow Viewing, Posting**	Allow LinkedIn Globally
ZTH_Allow_Facebook_Marketing	APPLICATIONS Facebook GROUPS Marketing	**Allow Viewing, Posting**	Allow users within the Group "Marketing" to access Facebook
ZTH_Block_Any_Social_Networking	APPLICATIONS Any	**Block Viewing, Posting**	Global block rule for all classified as "Social Networking"
Rule Name	**Criteria**	**Action**	**Description**
ZTH_Allow_YouTube_Globally	APPLICATIONS YouTube	**Block Uploading** **Allow Viewing/ Listening**	Allow YouTube Globally
ZTH_Isolate_Gmail_Globally	APPLICATIONS Gmail USER AGENT Opera; Firefox; Microsoft Internet Explorer; Microsoft Edge; Chrome; Safari; MS Chromium Edge	**Isolate Viewing Mail** **Isolation Profile IsoProfile_PersonalMailStorage_Global**	Isolate Gmail
ZTH_Block_Any_Webmail	APPLICATIONS Any	**Block Viewing Mail, Sending Attachments, Sending Mail**	Global block rule for all classified as "Webmail"

Cloud Sandboxing and Browser Isolation

It is important that you also have protections in place to offer browser isolation and cloud sandboxing, which are instrumental in ensuring that browsing activities and file downloads do not compromise network integrity or patient data privacy.

Browser Isolation

Browser isolation works by rendering web content in a secure, cloud-based environment away from the end user's device. This means potentially harmful content is kept at arm's length, preventing malware or phishing attacks from reaching the user or the organization's network.



KEY FEATURES FOR HEALTHCARE PROVIDERS

- **Cloud-based rendering:** This feature ensures that all active web content (JavaScript, HTML5, etc.) is executed away from the user's device, minimizing the risk of malware infections.

- **Data protection controls:** Browser isolation can prevent sensitive information from being typed into unauthorized web forms, helping to protect patient data and comply with regulations like HIPAA.

POLICY EXAMPLES

1. **High-risk web browsing:** Implement browser isolation for accessing websites not categorized as business-related or medical research, such as personal webmail, social media, or newly registered domains that could pose higher security risks.

2. **Patient education content:** To safeguard both network security and patient data, healthcare providers can utilize browser isolation when patients access educational content on shared devices within the healthcare facility, ensuring that any external risks are neutralized.

Sandboxing

Sandboxing involves executing or opening files in a secure, isolated environment to analyze their behavior for signs of malware or other threats. This is crucial for preventing zero-day threats and advanced malware from infiltrating healthcare networks.

KEY FEATURES FOR HEALTHCARE PROVIDERS

- **Automated file analysis:** Automatically sends files that are downloaded from the internet to the sandbox for analysis, ensuring they are safe before they reach an end user's device.

- **Quarantine and remediation:** If a file is found to be malicious, automatically quarantine it and prevent it from causing harm, while also providing tools for remediation.

POLICY EXAMPLES

Rule Name	Criteria	Action	AI Instant Verdict	Description
ZTH_Office PDF SandboxRule	**FILE TYPES** Microsoft Excel (xls, xlsx, xlsm, xlam, xlsb, slk, xltm); Microsoft Word (doc, docx, docm, dotx, dotm); Microsoft Rich Text Format (rtf); Microsoft PowerPoint (ppt, pptx, pptm, potx, ppsx, ppam, potm, ppsm) Portable Document Format (pdf) **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; Sandbox Suspicious **PROTOCOLS** HTTPS; HTTP	**Quarantine and Isolate First Time** **Block Subsequent Downloads** **Isolation Profile** **"ZTH_ IsolationProfile"**	Enabled	While sandbox analysis is in progress, a safer file version can be viewed within the isolation browser
ZTH_ Windows_ Executables	**FILE TYPES** Windows Library (dll64, dll, ocx, sys); Windows PowerShell Script (ps1); Windows Executable (exe, exe64, scr); Visual Basic Script (vbs) **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; Sandbox Suspicious	**Allow and scan First Time** **Block Subsequent Downloads**	Enabled	Users in the group "IT_Admins" download "Executables" from a destination that is classified as "Shareware Download" without "Quarantine First Time"
Rule Name	**Criteria**	**Action**	**AI Instant Verdict**	**Description**
	GROUPS IT_Admins **URL CATEGORIES** Shareware Download			
ZTH_ CatchAll	**FILE TYPES** All file types **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; Sandbox Suspicious **URL CATEGORIES** Any URL Category	**Quarantine First Time** **Block Subsequent Downloads**	Enabled	The first action is set to Quarantine for all file types and any URL Category

IMPLEMENTING BROWSER ISOLATION AND SANDBOXING

To effectively utilize browser isolation and sandboxing within a zero trust enforcement engine, healthcare providers should consider the following best practices:

- **User education and awareness:** Educate users on the importance of these security measures and how they protect the organization's network and patient data. Understanding the rationale behind browser isolation and sandboxing can foster compliance and reduce risky online behaviors.

- **Customize policies based on user roles:** Tailor browser isolation and sandboxing policies based on user roles and departments. For instance, research departments may require broader access to medical journals and educational content, whereas administrative departments might need stricter controls on web access and file downloads.

- **Continuous monitoring and adjustment:** Regularly review and adjust isolation and sandboxing policies to reflect the changing cyberthreat landscape and the evolving needs of the healthcare organization. This includes updating allowlists and blocklists and refining rules to ensure optimal balance between security and usability.

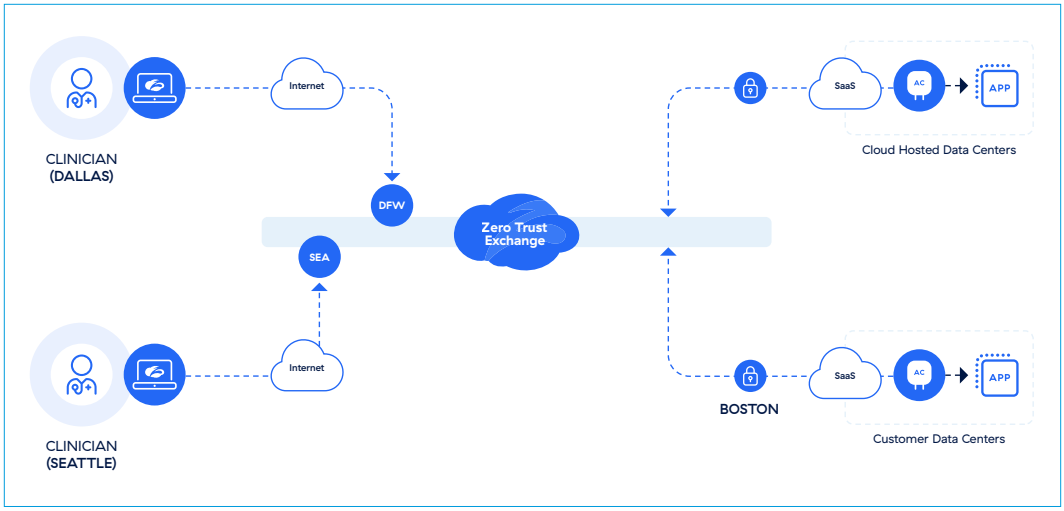
- **Integrate with other security layers:** Integrate browser isolation and sandboxing with other security features, such as cloud app controls.

Browser isolation works by rendering web content in a secure, cloud-based environment away from the end user's device. This means potentially harmful content is kept at arm's length, preventing malware or phishing attacks from reaching the user or the organization's network.

EXAMPLE: BROWSER ISOLATION SETTINGS

Isolation Profile Configuration	
General	
Name	ZTH_GlobalIsolation
Description	Forces Isolation for Websites that are labeled insecure such as Gdrive or other file Sharing websites or other websites deemed necessary. Enforces read only and Disables other features.
Security	
ALLOW COPY & PASTE FROM	
Local computer to isolation	Disabled
Isolation to local computer	Disabled
ALLOW FILE TRANSFERS FROM	
Local computer to isolation	Disabled
Isolation to local computer	Disabled
ALLOW PRINTING	
Allow printing from isolation	Disabled
RESTRICT TEXT INPUT	
Read-Only Isolation	**Enabled**
ALLOW VIEWING OFFICE FILES	
View office files in isolation	Disabled
LOCAL BROWSER RENDERING	
Allow local browser rendering	Disabled
Isolation Experience	
ISOLATION BANNER PREVIEW	
Isolation Banner	Disabled
Persist Browser Isolation URL bar	Disabled
Isolation Experience	Native browser experience
WATERMARKING	
Enable Watermarking	Disabled
COOKIE PERSISTENCE	
Cookie Persistence	Enabled

Private Application Access



Now that we have secured the internet for your workforce, it's time to move over to accessing applications, regardless of where they live. Zero trust network access (ZTNA) represents a cornerstone framework for healthcare providers navigating the complexities of securing access to private applications. In an era where digital transformation is happening rapidly, ZTNA ensures that only authenticated users can access critical healthcare applications whether on premise or in the cloud. This is different then a traditional VPN, as a traditional VPN connects a user to a network which offers an attacker the ability to move laterally to many other systems. ZTNA instead connects a user to the application and not the network. An NMAP or similar port scan would instead be greeted with a synthetic IP, versus a hospital's internal network layer. By leveraging features such as conditional access policies, SCIM attributes, location-based access, AI-generated application segments, and wildcard policies, healthcare organizations can rapidly deploy ZTNA to increase their security posture. Below, we explore best practices for utilizing ZTNA in a healthcare setting.

Utilizing Wildcard Policies for Streamlined Deployment

Wildcard policies in ZTNA help expedite the deployment process by allowing administrators to specify broad application access rules using wildcard characters. This approach is particularly useful when deploying application segmentation across diverse healthcare applications and services.

EXAMPLE POLICY:

Rule Name	Criteria	Action	Description
ZTH_EHR Access	**Application** EHRO1.hospital.org EHRO2.hospital.org **Ports** TCP 443 Group Doctors and Nurses **Device Posture** Managed Device Zero Trust Agent	**Allow**	Allows EHR access for the doctors and nurses group within the IDP while restricting access to only devices that are managed and using the ZT Agent
ZTH_Wildcard	**Application** *.hospital.org **Ports** TCP 1–52 54–6553 UDP 1–52 54–6553 Group Company Wide Device Posture Managed Device Zero Trust Agent Trusted Location	**Allow**	Wildcard policy used during a discovery phase of identifying what applications and ports are being used by which users. Only accessible by a trusted location, ZT agent, and managed device

REFINING WILDCARD POLICIES TOWARDS ZERO TRUST

Starting with wildcard policies allows for quick deployment, after which healthcare IT administrators can analyze usage patterns and progressively refine these policies to be more granular, moving closer to a true zero trust architecture.

