zscaler™

Healthcare Solutions

# Zero Trust Hospital

## The CXO Vision


**AUTHORS**

Tamer Baker
David Anderson

**FOREWORD BY**

Cris Ross

# Zero Trust Hospital

## The CXO Vision

**AUTHORS**
Tamer Baker
David Anderson
Foreword by Cris Ross

Published February, 2025
First Edition
ISBN Number: 979-8-9924738-0-3

# What industry leaders are saying about *Zero Trust Hospital: The CXO Vision*

"Cybersecurity in healthcare is not a challenge CISOs can face alone. *Zero Trust Hospital: The CXO Vision* lays out an understandable and actionable starting point to bring an organization together through a zero trust transformation. CISOs should not only read this book to structure their own thoughts but also share it with fellow CXOs who will be partners on this journey. Through the resulting partnership and understanding, hospital CISOs can start to bring control to what often feels like an uncontrollable problem."

***Nate Couture, Network AVP – CISO, The University of Vermont Health Network***

"While zero trust might be a difficult task to accomplish in a hospital environment, this book provides a very methodical approach to understanding and applying the concepts within the enterprise. Knowing what decisions have been made around the technical stack that have an impact on a proper zero trust implementation is foundational and this book helps to bring to light these points and topics that are critical between a successful and less than successful implementation."

***Christian AbouJaoude, Associate CIO & CTO, Keck Medicine of USC***

"Regardless of industry and organizational size, any zero trust transformation must start small and grow incrementally to achieve measurable success while meeting core objectives of the business. Kudos to the *Zero Trust Hospital: The CXO Vision* for bringing timely health sector awareness and education around the benefits of zero trust, its ability to shrink attack surface, improve identity management, and appropriately segment critical assets in what should become an imperative to safeguarding critical infrastructure healthcare."

***Carter Groome, CEO, First Health Advisory, CHIME Foundation Board Member***

"As organizations caring for people in their most vulnerable moments, we make an implicit contract—a commitment—not only to ensure the highest quality of care, but to deliver it with the confidence that everything shared with us remains secure. *Zero Trust Hospital: The CXO Vision* is an impeccable resource for all CXOs desiring to fulfill this promise."

***Edward Marx, CEO, Marx Advisory & Former Industry CIO***

"Digital transformation brings with it a lot of known and unknown risks — we need to do everything possible to insulate ourselves and our patients from that risk — zero trust isn't just a marketing phrase, it's a real strategy that can help us create better, faster, cheaper, SAFER, easier– to–access care for patients and families."

***Drex DeFord, President, This Week Health, Former Industry CIO***

# Table of Contents



# Foreword

Attacks by criminals, vandals, political actors, and nation-states are commonplace and in the common parlance. Attacks are becoming more frequent, more sophisticated, and more damaging. Theft of money, data, and IP is an ever-present threat. Executives of organizations large and small know that protecting against cyberattacks is an essential cost of doing business.

As healthcare organizations defend against cybercrime, they are also seeking to maintain the privacy of patient data while adopting more sophisticated digital services to improve care and provide a better patient experience. Privacy is regulated by law and is an ethical imperative.

How will our industry address these dual challenges? Zero trust is the modern framework for securing enterprises against cybercrime and protecting data privacy. The techniques we've used previously to defend against attacks and protect privacy were designed for a world of self-contained enterprises and are ineffective and cumbersome.

We have transitioned to a new world where most data and compute are in cloud and software-as-a-service environments, care is delivered by a combination of integrated and extended digital enterprises, and people continue to work from anywhere. If we were designing a security and privacy architecture from scratch for this new digital, extended enterprise world, it would start with zero trust.

This easy-to-digest book for healthcare technology and business leaders provides a clear and compelling overview of zero trust and a roadmap for how to get started and make a case for zero trust. For business leaders frustrated by the cost of defending against crime and vandalism, this book describes how zero trust has the promise to not only improve security but also to improve user experience.

The health seekers and patients of the future will have choices about where and how to receive advice and care. Everyone deserves to receive care from organizations that protect their data and their privacy. Increasingly, consumers of healthcare will also choose to receive care from organizations that are digitized and provide a great patient experience. Zero trust is the first step towards security and excellent service and will be a distinctive asset for leading organizations.