EXAMPLE REFINEMENT PROCESS:

1. **Initial deployment:** Implement a wildcard policy to cover all applications under a certain domain. Block known bad. Example: Known HR systems should be allowed for HR but blocking Finance from accessing those HR systems.

2. **Monitoring and analysis:** Use analytics to monitor access patterns and identify which applications are being accessed and by whom.

3. **Policy refinement:** Gradually refine the wildcard policy into more specific application segments or policies based on user role, department, or other attributes, ensuring that users have access only to the applications necessary for their specific job functions.

AI-Generated Application Segments

AI-generated application segments utilize machine learning to analyze traffic patterns and user behavior, automatically identifying and categorizing applications. This feature helps healthcare IT teams quickly understand application usage and adjust access policies accordingly. This can cut down deployment time as users use a wide variety of applications and it is not uncommon to see thousands of applications in an environment used by many different groups.

EXAMPLE POLICY:

- **Segmentation of research applications:** Automatically generate segments for various research applications used within the healthcare provider's network. Restrict access to these segments to authorized research personnel only, based on their specific research projects or departmental affiliations.

Conditional Access Policies

Conditional access policies ensure that access to applications is based on the context of the access request. In healthcare, where access to electronic health records (EHRs), patient management systems, and internal portals is restricted based on role, location, and device compliance, conditional access is indispensable.

EXAMPLE POLICY:

- **EHR System Access:** A policy can be created where only medical staff accessing the EHR system from a managed device within the hospital network is allowed. If access is attempted from an unmanaged device or external network, additional authentication (e.g., multifactor authentication) is required.

SCIM/SAML Attributes for Application Access

SAML/SCIM attributes allow for hospitals to assign access to applications based on user attributes such as group membership, speeding up time to deploy applications on ZTNA. This is particularly beneficial in large healthcare organizations with high staff turnover or fluctuating roles.

EXAMPLE POLICY:

- **Radiologist group:** Using SCIM, automate the process of granting or revoking access to specific applications based on the user's group. For instance, automatically grant new hires in the radiology department access to imaging software and patient databases as soon as their role is assigned in the HR system.

Location-Based Access Controls

ZTNA allows organizations to define location-based access controls that enhance security and compliance.

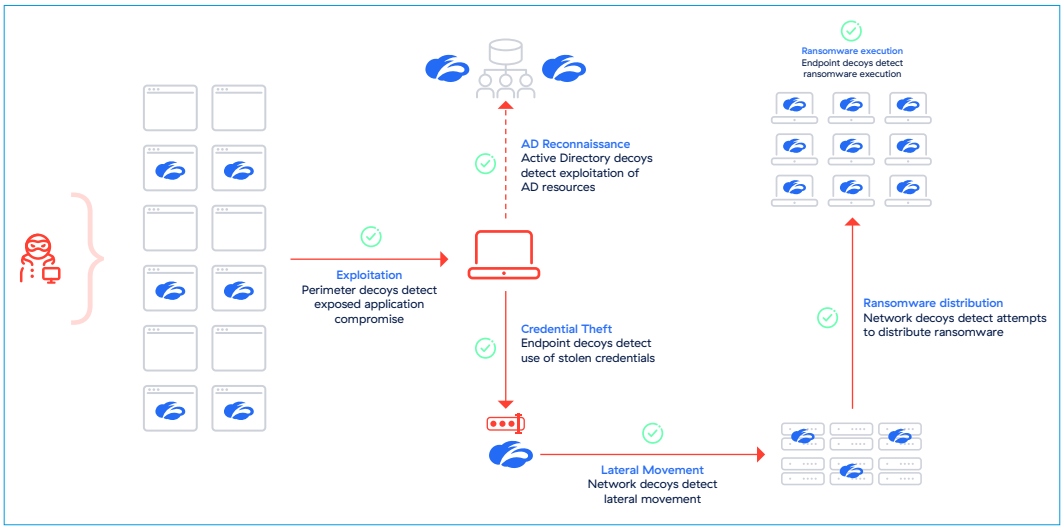
EXAMPLE POLICY:

- **Access to pharmacy systems:** Restrict access to pharmacy management systems to users within secure hospital locations. If a user attempts to access the system from a non-approved location, such as a public internet connection, access is denied or restricted.

ZTNA ensures that only authenticated users can access critical healthcare applications whether on premise or in the cloud.

Deception

Now that we have started to secure private applications, we need to discuss what happens for private applications that may get compromised or public applications still available on the internet. Deception technology serves as a fortification of existing defenses against increasingly sophisticated cyberthreats. Deception adds an active defense layer that misleads attackers, thereby not only preventing unauthorized access but also gathering intelligence about attack methodologies and intentions.



Key Features of Deception Technologies

1. **Decoys and lures:** Deception creates realistic, but entirely false, representations of network resources, applications, and data. These decoys mimic the behavior and appearance of critical systems, such as EHR systems (websites) or internal healthcare databases, to attract attackers, diverting them from real assets.

2. **Traffic and behavior analysis:** The system monitors network traffic and user behavior in real-time, using sophisticated algorithms to identify patterns indicative of a cyberattack. Once suspicious activity is detected, it redirects the activity to a decoy, effectively isolating the threat.

3. **Automated threat response:** Upon detection of an attack attempt, deception automatically triggers security protocols to isolate the threat, analyze the attack vector, and neutralize the threat. This immediate response limits the potential impact of the attack and provides valuable threat intelligence.

4. **Seamless integration:** Zscaler Deception™ integrates with existing security infrastructure and the broader security platform, enhancing overall security posture without requiring significant changes to current systems or workflows.

EXAMPLE POLICIES FOR HEALTHCARE PROVIDERS

Implementing Deception requires careful planning and policy formulation to ensure that deception strategies are both effective and aligned with healthcare operational needs. Below are examples of policies that healthcare providers can implement:

5. **Decoy patient records system:** Create a decoy version of the patient records system filled with fake patient data. Any attempt to access or exfiltrate data from this system can trigger an alert, indicating a potential breach or unauthorized access attempt.

- **Policy objective:** To detect and analyze attempts to access patient information, providing an early warning system for data breaches.

- **Implementation consideration:** Ensure that the decoy system is indistinguishable from the real patient records system to effectively attract attackers.

6. **Fake administrative portals:** Develop several fake administrative portals for finance, human resources, and other non-medical departments. These portals can serve to identify attackers targeting financial data or personal information of healthcare staff.

- **Policy objective:** To protect sensitive administrative data by misleading attackers with fake portals, thereby safeguarding real financial and HR systems.

- **Implementation consideration:** Regularly update the appearance and functionality of these decoy portals to match updates to the genuine portals.

7. **Lures in email communications:** Embed lures, such as links to decoy systems or fake login pages, in internal email communications. These lures can detect phishing attempts or unauthorized internal access.

- **Policy objective:** To identify malicious insiders or external attackers who have compromised internal email systems.
- **Implementation consideration:** Ensure that lures are discreet and plausible within the context of normal email communications to maintain operational integrity.

8. **Decoy research data repositories:** For healthcare providers involved in research, creating decoy versions of research data repositories can help identify unauthorized access attempts to sensitive research data.

- **Policy objective:** To protect intellectual property and sensitive research data by diverting attackers to fake repositories.
- **Implementation consideration:** Populate decoy repositories with realistic but fake research data and ensure they mimic the access patterns of genuine repositories.

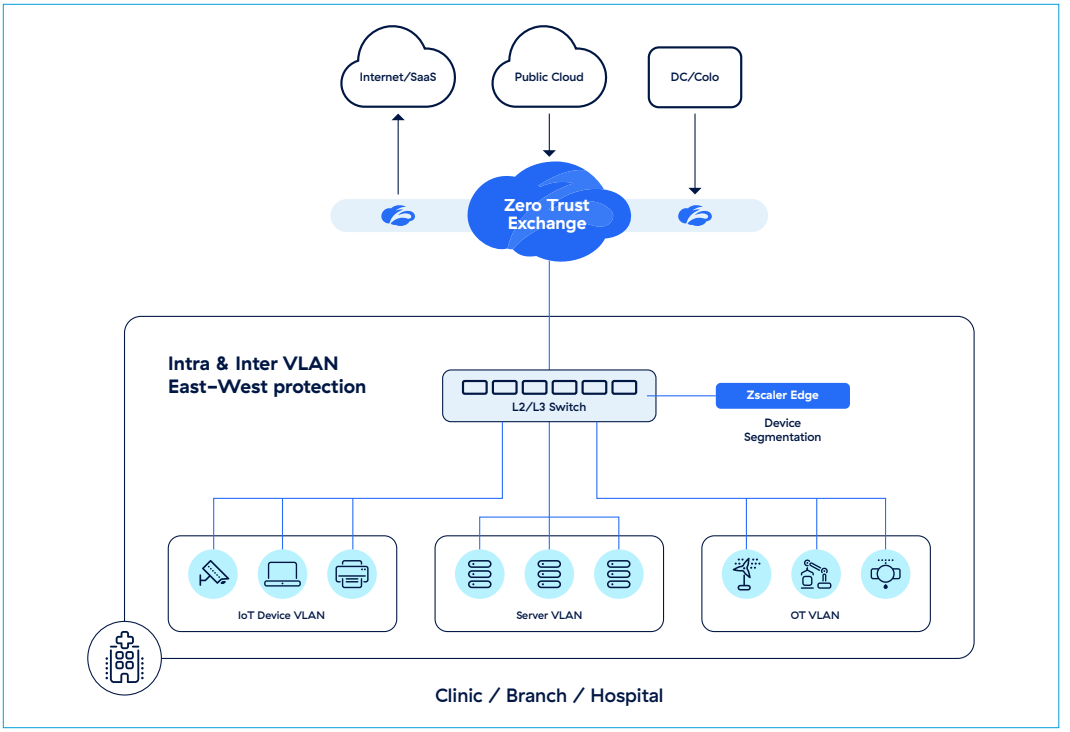
Through the strategic use of decoys, lures, and integrated threat response mechanisms, healthcare organizations can significantly enhance their ability to detect, deceive, and defeat cyberthreats.

Securing Internet of Medical Things (IoMT) and Guest Wi-Fi

Not every system or device can support an agent installation, especially when considering devices like IoMT equipment, printers, or other non-traditional endpoints that lack the capability to run an agent. Additionally, networks such as guest Wi-Fi require secure traffic forwarding without relying on endpoint agents. In this section, we'll explore the various methods available for forwarding traffic to a zero trust proxy, ensuring comprehensive protection across all types of devices and networks, even when an agent-based approach isn't feasible.

Internet of Medical Things

Internet of Medical Things (IoMT) make up a large number of devices in a healthcare provider environment. Securing them can be complicated due to the inability of leveraging agents and potentially heavily locked down operating systems. These devices though often serve as a risk for compromise due to the very nature that keeps them secured, such as difficulty patching.



Discovering IoMT Devices

The first step in securing IoMT devices is accurately discovering and inventorying them across the healthcare provider's network. To facilitate this process the following steps can be done:

1. **Traffic analysis:** You need to be able to analyze network traffic patterns to identify devices that communicate with known IoMT-specific services and applications. This analysis helps in pinpointing devices that might not be cataloged or known to IT departments.

2. **SSL inspection:** By inspecting encrypted SSL traffic, you can provide visibility into the data being transmitted to and from IoMT devices. This can reveal device types, manufacturers, and the nature of the information being processed, aiding in the identification process.

Classifying IoMT Devices

Once IoMT devices are discovered, classifying them according to their function, data sensitivity, and risk level is critical. Healthcare providers should classify devices based on several criteria:

1. **Device type and purpose:** Classify devices based on their medical purpose (e.g., patient monitoring, diagnostic equipment, wearable health devices) to understand the nature of the data they handle and their criticality to patient care.

1. **Manufacturer and model information:** Classify devices by their manufacturer and model to identify known vulnerabilities, supported protocols, and security features. This information can be used to assess the security posture of each device type.

2. **Communication patterns:** Analyze the communication patterns of IoMT devices, including destination services, frequency of communication, and data volume, to further classify devices by their operational behavior.

Defining Security Policies

With a clear understanding of the IoMT devices in operation and their classifications, healthcare providers can then define security policies that are both effective in mitigating risks and tailored to the operational needs of each device type. A zero trust engine facilitates this through:

1. **Segmentation policies:** Use a zero trust engine to create segmentation policies that isolate IoMT devices from other parts of the network, or group similar device types together, minimizing the risk of lateral movement by cyberthreats.

2. **Access control policies:** Define policies that restrict which services and applications IoMT devices can access, and which devices can access IoMT data, based on the classification of the device and the sensitivity of the data.

3. **Threat protection policies:** Implement threat protection policies tailored to the vulnerabilities and risks associated with specific IoMT device categories. This might include applying more stringent antivirus and malware protection to devices known to be vulnerable.

4. **Data protection policies:** For devices handling highly sensitive patient data, apply data protection policies that include encryption requirements for data at rest and in transit, as well as data loss prevention (DLP) mechanisms.

5. **Compliance monitoring:** Ensure that IoMT devices comply with healthcare regulations such as HIPAA by monitoring device activity and data handling practices against compliance benchmarks.

Guest Wi-Fi Policies

In a healthcare environment, securing guest Wi-Fi is essential to prevent unauthorized access and potential threats while ensuring that patients and visitors can enjoy a user-friendly experience. By leveraging traffic forwarding mechanisms such as GRE Tunnels, IPsec tunnels, or agentless forwarders, healthcare providers can route guest Wi-Fi traffic to a central zero trust enforcement point, enabling comprehensive policy enforcement. Here are key policies that healthcare providers should implement to secure guest Wi-Fi traffic effectively:

1. **Network segmentation:** Ensure that guest Wi-Fi traffic is completely segmented from the internal network. This can be achieved using traffic forwarding mechanisms like GRE or IPsec tunnels, which route guest traffic separately to a central inspection point. This approach prevents any potential threat actors from using the guest network to access sensitive healthcare systems, patient data, or IoMT devices.

2. **Content filtering:** Apply content filtering through your central proxy architecture to restrict access to inappropriate or high-risk websites, such as gambling, adult content, or known malware/phishing sites. This helps reduce the risk of malware infections and ensures that guest users are not engaging in potentially harmful activities while connected. Traffic forwarding mechanisms ensure that all guest traffic passes through the central inspection point for filtering.

3. **Bandwidth management:** Implement bandwidth throttling for guest Wi-Fi users to prevent them from consuming excessive bandwidth that could affect critical healthcare applications. This can be enforced through the zero trust proxy, ensuring activities like video streaming or large downloads don't impact network performance.

4. **Authentication and access control:** Require guest users to authenticate before accessing the Wi-Fi network, such as through a captive portal with terms and conditions, one-time passwords (OTPs), or temporary access codes. By forwarding this traffic to the central zero trust enforcement point, you can ensure that only authorized guests connect, while also maintaining a record of who is using the network.

5. **Malware protection:** Route all guest Wi-Fi traffic through your central zero trust proxy using GRE or IPsec tunnels to ensure that it is inspected for threats. This allows for real-time malware scanning, threat detection, and protection against cyberattacks originating from guest devices.

6. **Logging and monitoring:** Utilize the traffic forwarding mechanisms to route guest Wi-Fi traffic through a central enforcement engine where it can be logged and monitored in real-time. This approach allows for rapid identification and response to any suspicious behavior or potential security incidents, ensuring that any attempted breaches are quickly addressed.

7. **Restricted access to internal resources:** Ensure that guest Wi-Fi users cannot access any internal healthcare applications, systems, or IoMT devices. This includes blocking access to shared drives, printers, and other networked resources, and can be enforced through the traffic forwarding mechanisms, maintaining strict network separation.

8. **Session timeout and inactivity policies:** Implement automatic session timeouts for guest Wi-Fi users through the central proxy, ensuring that devices are disconnected after a specified period of inactivity. This reduces the risk of unauthorized access from abandoned devices and maintains the overall security of the network.

In a healthcare environment, securing guest Wi-Fi is essential to prevent unauthorized access and potential threats while ensuring that patients and visitors can enjoy a user-friendly experience.

EXAMPLE POLICY IMPLEMENTATION

- **Access policy:** All guest users must authenticate via a captive portal with OTPs, and access will be restricted to internet browsing only. Internal resources such as file servers, IoMT devices, or printers will be blocked, maintaining a clear separation enforced through GRE or IPsec tunnels.
- **Content filtering policy:** Websites associated with gambling, adult content, or known threat categories will be restricted at the central enforcement point. Additionally, bandwidth for activities like video streaming will be limited to ensure network performance for critical healthcare applications.
- **Session management policy:** Users will be automatically disconnected after 30 minutes of inactivity, requiring reauthentication to regain access.

By integrating traffic forwarding mechanisms like GRE tunnels, IPsec tunnels, or agentless forwarders with these policies, healthcare providers can effectively enforce security controls on guest Wi-Fi traffic. This approach ensures that all traffic is routed through a central zero trust proxy, allowing for comprehensive inspection, monitoring, and control, while simultaneously providing a safe and convenient service for visitors. This strategy not only protects against potential threats but also ensures compliance with security standards, maintaining a secure environment across all aspects of the healthcare network.

CHAPTER 3

Prevent Data Loss

You have now provided application access and secure internet access to your workforce, but a crucial step still remains. Data protection encompasses more than just a file being sent to the wrong person but inadvertently using tools that are not sanctioned or exposing data via publicly accessible links. Data loss protection (DLP) has 5 critical steps to be successful.

1. Obtain full visibility
2. Block risky destinations and threats
3. Gain control of content types
4. Control sensitive data
5. Manage incidents through the entire life cycle

Acronyms and definitions that will be used throughout this section:

Acronym	Definition
DLP – Data Loss Prevention	This technology typically will incorporate discovery, monitoring, visibility and control of data. Deployed for data in motion or data in use.
CASB – Cloud Access Security Broker	Developed for discovery, control, protection and governance of SaaS applications. Traditionally, CASB was primarily an out of band tool meaning not in line of the traffic to provide shadow IT visibility and take actions in SaaS services like to prevent sharing or remove collaborators. A key pillar of CASB is preventing data loss from the data at rest in these SaaS apps.
EDM – Exact Data Match	Typically, customers will have databases of information, like their customer data or their own user data in columns and rows stored. This data is vital for an organization to protect. EDM removes any false positives because it is looking for very specific information. For example: John Smith at 1 Privet Drive with SSN 345–47–8842
IDM – Indexed Document Matching	IDM allows customers to submit templates of their unstructured data. Unstructured data is data that is not organized in tables with columns and rows. The data is all over the page. We basically take the words out of the document and then look for those words in any uploaded files. This helps a customer protect their intellectual property, confidential information, forms, and PII.
OCR – Optical Character Recognition	When thinking about DLP, office documents, PDFs or simple text comes to mind. However, what about a scenario in which a PDF includes an image that has information or when a plain image is uploaded that has sensitive content? In that case, OCR will extract the text from the image to make it available to the DLP engines. This expands coverage and mitigates the risk of loss or leakage significantly. Just remember OCR is not an exact science, think of our banking app scanning checks, you have to have perfect light, zoom, angle, etc.

The wide use of risky and unsanctioned applications is a challenge for hospital providers. It can be difficult to control what you can't see, and this impacts the effectiveness of corporate/sanctioned applications. This is why the first step to securing your data is complete visibility. A zero trust engine is not only your proxy to move data away from your data center assets but also your inline SSL inspection platform, identifying data at rest using CASB and securing third party applications. Using a zero trust engine you can inspect all users and devices, on or off the network. Leverage a comprehensive cloud app database to enable providers to sanction applications based on usage and risk score. You can then allow providers to define policy based upon risk score and company tolerance.

File Type Controls

File type controls are crucial for preventing unauthorized transfer or sharing of sensitive files. Healthcare providers can leverage their zero trust platform to block or restrict the transfer of specific file types for unscannable files.

EXAMPLE POLICIES

Rule Name	Criteria	Action	Description
ZTH_Block_Suspicious	**ACTIVE CONTENT** Disabled **FILE TYPES** ZIP w/Suspicious Script (js, vbs, svg, ps1, hta, cmd, lnk) **UNSCANNABLE FILE** Disabled	Block	Block "ZIP w/Suspicious Script File" File Type
ZTH_Block_Database	**ACTIVE CONTENT** Disabled **FILE TYPES** Virtual Hard Disk Files (vhd, vhdx, vmdk); ACCDB (accdb); DBF (dbf); DB2SQL (sql, sqlproj, eql); KeePass Password Manager Files (kdbx); EDMX Files (edmx); FRM (frm); DB file (db);	Block	Block all "Database" File Type

Rule Name	Criteria	Action	Description
	MS Access Project (ade); SDB files (sdb) **UNSCANNABLE FILE** Disabled		
ZTH_Allow Executables URL Category	**ACTIVE CONTENT** Disabled **FILE TYPES** Microsoft Installer (msi); Windows Executable (exe, exe64, scr); Appx (appx) **URL CATEGORIES** Operating System and Software Updates **UNSCANNABLE FILE** Disabled	Allow	Allow specific executables types from the URL Category "Operating System and Software Updates"
ZTH_BlockExecutable	**ACTIVE CONTENT** Disabled **FILE TYPES** Bash Script (sh); Registry (reg); Batch (.cmd, .bat); Shell Scrap Object (shs); Microsoft Installer Patch (msp); Appx (appx); DEB; Microsoft Installer (msi); Msc (msc); ELF (elf); Windows Shortcut (lnk); Python (py, p, pkl, pickle, pyd, pyw) **UNSCANNABLE FILE** Disabled	Block	Block Executables
ZTH_Block_ALL_ Shareware	**ACTIVE CONTENT** Disabled **FILE TYPES** Choose ALL File Types **URL CATEGORIES** Shareware Download **UNSCANNABLE FILE** Disabled	Block	Block ALL File Types from specific URL SubCategory "Shareware Download"

Inline DLP

Data loss prevention engines and dictionaries come out of the box with most DLP platforms. These engines and dictionaries can be used to create policies to secure your organizations data. Some of these out of the box dictionaries include medical information, legal documents, gambling, tax information, financial information, and many others. You can also add your own dictionaries. Some common ways to add these dictionaries is by using IDM and using a pattern in Regex. Some common IDM patterns that healthcare providers may want to add are the following:

ICD-10 CODES

```
\b[A-TV-Z]\d{2}(?:\.\d{1,4})?\b
```

Explanation of the regex pattern:

- \b – Matches a word boundary to ensure that the ICD-10 code is a standalone word.
- [A-TV-Z] – Matches a single uppercase letter from A to T or V to Z. This excludes the letter U, as it is not used as an initial letter in ICD-10 codes.
- \d{2} – Matches exactly two digits.
- (?:\.\d{1,4})? – Matches an optional decimal point followed by one to four digits. This allows for the inclusion of a decimal in the ICD-10 code, such as "A00.1" or "B99.9999."
- \b – Matches another word boundary to ensure the ICD-10 code ends as a standalone word.