**Cris Ross**
Former CIO, Mayo Clinic

CHAPTER 1

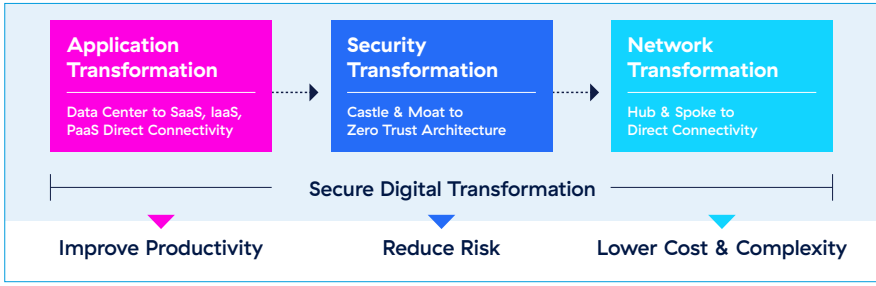
# Digital Transformation is Here

In the rapidly evolving digital landscape, the healthcare sector stands at a critical juncture. Cyberthreats are sophisticated, persistent, and growing in number, placing sensitive patient data and hospital operations at significant risk. The need for modernizing both infrastructure and your security framework has never been more pressing. This chapter, "Introduction to Transformation," aims to illuminate the pathway towards a zero trust architecture, essential for safeguarding modern hospitals.

Digital transformation is a heavily used term for an all-encompassing undertaking that affects the CXO role more than any other initiative. Wikipedia defines it as "the adoption of digital technology by an organization to digitize non-digital products, services, or operations. The goal for its implementation is to increase value through innovation, invention, customer experience, or efficiency."

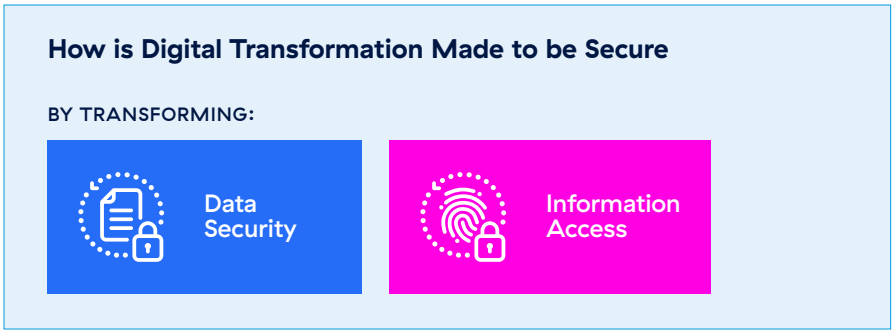
The COVID-19 pandemic accelerated the need for hospitals to transform to stay functional. So, while "transformation" has become a buzzword, organizations must stay competitive in a world where success is increasingly influenced by technology. Digital is the new word for "modern." At heart, a digital transformation is about connecting all the components of a health system: its patients, its suppliers, its clinicians & employees, and its physical assets, like modern medical devices. While bringing fantastic progress, this also embeds major new risks.

Transforming digitally must be done in a secure way, and this is difficult as cyber threats increase, clinicians become more mobile, and apps become distributed. It means that transformation needs to happen in several ways, including transforming application, network, and security architecture to cope with the modern trends in cloud and workforce mobility. This ultimately leads to improved productivity, reduced risk, and lower cost and complexity.



Specifically, the fundamental goal of network and security transformation is to address how data is secured and how information is accessed. This is where the zero trust architecture comes into play.

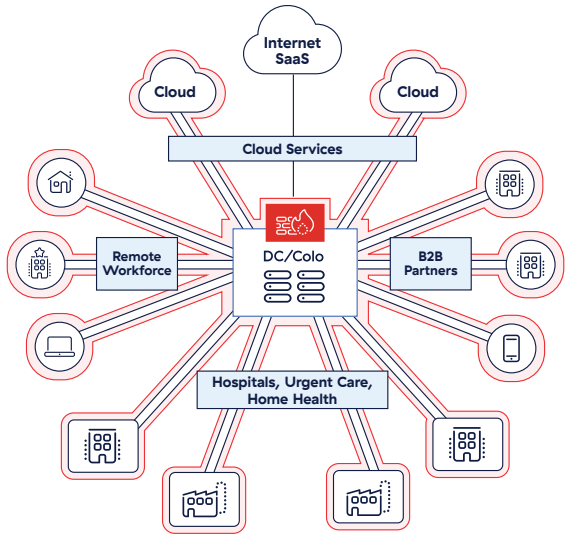
## Securing Digital Transformation




Adequately providing data security and secure information access is challenging for health systems today. Over the last 30 years, many hospitals have been building “hub-and-spoke networks” where every hospital, clinic, and branch is connected to the data center over a private network. They then deployed numerous and disparate security appliances or networking appliances, like routers, switches, and firewalls, to protect the data center where all the applications sat.