NDC-10

```
\b\d{4}-\d{4}-\d{2}\b
```

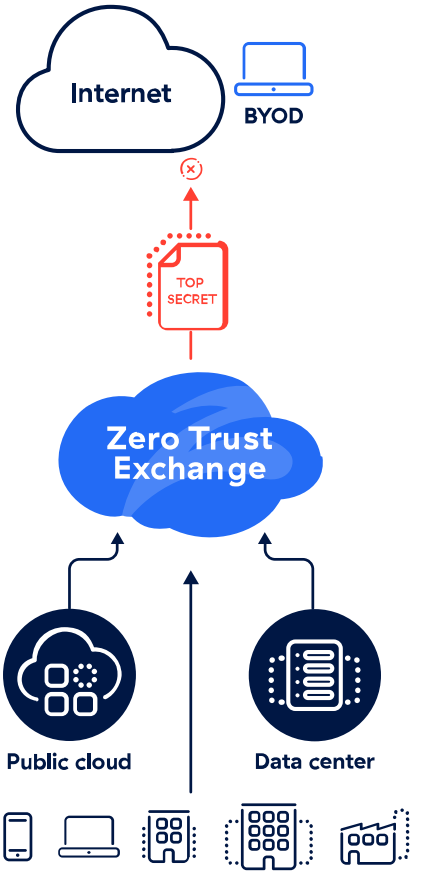
Explanation of the regex pattern:

- \b ensures that the code is bounded by word boundaries, so it matches standalone NDC-10 codes.
- \d represents any digit (0-9).
- {4} specifies that the previous pattern (digit) should be repeated exactly 4 times.
- - matches the hyphen character literally, as it separates the three parts of the NDC-10 code.
- {2} specifies that the previous pattern (digit) should be repeated exactly 2 times.

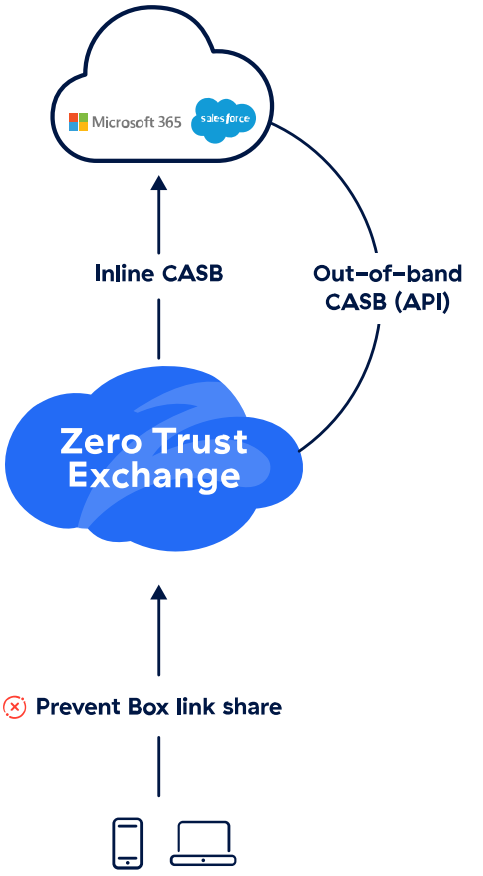
It is important to note these patterns are not checked against a database and matched exactly to those codes. These are looking for patterns that contain these variables. If you want to use a database of codes, you should use EDM. EDM is another common way to add dictionaries to your DLP platform. EDM will allow you to upload a file that contains a database of information such as all of the ICD-10 codes. This will allow the DLP platform to do exact matches on those codes.

Once you have added your dictionaries you will be able to add these into a DLP engine. Engines that come out of the box include HIPAA, medical information, PCI, etc. These engines will use a combination of dictionaries and counts based on what is found to then put into policy. A sample engine would be "((Medical Information > 0))" which takes the medical information dictionary and anything greater than a count of 0 will trigger the engine.

Prevent inline data loss to Web and BYOD



Secure SaaS data with CASB



EXAMPLE POLICIES

Rule Name	Criteria	Action	Description
ZTH_PHIAlert	**DLP Engine** PHI < 5 **Groups** Radiologists, HR, Doctors, Nurses **URL Categories** ALL	**Alert/Allow**	Allow and alert any PHI hit record that is under 5 records for Radiologists, Nurses, HR, Doctors, and Nurses for any url category
ZTH_EDMAlert	**DLP Engine** EDMO1 > O **Groups** Doctors **URL Categories** Cloud Storage Platform	**Alert/Allow**	Alert and allow anything in the EDM database greater than O records but less than 24 for the group “Doctors” for a chosen cloud storage platform
ZTH_PHI	**DLP Engine** PHI > 24 **Groups** ALL **URL Categories** ALL	**Block**	Block anything that is labeled as PHI that is greater than 24 records for all users and categories
ZTH_EDMBlock	**DLP Engine** EDMO1 > 24 **URL Categories** File Sharing, PDF Converters, Social Media	**Block**	Block anything in the EDM database greater than 24 records for the URL categories File Sharing, PDF Converters, Social Media

Endpoint DLP

Healthcare institutions now have the means to implement endpoint DLP policies tailored to their unique environments. Endpoint DLP policies play a crucial role in safeguarding data across various “channels,” such as removable media, cloud storage, and applications. Endpoint DLP solutions offer flexible policy configuration options tailored to specific data protection needs. For healthcare organizations, this means the ability to set policies based on factors like data type, user roles, and the context of data use.

CONFIGURING POLICIES FOR SPECIFIC CHANNELS

The first step in deploying Endpoint DLP is to identify the channels through which sensitive data could potentially be exposed. In a healthcare context, this often includes:

- **Removable media:** USB drives and other removable storage devices are convenient but pose a high risk for data loss. Policies can be configured to monitor and restrict the transfer of patient information to unauthorized devices.

- **Cloud storage and applications:** With the increasing use of cloud services for data storage and collaboration, policies must ensure that sensitive data is not inadvertently shared outside the organization.

For each channel, a DLP platform allows the selection of specific "channel settings" that dictate how data transfers are monitored and controlled.

LEVERAGING USER AND CONTEXTUAL CRITERIA

Beyond channel settings, endpoint DLP policies in your platform should be further refined by defining criteria such as user roles, file types, and the sensitivity of the data. For example:

- **User-based policies:** Differentiating policies based on user roles—such as clinicians, administrative staff, and IT personnel—ensures that data access and transfer permissions align with job requirements.

- **File type restrictions:** Healthcare organizations can specify policies based on file types, ensuring that sensitive formats containing patient data (e.g., DICOM files for medical imaging) are adequately protected.

PROMOTING USER ENGAGEMENT AND COMPLIANCE

A feature of an endpoint DLP solution is its ability to engage users directly through prompts and notifications. When a user's action is blocked due to policy violation, they can receive a customizable notification explaining the reason. This notification can include an option for the user to provide justification for the action, such as verifying the absence of sensitive information in the file. This "user coaching" approach not only enhances policy compliance but also educates users about data protection best practices.

POLICY EXAMPLES FOR HEALTHCARE DEPLOYMENT

- **Removable media control:** A policy might block the transfer of any file containing protected health information (PHI) to removable media, unless the user is a designated IT administrator performing a backup process.

- **Cloud storage monitoring:** Another policy could automatically encrypt files containing sensitive patient data before they are uploaded to approved cloud storage solutions, ensuring that data remains protected even outside the organization's direct control.

Out-of-Band CASB

The healthcare industry's increasing reliance on software as a service (SaaS) applications for data storage, communication, and operations management necessitates robust cybersecurity measures. A CASB platform facilitates the onboarding of SaaS applications, provides granular access control, and enables automatic remediation—all without the need for an agent.

GRANULAR ACCESS CONTROL AND REPORTING

Through the CASB platform, healthcare IT administrators can configure detailed access control policies tailored to the organization's specific needs. These policies can range from prohibiting the use of public sharing links to enforcing read-only access for sensitive data. Restrictions can also be applied to specific groups or users, ensuring that access to critical healthcare data is tightly controlled.

For example, a policy might restrict access to patient records in Salesforce to only those healthcare professionals directly involved in patient care, while another policy could prevent the use of public sharing links for any data stored in Box, mitigating the risk of accidental exposure.

Your platform should have robust reporting capabilities that provide administrators with a clear view of SaaS application traffic, enabling the identification of potential security risks. The Analytics -> SaaS Security Reports section allows for the monitoring of compliance with established policies, and automatic or manual remediation actions can be taken directly from the platform.

AUTOMATED REMEDIATION AND REAL-TIME PROTECTION

One of the features of CASB platforms SaaS security capabilities is the use of webhooks for near real-time remediation. For instance, if a user inadvertently shares sensitive healthcare data using a public link, CASB platforms can automatically disable the link if it violates the organization's internal sharing policy. This level of automation not only enhances security but also reduces the administrative burden on IT staff.

OUT-OF-BAND VISIBILITY AND DATA DISCOVERY

Beyond immediate threat mitigation, CASB platforms should offer visibility into the historical use of SaaS applications, including data discovery, file exposure, and file paths. This out-of-band visibility is invaluable for healthcare organizations, enabling them to conduct thorough audits of their SaaS application usage and ensure compliance with healthcare data protection regulations.

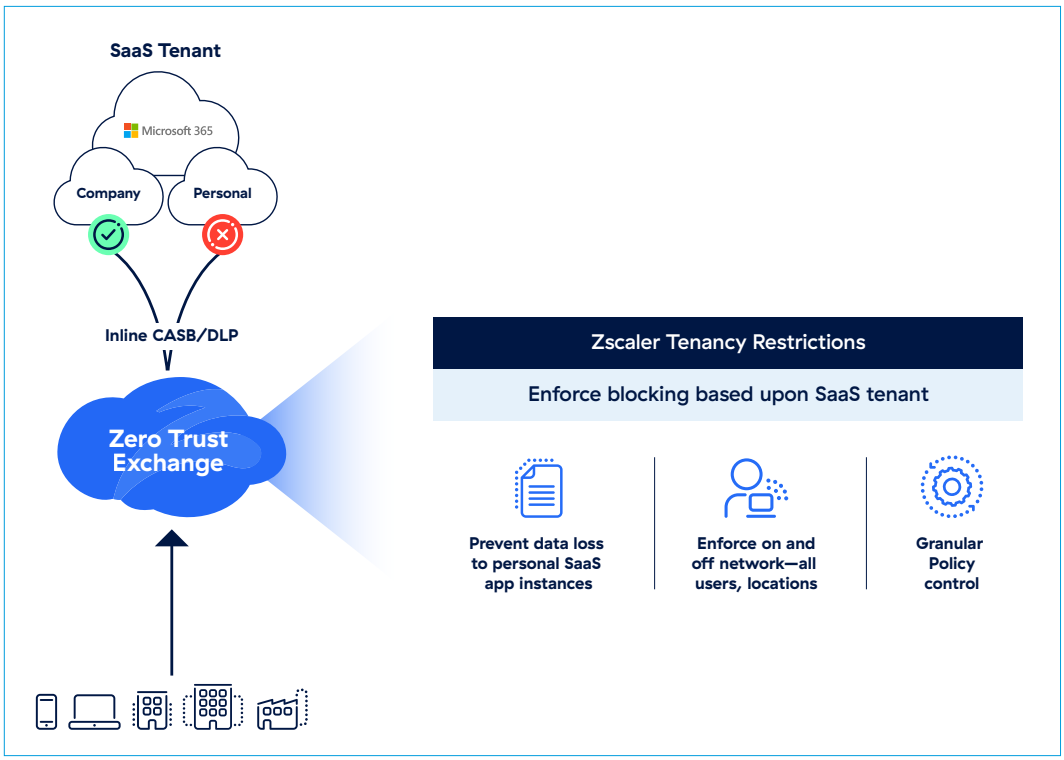
For example, an out-of-band analysis might reveal that historical patient information stored in Amazon S3 was inadvertently exposed due to misconfigured permissions. With this insight, healthcare IT administrators can take corrective action, adjusting permissions and policies as needed to prevent future exposures.

Tenancy Restrictions

Tenancy restrictions are designed to enforce strict data isolation in multi-tenant cloud environments. By controlling data access and sharing at a granular level, healthcare organizations can prevent unauthorized data exposure, ensuring compliance with regulations like HIPAA and GDPR. This is crucial in scenarios where different departments within an organization manage highly sensitive data that must remain compartmentalized, such as research data from clinical trials and patient health records.

Implementing Tenancy Restrictions

Implementing tenancy restrictions involves configuring policies that define who can access what data and under what circumstances. This ensures that, for example, users cannot inadvertently or maliciously upload documents to another organization's OneDrive or access data from another department not related to their work.



SCENARIO: SEPARATING RESEARCH AND CLINICAL DEPARTMENTS

Consider a healthcare organization with distinct Research and Clinical departments, each handling sensitive data relevant to their operations. The Research department works on confidential clinical trials, generating data that must not be accessible to the Clinical department to maintain the integrity of the trials and protect patient confidentiality.

Policy Example 1: Restricting Cross-Department Data Access

- **Objective:** Ensure that research data cannot be accessed by or shared with the Clinical department.

- **Implementation:** Configure Zscaler policies to identify and segregate traffic based on departmental identifiers. Utilize Zscaler's DLP capabilities to detect and block attempts to transfer research data into the Clinical department's network segment or cloud storage spaces.

Policy Example 2: Controlling External Sharing

- **Objective:** Prevent unauthorized external sharing of sensitive documents from the Research department.

- **Implementation:** Set up tenancy restrictions within Zscaler to block the creation of public sharing links for documents stored in cloud storage solutions used by the Research department. Allow exceptions only when explicitly authorized by policy, ensuring all sharing activities are logged and auditable.

Policy Example 3: Granular Access Based on Tenancy

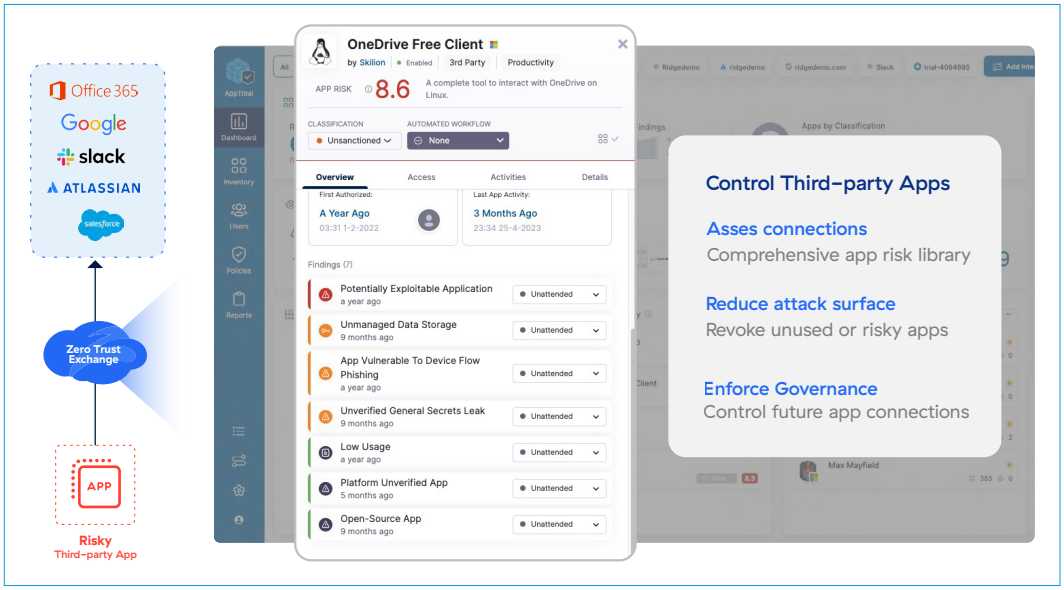
- **Objective:** Provide granular access control within multi-tenant applications based on user roles and data sensitivity.

- **Implementation:** Use Zscaler to enforce policies that grant access to specific data sets within a SaaS application based on the user's department and role. For instance, researchers may have access to anonymized patient data for analysis, while clinicians access detailed patient records for treatment purposes.

Third-Party Application Integrations

You will need a platform that also offers deep insights into third-party applications' security postures and their integration with your organization's network and data systems. In the context of an increasingly interconnected digital ecosystem, healthcare providers leverage numerous third-party applications for various functions ranging from patient care coordination to administrative tasks. While these applications can offer significant benefits in terms of functionality and efficiency, they also pose potential risks if not properly vetted and managed. Your zero trust platform should provide the ability for identifying, assessing, and mitigating the risks associated with these third-party applications.

Identifying Risky Third-Party Applications



The platform should utilize databases and real-time analysis to assess the risk level of third-party applications. It examines factors such as the application's compliance with data protection regulations, known vulnerabilities, data encryption standards, and the permissions it requires to operate. For healthcare providers, this means gaining visibility into which applications may pose a risk to sensitive patient data and overall network security.

Your zero trust platform should provide the ability for identifying, assessing, and mitigating the risks associated with integrated third-party applications.

Revoking Access for Integrations

One of the capabilities that is crucial when it comes to managing third-party applications is the ability to not only identify risky third-party applications but also facilitate the revocation of access for such applications. This is particularly useful when an application is found to be non-compliant with healthcare regulations like HIPAA, exhibits abnormal behavior indicative of a compromised state, or requests more permissions than necessary for its function, potentially exposing sensitive data.

POLICY EXAMPLES

Policy for Third-Party Application Assessment

Objective: Ensure all third-party applications integrated into the healthcare provider's systems are assessed for security and compliance risks.

Policy description: All third-party applications must undergo a risk assessment through the security team before integration. Applications must meet predefined criteria related to data security, privacy compliance, and minimum necessary permissions.

Enforcement steps:

1. Before integration, the application should be evaluated using third-party databases or internal to the organization databases on risk scores to identify potential risks.

2. Applications failing to meet the security criteria (e.g., mandatory multifactor authentication) are either rejected or flagged for further review.

3. Periodic reassessments are conducted to ensure ongoing compliance.

Policy for Revoking Access to Non-Compliant Applications

Objective: Maintain the integrity and security of the healthcare provider's data by revoking access to third-party applications that fail to comply with data protection standards.

Policy description: Your platform should monitor third-party applications for compliance with healthcare data protection standards. Access for non-compliant applications is revoked automatically, with exceptions subject to a rigorous review process.

Enforcement steps:

1. Continuous monitoring of third-party applications using your zero trust platform.

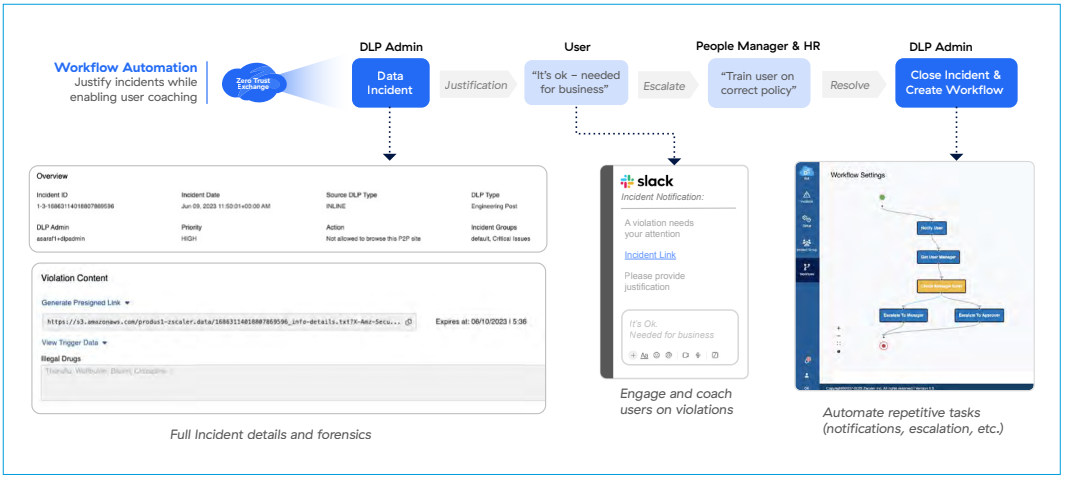
2. Automatic revocation of access for applications found to be non-compliant or posing security risks.