This model worked well when the data center was the center of gravity and employees & clinicians mostly worked in a hospital/clinic. However, application transformation has moved many applications to the cloud, where providers are embracing software as a service (SaaS) or moving/building applications in the public cloud like Microsoft Azure or Amazon Web Services (AWS). Sensitive data is now everywhere. Additionally, employees, clinicians and contractors in the post-pandemic workplace are working from everywhere. This change resulted in the architecture of hub-and-spoke networks (also called “castle-and-moat security”) jeopardizing data security and proper information access.

## Traditional Network and Firewall Architecture




A trusted private network connects everything

Secure the network with perimeter firewalls

Worked well in the past, but is now a liability

**Expensive, Security Risk, Poor Experience**

Legacy architectures do not provide an optimal user experience because they introduce unneeded latency and complicated routing to reach applications. Users should have direct access to applications for both efficiency of use and security, which requires a transition from a hub–and–spoke network to direct connectivity. Who likes to fly from San Francisco to New York via Houston, instead of flying direct and non–stop?

When this required cloud transformation is completed, security breaks because security remains in the data center. This necessitates security transformation—a move away from the castle–and–moat model based on firewalls and VPNs. Enter zero trust architecture (ZTA), which transforms both data security and information access.

The challenges caused by legacy network and security architectures are pervasive and long–standing, and require rethinking the way connectivity is granted in the modern world. This is where ZTA is leveraged—as an architecture where no user or application is trusted by default.

Zero trust is based on least privileged access, which ensures that trust is only granted once identity and context are verified, and policy checks are enforced. The US National Institute of Standards and Technology (NIST) defines the underlying principle of a zero trust architecture as "no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)" (NIST Special Publication 800–207). It's an overhaul of the old proverb "Never trust. Always verify."

This approach treats all network communications as hostile, where communications between users and workloads or among workloads are blocked until identity–based policies validate them. It ensures that inappropriate access and lateral movement are prevented. This validation carries across any network environment, where the network location of an entity is no longer a factor and not reliant on rigid network segmentation.

## Why Healthcare Needs to Transform Now

Let's dig a little bit deeper into why, after spending millions of dollars on network and cybersecurity, healthcare providers still have major security risks and experience breaches. The main problem is the IP–based networking architecture designed in the late eighties created an ever expanding corporate network where users and applications were all interconnected. Companies like Cisco built great routers and switches so an enterprise could extend its data center to every hospital, clinic, branch, etc.

In this networking model, if an employee was granted access to the network, he or she could move laterally and access these data center–hosted applications. This happens because the network is routable. Users and applications occupy the same network. This represented a big breakthrough for networking and distributed computing. Unfortunately, this approach cannot adapt to the world we live in today.

As the need arose for people to work remotely, remote access virtual private networks (VPNs) extended the network to every household. Employees working from home or on the road could access the network from anywhere and move laterally to access applications. The VPN makes it appear as if the employee/clinician is in the office while sitting at home, in Moscow, or wherever they may be. If there are 50,000 users, the VPN extends the network to 50,000 households.

Couple this predicament with the embrace of the public cloud. Because users and applications must be on the same network, there is now an extension of the network to every cloud region.

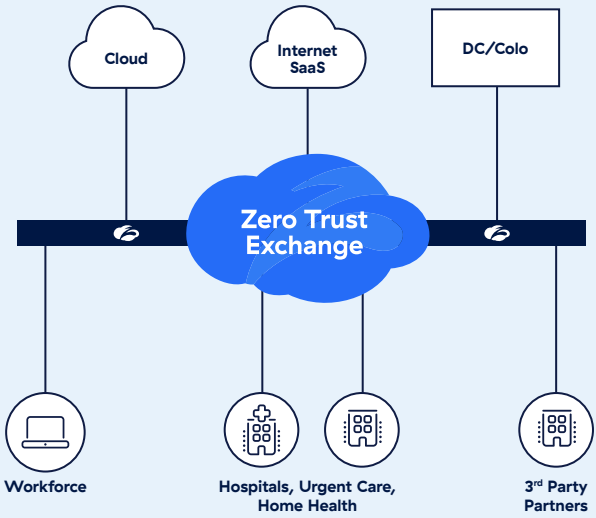
To mitigate some of these challenges, and since physical security appliances don't work well in cloud environments, organizations began to spin up virtual firewalls and virtual private networks (VPNs) in the cloud, deeming it cloud security. It is not. A firewall is still an IP device, even in the cloud. A VPN is still an IP device, even in the cloud.

Wherever those virtual instances are spun, the corporate network gets extended to those locations. As it starts growing, it turns into a big, flat network that can and will create headaches as it enables lateral movement for users as well as for attackers.

## Zero Trust Architecture

Zero trust is not merely a buzzword; it is a paradigm shift in how we think about security. It operates on the premise that threats can come from both outside and within the network. Therefore no entity, whether human or machine, should be trusted by default. Every access request must be verified, authenticated, and authorized based on stringent policies. Zero trust is a framework based on a least privileged security model — a framework of multiple products and solutions working together. There are many misconceptions about zero trust — namely that it's disruptive to patient care, difficult and takes years to deploy, expensive, and offers a poor user experience. These myths will all be dispelled throughout this book.

**Zscaler Vision: Reimagining a New Architecture for Networking and Security**




An exchange/a switchboard to connect user, devices, and workloads using business policies over any network

**Lower TCO, Superior Security, Great Experience**

## Why Switch to Zero Trust Now?

IT leaders started doing application transformation to the cloud by lifting and shifting the applications. Then they realized that this did not give them many productivity benefits. Now they are building cloud native applications using Platform–as–a–Service (PaaS) platforms that provide many productivity functions and tools.

## Embracing New Technologies

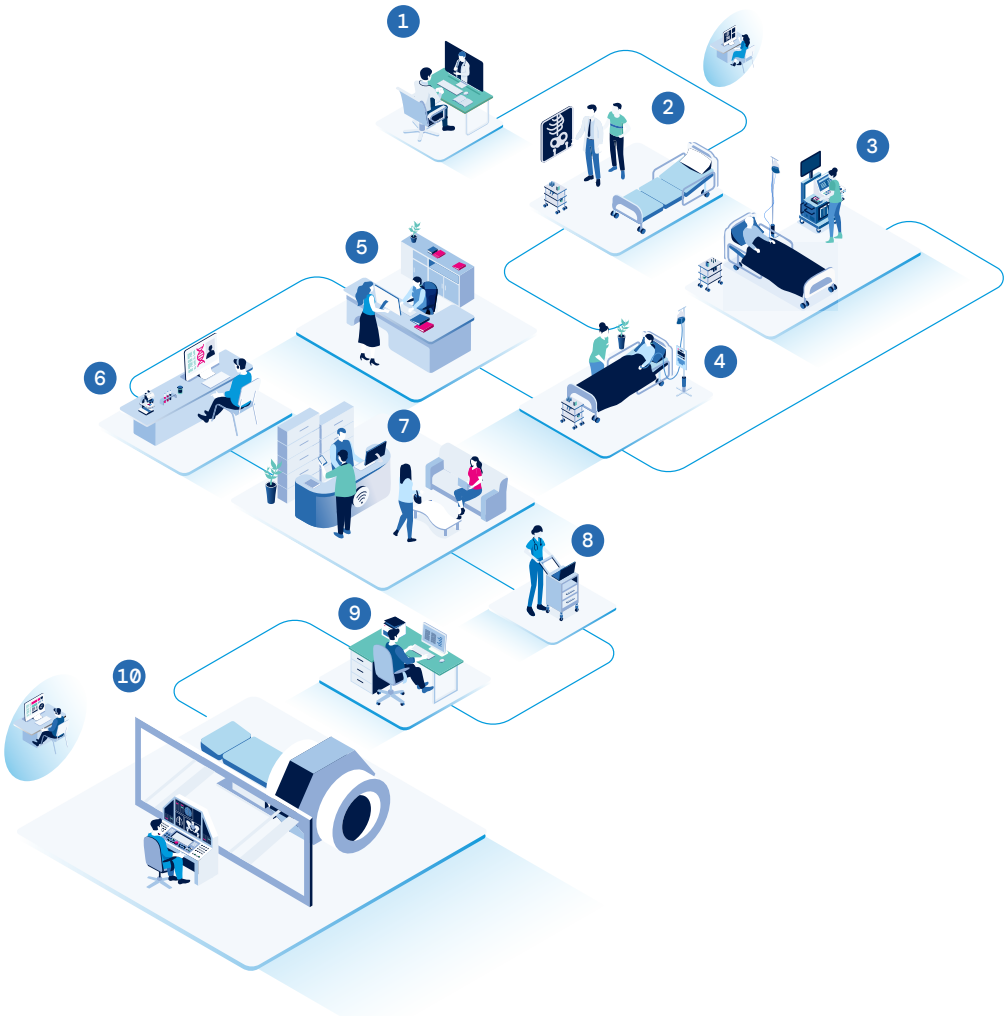
The journey towards a Zero Trust Hospital necessitates the integration of new technologies and applications into existing infrastructures. While the underlying architecture and medical devices may be decades old, modern solutions can be seamlessly integrated to enhance security For instance, deploying advanced identity and access management (IAM) systems ensures that only authorized personnel can access

critical systems. Implementing network segmentation limits lateral movement, containing potential breaches. The major advancements in healthcare with the use of AI poses not only an opportunity for significantly better patient care and outcomes, but also adds significant risk into the enterprise. This technology needs to be embraced and implemented safely.