3. Implementation of a review process for applications that are essential for operations but flagged for potential risks, ensuring that necessary security measures are taken before reinstating access.

Policies enable you to easily and efficiently set and perform automatic actions such as classifying an app as sanctioned or unsanctioned, or take automated action such as revoke, ban, or review.

Incident Triage

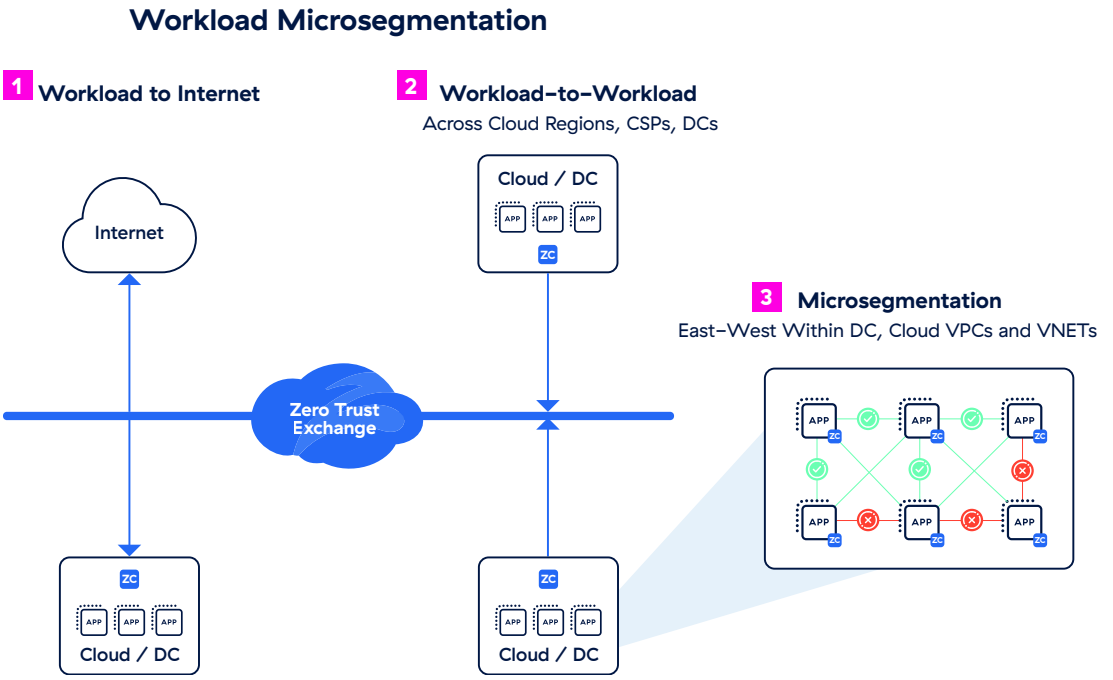
Incident triage and alerting are critical components of a robust DLP strategy, especially for healthcare providers who manage highly sensitive data. Efficiently identifying, categorizing, and responding to potential data exfiltration attempts are vital to maintaining the integrity and confidentiality of patient information and ensuring compliance with healthcare regulations like HIPAA. End–to–End Incident Workflow significantly simplifies this process, enhancing the maturity of DLP programs by reducing operational complexity and minimizing false positives.



CHAPTER 4

Secure Workloads

Securing workloads is a critical phase in implementing a zero trust architecture within a healthcare environment, especially after securing user access and data. Workloads include servers, containers, virtual machines, and cloud-based applications that often hold valuable data, making them prime targets for attackers. By applying zero trust principles, we can ensure that each workload is authenticated, authorized, and continuously monitored before being allowed to communicate within the network, thereby reducing the overall attack surface. In modern healthcare settings that span on-premises, hybrid, and multi cloud environments, traditional perimeter-based security models are no longer sufficient, making zero trust essential for protecting workloads.



Zero Trust Workload Communications

To secure workload communications in line with zero trust principles, whether on-premises or in the cloud, the following strategies should be implemented:

1. **Identity and access management (IAM):**
   Ensure all entities (users, services, and devices) attempting to access a workload are verified using strong identity controls, such as multifactor authentication (MFA) and identity providers (IdP). For instance, workloads should authenticate using service accounts, certificates, or OAuth tokens, ensuring only authorized entities gain access.

2. **Microsegmentation:**
   Divide your workload environment into smaller, secure segments based on the function and sensitivity of each workload. Microsegmentation restricts lateral movement within the network, confining any potential breaches to isolated segments, significantly reducing the impact of a threat.

3. **Least-privileged access:**
   Implement least-privileged access policies for workloads, ensuring they can only communicate with the resources necessary for their specific functions. This limits both internal and external access, preventing unauthorized interactions or data exposure.

Examples of Zero Trust for Workload Communications

WORKLOAD COMMUNICATIONS TO THE INTERNET

Scenario: A healthcare application hosted in the cloud requires access to an external API for updates.

Zero trust implementation:

- **Identity verification:** The cloud application must authenticate using securely stored credentials like API keys or OAuth tokens before accessing the external API, ensuring only authorized requests are processed.

- **Microsegmentation:** Segment the cloud environment so that only this application can reach the necessary internet resources, while other workloads remain isolated from external access.

- **Least-privileged access:** Restrict outbound access to only the required API endpoints, blocking all other internet traffic.

INTER-WORKLOAD COMMUNICATION

Scenario: An on-premises electronic health records (EHR) system needs to communicate with a cloud-based billing application but should be restricted from accessing any non-essential services.

Zero trust implementation:

- **Application whitelisting:** Define policies that allow only the EHR system to communicate with the billing application while blocking access to all other external services.
- **Microsegmentation:** Segment the EHR workload from the rest of the network, ensuring it can only interact with the billing application, minimizing the potential attack surface.
- **Continuous monitoring:** Employ real-time monitoring to track the EHR system's activity, quickly detecting and responding to any unauthorized attempts to access other systems.

Workload Segmentation Strategies

Segmenting workload traffic is vital for implementing zero trust principles, preventing unauthorized lateral movement within your environment:

1. **Identify and classify workloads:** Begin by identifying all workloads and classifying them based on their function, sensitivity, and communication requirements. For example, categorize workloads into groups such as patient management, billing, and internal communications within a healthcare provider's network.
2. **Define segmentation policies:** Create segmentation policies based on least privilege, specifying which workloads can communicate with each other. These policies should ensure that each workload only has access to the resources required for its function.

3. **Enforce encrypted communications:** All communication between workloads should be encrypted using SSL/TLS, ensuring data integrity and confidentiality. Apply SSL inspection and content filtering to prevent data leaks and protect against potential threats.

Secure Workloads in Cloud and On-Premises Environments

Cloud-Based Workloads

- Use cloud native controls, such as security groups or virtual private clouds (VPCs), to enforce zero trust principles by restricting access to only authorized workloads.
- Implement microsegmentation within the cloud environment to separate workloads based on their purpose and data sensitivity.

On-Premises Workloads

- Apply network segmentation using VLANs, firewalls, or software-defined networking (SDN) to control traffic between workloads.
- Use agent-based or agentless forwarding mechanisms, as discussed previously, to ensure all workload traffic is routed through a central zero trust enforcement point for inspection.

Enhancing Workload Security with Traffic Forwarding Mechanisms

To achieve effective zero trust for workloads, you must use traffic forwarding mechanisms (e.g., GRE tunnels, IPsec tunnels, or agentless forwarders) to route all workload traffic to a central enforcement point for inspection. This ensures that every communication between workloads or between workloads and the internet adheres to zero trust principles.

Best Practices for Zero Trust Workload Segmentation

1. **Continuous monitoring and logging:** Implement continuous monitoring and logging for all workload communications to identify and respond to unauthorized access attempts or suspicious behavior promptly.

2. **Dynamic policy adjustments:** Regularly review and adjust segmentation policies based on changes in the network environment, emerging security threats, or operational requirements to maintain an up-to-date zero trust posture.

3. **User and device context integration:** Incorporate user and device context into workload access policies by integrating with identity and access management solutions. This allows for more refined access controls based on the user's role and the device's security posture.

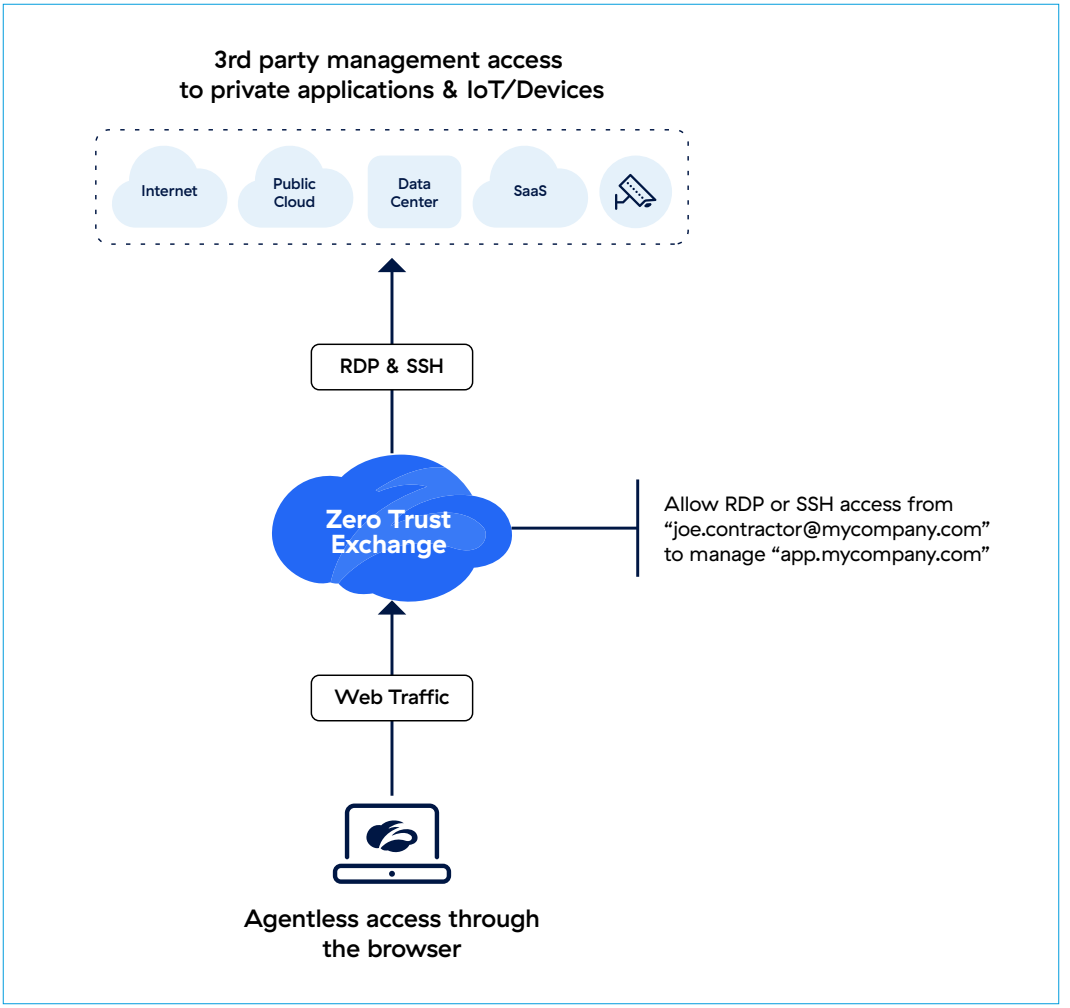
By following these zero trust principles and leveraging traffic forwarding mechanisms, healthcare organizations can ensure that their workloads are protected from internal and external threats, regardless of where they reside—whether on-premises or in the cloud.