## The Zero Trust Hospital in Action

Zero trust is the modern framework for securing healthcare enterprises against cybercrime and protecting data privacy. The adoption of a zero trust architecture in health IT is not just a security measure, but a comprehensive approach to modernizing and optimizing the entire healthcare ecosystem.



1. **Secure Telehealth Solutions**
   Provide secure, seamless connectivity for telehealth services, ensuring patient data privacy and compliance with healthcare regulations while delivering excellent clinician and patient experience.

2. **Remote Imaging Access**
   Ensure radiologists can quickly and easily access medical imaging data from any location, maintaining patient confidentiality and data integrity.

3. **Shared Workstation Security**
   As users/clinicians tap in and out of workstations, their personalized security policies are applied versus having generic all–or–nothing security policies on shared workstations.

4. **Medical Device Segmentation**
   Ensure medical devices can only communicate as designed while making these devices invisible on the network to unauthorized users.

5. **Patient Data Protection**
   Protect access to EHR platforms and other systems with sensitive data while preventing data exfiltration to maintain the confidentiality, integrity, and availability of patient data.

6. **Secure Research Data & Access**
   Grant easy and secure access to data for researchers regardless of system management.

7. **Malware and Phishing Protection**
   Decrypting all traffic to ensure encrypted malware cannot reach the device while also preventing users from visiting phishing sites not blocked by traditional means.

8. **Zero Trust Access on 5G**
   Implement zero trust security principles on 5G networks to ensure secure, seamless connectivity for healthcare applications and devices.

9. **Secure Generative AI**
   Leverage secure generative AI technologies to enhance healthcare innovation while blocking sensitive data from going into prompts, safeguarding sensitive patient and proprietary data.

10. **Secure Third Party Access**
    Provide affiliates, contractors and other third parties secure access to critical healthcare systems and data without agent installation or vulnerable internet exposed security appliances.

## Benefits of Transformation

The benefits of this transformation are multifaceted. Enhanced security measures protect patient data, ensuring compliance with regulatory standards. Improved operational efficiency results from the streamlined integration of new technologies. This makes you not only more agile—giving you the ability to innovate faster—but also reduces both CapEx and OpEx costs. Modernization allows you to better secure the hospital (reduce business risk), simplify IT (eliminate costs and complexities), and transform the health system (increase business agility). Furthermore, a zero trust approach fosters a culture of vigilance and continuous improvement, essential in the ever-evolving threat landscape.

> "We have so much technical debt built up over the years. We will never get through it if we keep trying to just update and leverage the same technologies. I am ready to just default on all that technical debt and start fresh with a modern approach to security and infrastructure."
>
> **CISO** | Florida

In conclusion, the transformation to a Zero Trust Hospital is not just necessary—it is imperative. By understanding the anatomy of breaches and the primary attack vectors, and by embracing innovative solutions, hospitals can build a resilient defense against cyberthreats. This chapter sets the stage for a comprehensive exploration of zero trust principles and their application in the healthcare sector, guiding CXOs through the essential steps to secure their institutions in the digital age.

CHAPTER 2

# The Benefits of Zero Trust

As we delve deeper into the zero trust paradigm, it is essential to understand the tangible benefits that this approach can bring to hospitals. Implementing a zero trust architecture is not only about enhancing security—it's about transforming the way hospitals operate, improving productivity, safeguarding trust, and optimizing economic value. This chapter explores these multifaceted benefits, providing a compelling case for why zero trust is an imperative investment for modern healthcare institutions. Later chapters will describe how zero trust works to stop threats, where to begin, and more. Let's first understand the benefits before we dive deeper into the "how."

The benefits of zero trust extend far beyond enhanced security. By improving productivity, reducing risks, and delivering economic value, zero trust transforms the way hospitals operate, providing a robust foundation for future growth and innovation. As we continue to explore the principles and implementation of zero trust in subsequent chapters, it becomes increasingly clear that this approach is not just a security strategy—it is a comprehensive framework for achieving excellence in healthcare.

The following sections will dive deeper into the benefits of zero trust to include: improved productivity, significant improvements in risk management, and the economic values of zero trust.

## Benefit 1: Improved Productivity

One of the most profound benefits of adopting a zero trust architecture is the significant boost in productivity. Traditional security models often rely on perimeter-based and castle-and-moat defenses, which can create bottlenecks and slow down access to critical applications and data. Zero trust, by contrast, emphasizes secure, seamless access from anywhere, ensuring that healthcare professionals can perform their duties without unnecessary hindrances. Having the same seamless experience no matter where the user is connecting from and where the applications live means those users have fewer clicks and log-ins to perform while providing care.

## Clinician Experience and Patient Experience

Zero trust directly enhances the clinician experience by simplifying and securing access to patient records and other critical systems. This seamless access allows healthcare providers to focus on patient care rather than dealing with complex security protocols. Integration of security and zero trust with the existing clinician workflows (such as tap–and–go login) is a prime example of that seamless experience.

Zero trust offers security in the background for the care provider versus being in the more obvious foreground, as traditionally seen. As a result, clinicians can spend less time dealing with security measures and deliver faster, more accurate care, leading to improved patient outcomes and satisfaction. The modern approach to network and security also affords the kind of innovation clinicians strive to implement within their practices in order to enhance the patience experience.

## Positive Impacts on Patient Care

The immediate and secure access to patient data facilitated by zero trust ensures that healthcare professionals have the information they need, when they need it. This agility improves the quality of patient care, enabling timely interventions and reducing the likelihood of errors. The enhanced communication and collaboration among healthcare teams further contribute to better patient care.

Remote radiologists are crucial and essential to healthcare providers and patient care. They are also traditionally weighed down with cumbersome networking gear sent to their homes and/or have to go through very slow legacy VPNs in order to provide reads. Upgrading them to the modern zero trust approach means giving them direct access to PACS systems without extra infrastructure to manage, connectivity from anywhere they are/go, and as fast as the internet will allow (without the bottleneck of VPNs and VDI). This not only improves patient care and satisfaction by shortening the time spent waiting for results, but also enables the care provider to get more reads per day/week.

### Patient Safety and Privacy

Zero trust ensures that only authorized personnel can access sensitive patient information, significantly enhancing patient privacy and safety. By continuously monitoring and authenticating users, zero trust minimizes the risk of unauthorized access. The inclusion of an all–inclusive data protection program into zero trust also minimizes the risk of data breaches, thereby protecting patients' confidential information and your brand reputation.

### Business Continuity and Disaster Recovery (BCDR)

Zero trust architectures are designed to ensure business continuity and facilitate disaster recovery. By providing secure, remote access to critical systems, zero trust enables hospitals to maintain operations during emergencies or disruptions. This resilience ensures that patient care continues uninterrupted, even in the face of unforeseen challenges.

### Mergers and Acquisitions (M&A)

Zero trust can streamline the integration process during mergers and acquisitions by providing a unified, infrastructure agnostic, security framework. This reduces the complexity and risk associated with integrating disparate IT systems and networks, ensuring that the newly formed entity operates securely and efficiently from the outset. With zero trust, you no longer have to deconflict overlapping IPs and network segments. Users from the acquiring entity can immediately have secure access to your applications to be productive on Day 1. The IT struggle to meet TSA deadlines on Day 1 becomes easier with a zero trust approach.

## Benefit 2: Risk Management

### Reduce Risk of Lost Trust, Revenues, Brand Damage, and Patient Outcomes

In the healthcare industry, trust is paramount. Patients trust hospitals with not only their lives, but also their most sensitive information while expecting the highest standards of care. A breach of this trust can have devastating consequences, including loss of revenue, brand damage, and compromised patient outcomes. As referenced earlier, the HIPAA Journal Study, as well as many other studies have proven that cybersecurity is patient security. Zero trust helps mitigate these risks by providing a robust security framework that protects against internal and external threats.

### Outages in Patient Care

Security breaches can lead to system outages that disrupt patient care. Zero trust minimizes this risk by ensuring that all access is continuously monitored and verified, preventing unauthorized actions that could compromise system availability. With zero trust, phishing attempts and malware hidden inside encryption are blocked—preventing devastating ransomware deployments. This ensures that patient care remains consistent and uninterrupted.

### Rescheduling Patients

System outages or breaches can force hospitals to reschedule patient appointments, leading to delays in treatment and care. Unplanned downtime during application migrations to the cloud can also affect clinicians being able to see patients. By maintaining a secure and resilient IT environment, zero trust reduces the likelihood of such disruptions, ensuring that patient schedules are adhered to and care is delivered as planned.

### Mergers and Acquisitions (M&A)

During mergers and acquisitions, the integration of different IT systems can introduce vulnerabilities and risks. In speaking with both CXO and hospital board members, countless breaches have been confirmed to come in through a newly acquired entity. Zero trust provides a cohesive security model that safeguards sensitive data and ensures that the integration process does not compromise security. This reduces the risk of data breaches and ensures a smooth transition.