CHAPTER 5

Secure B2B

The final step to a Zero Trust Hospital is Implementing a zero trust architecture for Business–to–Business (B2B). B2B relationships often necessitate sharing between organizations (ex. data or applications), this does not mean that a shared network is needed to facilitate this collaboration. Historically, a shared network will either be something like an Application VPN, VDI solutions, or full network VPN access. A zero trust model should ensure rigorous verification and continuous monitoring of all access requests, significantly reducing the risk of data breaches and cyberattacks that could compromise both parties.

Securing Vendor Access



1. **Clientless access:** A vendor management system should secure clientless access for vendors to an organization's network and applications. This approach eliminates the need for installing specialized software on the vendor's devices, reducing complexity and potential security vulnerabilities associated with software clients.

2. **Timed access:** Administrators can grant vendors timed access to systems, ensuring that access is available only for the duration necessary to complete a specific task or project. This minimizes the window of opportunity for potential security breaches.

3. **On-demand access:** On-demand access allows organizations to grant access permissions dynamically, based on the immediate needs of the vendor. This ensures that vendors have access only when necessary, enhancing security and control.

4. **Session recording:** For critical systems or sensitive operations, enable session recording, allowing administrators to review vendor activities for compliance, auditing, and forensic purposes. This is particularly important in healthcare, where accessing patient data and systems requires strict oversight.

5. **Credential management:** Your tool of choice should be able to have a store for credentials that the security team can control, audit, and enforce granular permissions upon. This can also improve experience for the vendor by allowing things such as "credential vaulting" which allows an admin to assign specific privileges/accounts to a particular shared system.

6. **The vendor management system** should support multiple protocols including remote desktop protocol (RDP), secure shell (SSH), , and virtual network computing (VNC), providing flexibility in how vendors connect to and interact with different systems.

Specific Policy Examples

POLICY FOR TIMED ACCESS TO PATIENT DATA SYSTEMS

Objective: To allow vendors temporary access to patient data systems for maintenance purposes while ensuring compliance with healthcare regulations.

Policy:

- Vendors are granted access to the specified patient data system only for the duration of the maintenance window, as predefined by the agreement.
- Access is automatically revoked upon the expiration of the access period.
- All sessions are recorded and monitored for unusual activity.

POLICY FOR ON-DEMAND ACCESS FOR EMERGENCY SUPPORT

Objective: To provide vendors with on-demand access for emergency technical support, ensuring minimal disruption to healthcare services.

Policy:

- On-demand access requests must be approved by a designated administrator before access is granted.
- Access is limited to the specific systems or components requiring support, and all activities are recorded for auditing purposes.
- Access permissions expire automatically once the support issue is resolved or after a predefined time limit.

POLICY FOR SESSION RECORDING FOR COMPLIANCE AUDITING

Objective: To maintain a record of all vendor activities within the network for compliance with healthcare regulations and internal auditing.

Policy:

- All vendor sessions involving access to systems that process or store sensitive patient data are recorded.
- Recorded sessions are stored securely and are subject to regular review by the compliance team.
- Unauthorized actions detected during session review trigger an immediate security investigation.

CHAPTER 6

Monitoring and Troubleshooting

Cybersecurity and user experience are often seen as being at odds, with security measures perceived as slowing down systems or disrupting workflow. This perception can be especially challenging when implementing zero trust projects, where the focus on robust security may lead users to blame new security tools for sluggish performance or application issues. It is crucial to address these frustrations proactively to prevent a stigma around zero trust and other security initiatives. A dynamic, business-aligned approach is essential—especially in sectors like healthcare, where application performance impacts patient care.

Organizations should implement security solutions that not only protect but also enhance user experience. By adopting agile solutions tailored to modern digital demands, such as SaaS platforms and telehealth applications, businesses can support zero trust initiatives while maintaining operational efficiency. Tools that offer real-time insights into areas for experience optimization and root causes of work degradation can help balance security and usability. Building a resilient security culture requires more than just training—it also demands continuous refinement of both security measures and the user experience to keep employees engaged and vigilant.

This balanced, agile approach enables organizations to drive successful zero trust projects forward, integrating business-based policies that ensure both security and productivity. By fostering a security culture that also prioritizes user satisfaction, organizations can create an environment where security enhances, rather than hinders, everyday operations.

Digital Experience Score

In order to understand user experience, we must first baseline and accurately track employee experience. We need a quantifiable metric that reflects the overall digital experience of each user within an organization, we will call that a DEX (Digital Experience Score). This score gathers and analyzes data from application performance, network conditions, and device health to provide a comprehensive view of what each user is experiencing. This score is pivotal in identifying and diagnosing the root causes of issues, enabling faster resolution and optimizing user satisfaction.

Other Key Features and Capabilities

- **Self-help feature:** DEX products should enable end-users to troubleshoot issues on their own, reducing the workload on IT teams and improving user satisfaction by minimizing disruptions.

- **CloudPath and web probes:** These probes are used to monitor the performance of SaaS and web applications. CloudPath probes provide insights into the health and performance of cloud-based applications at each hop along the network path. Web probes monitor the performance of web services. This dual approach ensures comprehensive coverage of all external services critical to healthcare operations, including telehealth platforms.

- **Proactive webhooks:** DEX products can send timely alerts through email, IM, or tools like PagerDuty when user experience degrades, enabling proactive issue resolution before they impact critical healthcare services.

- **UCaaS monitoring capabilities:** With a significant portion of healthcare communications relying on unified communications as a service (UCaaS) platforms like Microsoft Teams and Zoom, a DEX's ability to monitor these platforms ensures high-quality virtual consultations and internal communications. It provides granular user and application telemetry data, helping IT teams detect and resolve sources of latency and packet loss that may impact the digital experience.

66%

of companies invested in Digital Experience Monitoring to achieve their zero trust goals **(TechTarget)**

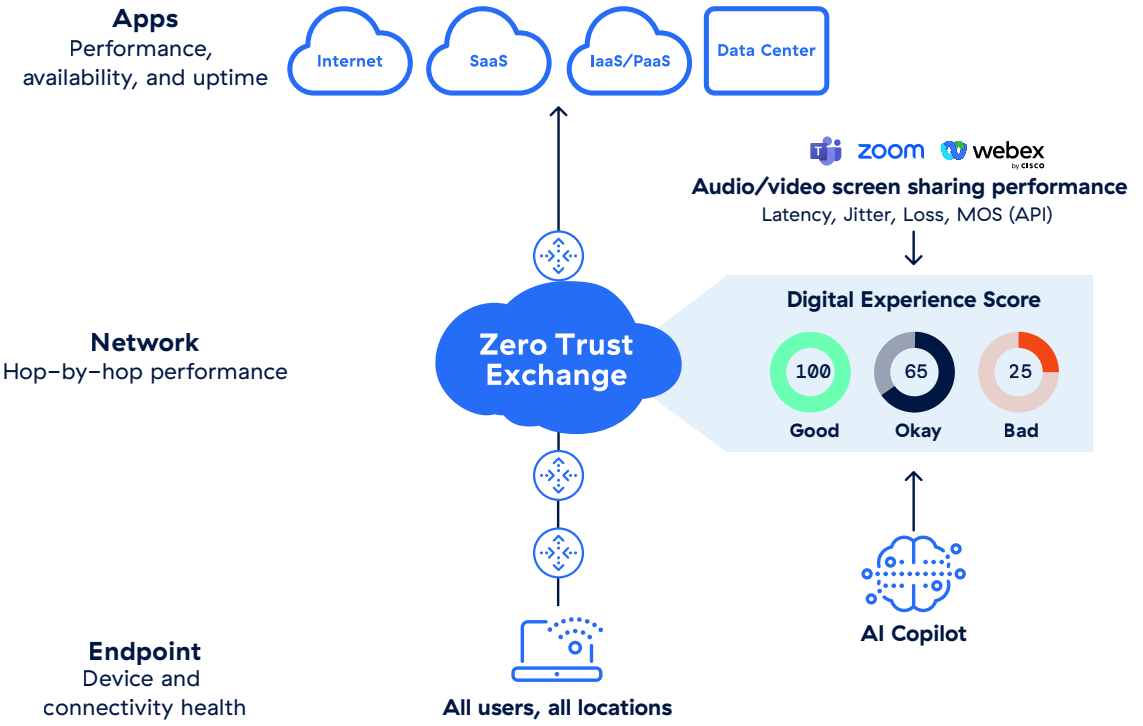
74%

of companies have at least one significant outage per quarter **(Enterprise Management Associates)**

91%

of employees say they're frustrated with their work software **(Freshworks)**

Visibility from Endpoint to App



CHAPTER 7

Endpoint Security

In the zero trust model, all network traffic, including traffic from internal devices, is untrusted by default. This approach is particularly relevant to healthcare organizations, where endpoints are scattered across various locations and networks, from hospital rooms to doctors' offices and even patients' homes. As such, endpoint security is critical for enforcing zero trust principles at the device level.

Endpoint security solutions involve a combination of technologies designed to protect individual devices from cyberthreats. These may include antivirus software, endpoint detection and response (EDR) tools, mobile device management (MDM), and data encryption. By continuously monitoring and enforcing security policies on each device, endpoint security helps healthcare providers ensure that only authorized users and devices can access their networks and sensitive patient data.

Least-Privileged Access and Continuous Verification

A cornerstone of the zero trust model is the principle of **least-privileged access**, which mandates that users and devices are granted only the minimum level of access required to perform their duties. In a healthcare environment, this ensures that a nurse, for instance, has access to patient records only for the departments they work in and not for the entire hospital. Endpoint security plays a key role in enforcing these access controls by ensuring that only trusted devices can connect to the network, and that these devices are subject to ongoing verification.