## Benefit 3: Do More with Less (by removing waste): The Economic Value of Zero Trust

Adopting a zero trust architecture is not just a security measure; it is also a strategic investment that delivers significant economic value and quantifiable ROI. By streamlining security processes, removing legacy infrastructure and technologies and improving operational efficiencies, zero trust enables hospitals to "do more with less." One Fortune 500 CIO even stated, "It's a rare occasion in history where it got more secure, better, and cheaper all at once."

### Cost Savings

Implementing zero trust can lead to substantial cost savings by reducing the need for multiple, disparate point products and security solutions. By consolidating security measures into a cohesive zero trust framework, hospitals can eliminate redundancies and optimize their security investments. Additionally, the automated nature of zero trust reduces the need for extensive manual intervention, lowering operational costs.

Zero trust also leads to cost savings through infrastructure savings. Removing and reducing legacy infrastructure, especially the increasingly more costly vendors who have been recently acquired in the VDI space, dramatically lowers expenses and operational overhead. No longer owning and managing expensive appliances—adopting security as a service you do not need to maintain yourself—not only reduces capital costs, but also human capital costs.

### Increased Efficiency

Zero trust enhances operational efficiency by providing secure, direct access to applications and data. This reduces the time and resources spent on managing and troubleshooting security issues. Removing all the external attack surfaces and legacy internet exposed network/security appliances also means less time spent trying to patch critical vulnerabilities on those systems and applications. All this allows IT teams to focus on strategic initiatives that drive value for the hospital.

With regard to income generation, versus saving costs, enabling the remote radiologist to provide more reads per week directly ties to more income being generated for the health system.

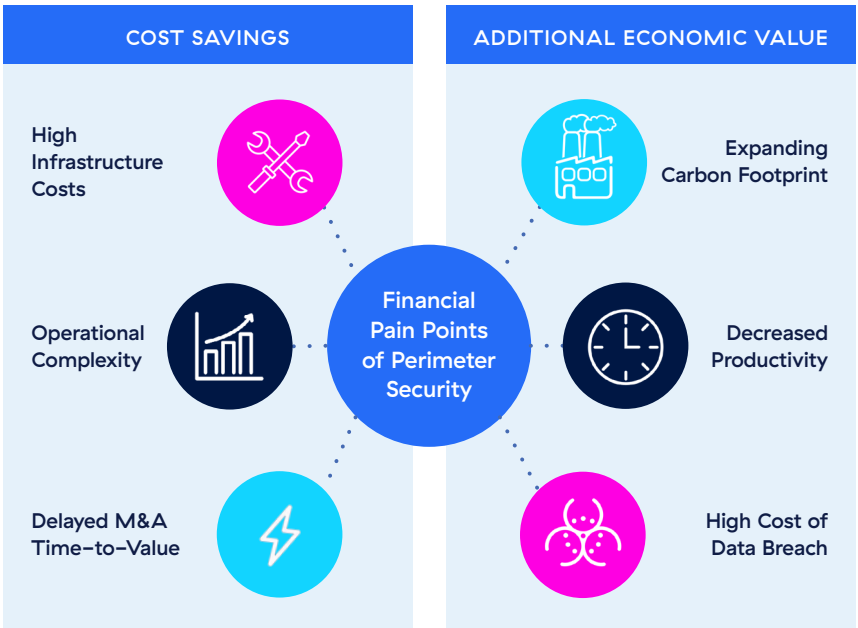
### Better Resource Allocation

By minimizing the risk of breaches and the associated costs of remediation, zero trust allows hospitals to allocate resources more effectively. Zero trust implementation has also proven to decrease the costs of cyber insurance premiums. Spending less money on insurance premiums, operational overhead and human capital, on breach response and recovery means hospitals can invest in other technologies and initiatives that improve patient care and outcomes without sacrificing security.