For example, if a healthcare worker attempts to log in to the electronic health record (EHR) system from an endpoint that hasn't been registered or doesn't comply with security policies (e.g., outdated antivirus software or missing security patches), the system can deny access or trigger further authentication measures. This continuous verification is crucial in preventing unauthorized access, particularly in a healthcare setting where patient data is extremely sensitive and regulated.

The zero trust framework emphasizes the need to authenticate and verify every access request, regardless of where the user is located. Endpoint security solutions that incorporate remote access controls, such as multifactor authentication (MFA) and device compliance checks, enable healthcare organizations to extend zero trust protections to remote workers.

For instance, a doctor accessing patient records from a personal device at home would be subject to the same rigorous security checks as they would be within the hospital's network. The endpoint security solution would ensure that the device meets all security requirements—such as encryption, antivirus protection, and proper configuration—before allowing access to any sensitive data.

Securing Medical Devices

Healthcare providers must also contend with a growing number of connected medical devices, such as heart monitors, infusion pumps, and imaging equipment that are often part of the internet of medical things (IoMT). These devices are increasingly targeted by cybercriminals due to their critical role in patient care and the sensitive data they handle. Unfortunately, many medical devices lack robust built-in security features, making them vulnerable to attacks.

Endpoint security solutions, particularly those that incorporate internet of things (IoT) security capabilities, are essential in securing these devices within a zero trust framework. By continuously monitoring the behavior of medical devices and ensuring that they are not communicating with unauthorized networks or systems, endpoint security can help healthcare providers maintain the integrity of their medical devices. If a medical device starts acting abnormally—such as transmitting data to an unknown IP address or initiating unusual network connections—the security solution can isolate the device from the network, preventing a potential breach. In the ideal end state, these medical devices are given a least-privileged access profile so they can only access what they need to access to perform their duties.

85% of healthcare providers use IoMT devices to support patient engagement and monitoring. (Source: Deloitte)

Compliance with HIPAA and Other Regulations

The healthcare sector is highly regulated, with strict standards for the protection of patient data. Endpoint security solutions play a critical role in ensuring compliance with regulations such as HIPAA, which requires healthcare providers to implement administrative, physical, and technical safeguards to protect electronic protected health information (ePHI).

HIPAA mandates that organizations must protect against reasonably anticipated threats to patient data, including ensuring that devices accessing ePHI are secure. Endpoint security solutions provide healthcare organizations with the tools needed to comply with these regulations by offering encryption, monitoring, and access controls that protect ePHI from unauthorized access or tampering. For example, encryption ensures that even if an endpoint is lost or stolen, the data on the device remains inaccessible to unauthorized users. Additionally, audit logs generated by endpoint security solutions help healthcare organizations track access to ePHI, enabling them to detect potential breaches and respond quickly.

CHAPTER 8

Security and Event Management

SIEM systems collect, analyze, and correlate logs from various sources across an organization's IT infrastructure. They provide real-time alerts, dashboards, and reports on potential security threats. This visibility is essential for maintaining zero trust principles, which emphasize continuous monitoring and never assuming trust, even for internal users. Healthcare providers, with their complex IT environments consisting of EHR systems, connected medical devices, and administrative platforms, rely on SIEM to achieve a cohesive security strategy.

One of the core principles of zero trust is continuous verification. Unlike traditional perimeter-based security, where users inside the network are implicitly trusted, zero trust demands that every access request is verified, regardless of the user's location. SIEM supports this by offering real-time visibility into user activities and potential threats.

Enforcing Compliance and Protecting Patient Data

Healthcare providers are subject to rigorous regulations like HIPAA, which mandates strict controls over the handling and access to protected health information (PHI). Under HIPAA, organizations must implement safeguards to ensure the confidentiality, integrity, and availability of patient data. SIEM systems play a vital role in helping healthcare organizations meet these compliance requirements by continuously monitoring and logging access to sensitive data, providing audit trails, and ensuring that any deviations from security policies are immediately detected and addressed.

In 2023, there were more than 133 million records exposed or disclosed in 725 reported data breaches. This was a record-breaking number of breaches and exposed records.
(Source: The HIPAA Journal)

For instance, healthcare organizations often deal with role-based access control (RBAC), where different roles, such as doctors, nurses, and administrative staff, have different levels of access to patient data. A SIEM solution can ensure that access control policies are enforced consistently across the organization. If a hospital employee attempts to access information outside of their permission level, such as a billing department worker attempting to view clinical records, the SIEM system will detect this violation and generate an alert for investigation.

Correlation of Data for Enhanced Security Insights

The NIST zero trust framework stresses the importance of continuous monitoring and adaptive policies, which can be bolstered by SIEM's ability to correlate data from diverse sources. In a healthcare context, this might involve logs from various medical devices, endpoints, cloud services, and on-premises applications. SIEM analyzes and correlates this data to detect patterns that might indicate a security threat.

For example, a SIEM solution could correlate login data from a remote access system with data from an internal EHR system and discover that an external attacker has compromised an account. If an employee logs into the hospital's network from one geographic location but then attempts to access sensitive EHR data from another distant location in a short period, this inconsistency would be flagged. SIEM could integrate this information with data from threat intelligence feeds, potentially revealing that the remote login originates from a known malicious IP address. This type of threat correlation allows healthcare providers to quickly identify and mitigate security risks, protecting critical patient data.

Insider threats are a growing concern in healthcare environments, where employees may misuse their access to patient data either for financial gain or out of negligence. SIEM is particularly effective at detecting these insider threats by monitoring behavior patterns across systems. Getting to least-privileged access is a journey and a marathon not a sprint; therefore you may not be quite at the point where everyone is only accessing exactly what applications they should be accessing in a zero trust framework. For instance, if a hospital employee who typically only accesses patient billing information suddenly starts accessing detailed medical records across various departments, this deviation from their normal behavior would trigger an alert due to them not being authorized to access that information.

Another example could involve a physician using their credentials to access an unusual number of patient records in a short timeframe. This activity could be a sign of data harvesting, where an insider is collecting patient data for unauthorized use. By leveraging SIEM, healthcare providers can quickly detect these anomalies, reducing the risk of data breaches and ensuring compliance with regulatory standards.

Incident Response and Automation

SIEM also plays a critical role in incident response, particularly in zero trust environments where every action must be scrutinized. Once a threat is identified, SIEM can automatically initiate predefined workflows to respond to the incident. For example, if a SIEM system detects that a user account has been compromised, it can automatically disable the account, block the user from accessing sensitive systems, and alert the security team to investigate further.

Moreover, SIEM solutions can integrate with security orchestration, automation, and response (SOAR) tools to streamline the response process. For healthcare providers, where speed is of the essence, automating incident response can significantly reduce the time it takes to mitigate security incidents, thereby minimizing potential harm to patient data and clinical operations.

CHAPTER 9

Conclusion

As we close the final chapter of our journey of achieving the Zero Trust Hospital, it's crucial to reflect on the landscape that has shaped the need for a paradigm shift in how we approach cybersecurity, particularly in the healthcare sector. The rise of cyberthreats, sophisticated attack vectors, and the increasing value of healthcare data have made traditional security models obsolete. It is of critical importance to healthcare providers to adopt a new way of thinking.

At the heart of the zero trust model is the principle that no entity, whether inside or outside the network, should be automatically trusted. This concept has become increasingly relevant as healthcare providers face a surge in cyberthreats, from ransomware attacks to data breaches, endangering patient data and healthcare operations. Zero trust addresses these challenges by ensuring rigorous verification and minimizing the attack surface.

The foundation of zero trust security is protecting user identities and their context. This involves comprehensive internet access controls, utilizing proxy architecture for both managed and unmanaged devices, and applying conditional access based on network conditions. Key components like DNS (security), firewall rules, SSL inspection, URL filtering, and cloud application specific controls are essential, along with advanced threat protection mechanisms such as sandboxing and isolation to guard against sophisticated threats.

Zero trust extends beyond user protection to application access and branch connectivity. It emphasizes secure, direct-to-application connections, regardless of the application's location, be it on-premises or in the cloud. This approach is complemented by deception techniques and identity threat detection and response (ITDR) to enhance security. In the realm of branch connectivity, the classification of IoT and IoMT devices and tailored internet and application policies play crucial roles in securing healthcare networks.

A critical aspect of zero trust in healthcare is preventing data loss across both managed and unmanaged devices. Inline data loss prevention (DLP) and endpoint DLP, coupled with comprehensive policy rules, tenancy restrictions, and out-of-band (OOB) CASB strategies, ensure sensitive data, especially patient information, is safeguarded.

Securing workloads involves restricting internet access based on policies and segmenting applications to prevent unauthorized interactions. Cloud applications in particular require stringent controls to ensure secure communication. In B2B scenarios zero trust facilitates secure portals and privilege–remote access (PRA), offering timed access, session recording, and on–demand access, thereby enhancing the security of inter–organizational interactions.

The journey towards a zero trust architecture is both necessary and complex, especially for healthcare providers navigating an ever–evolving cyberthreat landscape. By adopting a zero trust model, healthcare organizations can significantly enhance their security posture, protect sensitive patient data, and maintain the integrity of their healthcare delivery systems.

For More Information

Congratulations on becoming well-armed with the knowledge necessary to drive a successful digital transformation to the Zero Trust Hospital. The need, benefits, and process for migrating to the cloud and implementing zero trust security are well established. The obstacles, challenges, and objections for doing so are known and navigable. All that remains is to put this newfound knowledge into action.

The following resources are available for additional assistance:

Zero Trust Hospital: The CXO Vision

Seven Elements of Highly Successful Zero Trust Architecture

Zscaler.com/healthcare

Zscaler, creator of the Zero Trust Exchange platform, uses the largest security cloud on the planet to make doing business and navigating change a simpler, faster, and more productive experience.

About the Authors

Steven Z. Hajny (Zscaler Healthcare Technology Evangelist & Principal Solutions Engineer), Ryan Ulrick (Zscaler Principal Product Manager), Dave Steinke (Zscaler Transformation Architect), and Derek Brodeur (Zscaler Sales Engineering Manager) bring extensive expertise and diverse perspectives to the realm of cybersecurity. With extensive backgrounds in companies such as VMware, Forescout Technologies, Dell, MITRE, and CDW, their combined experience spans over two decades in the industry. Their combined knowledge and dedication make them key influencers in the ever-evolving landscape of cloud security, collectively driving innovation and excellence in zero trust to advance secure digital transformations in healthcare.

Reimagining healthcare cybersecurity for the digital age

Our groundbreaking Zero Trust Hospital books offer comprehensive guidance for zero trust security in healthcare institutions. We've designed these resources to help you safeguard sensitive patient data, navigate the complexities of regulatory compliance, and protect your organization from evolving cyberthreats.

Dive into our expert insights, practical strategies, and real-world case studies to transform your hospital into a more secure, resilient, and trusted healthcare provider. This book provides targeted insights and actionable strategies tailored to the unique needs of Architects.