### Mergers and Acquisitions (M&A)

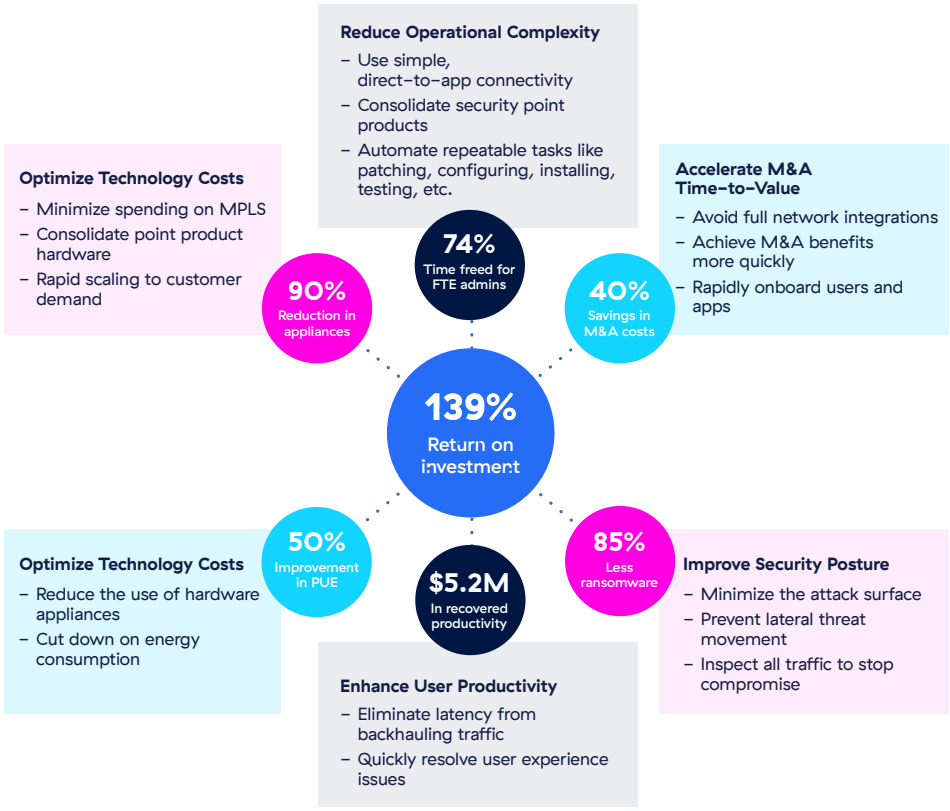
Zero trust can significantly reduce the cost and complexity of integrating IT systems during mergers and acquisitions. By providing a network agnostic, unified security framework, zero trust ensures that the integration process is secure and efficient, reducing the risk of costly disruptions and breaches. Meeting TSA deadlines and providing Day 1 integrations means you get an ROI from the acquisition immediately after Day 0. This enables the newly formed entity to achieve synergies and realize value faster.

## Reducing Cost and Complexity with Zero Trust



# The Economic Advantage of Zero Trust



CHAPTER 3

# Understanding the Anatomy of a Breach

Now that we see many of the benefits zero trust brings, let's next explore how breaches occur so you may better understand how zero trust helps prevent them.

## Impact of Breaches on Patient Care and Hospital Operations

Breaches are not only severely detrimental to the hospital finances and brand reputation, but disruption of patient care is the worst case scenario. Studies have shown that after a significant cyberattack, there are increases in mortality rates, poorer patient outcomes, increases in medical complications, and delayed procedures and tests. The latest insights on cybersecurity risks and trends facing healthcare organizations, informed by the 2024 Digital Health Most Wired Survey National Trends Report showed that security is the top priority for healthcare organizations. Everyone at a health system should be classified as a caregiver—as IT and security are paramount for providing care and preventing devastating breaches.

## Anatomy of a Breach

Understanding the anatomy of a breach is the first step in fortifying our defenses. A typical cyberattack unfolds in a series of calculated steps, often initiated by exploiting human vulnerabilities. Phishing attacks, for instance, are a favored tactic among cybercriminals. These attacks use deceptive emails to trick hospital staff into revealing their credentials. Bad actors then utilize those credentials via internet-exposed appliances and applications in order to gain access to the network. Once inside, attackers can move laterally across the network, gaining unauthorized access to critical systems and data.

Another common attack vector is through internet-exposed networking and security devices. Legacy appliances, often riddled with zero-day and unpatched vulnerabilities, provide an open door for cyber attackers. These outdated systems lack the robust defenses needed to withstand modern threats, making them easy targets even without first having a user's credentials.

There are four key stages, or steps, attackers take to breach organizations even after organizations have spent millions of dollars on next generation firewalls and VPNs.

### 1 – THE BAD GUYS FIND YOUR OPEN ATTACK SURFACE.

What is the attack surface? Every IP that resolves to the internet for the organization is an attack surface. It may be applications. It may be the firewall and the VPN. All those systems with vulnerabilities, like servers with outdated encryption standards, can be compromised. Zero trust architecture helps eliminate the attack surface. If you're reachable, you're breachable.

### 2 – THE BAD GUYS COMPROMISE YOUR NETWORK.

Every compromise comes from the internet and looks for weak links, like unsuspecting users or unprotected devices, to compromise them and set up a beachhead. This beachhead is leveraged to launch further attacks. The goal should be to prevent compromise.

### 3 – THE BAD GUYS GET ON YOUR ROUTABLE NETWORK AND MOVE LATERALLY TO FIND HIGH-VALUE TARGETS.

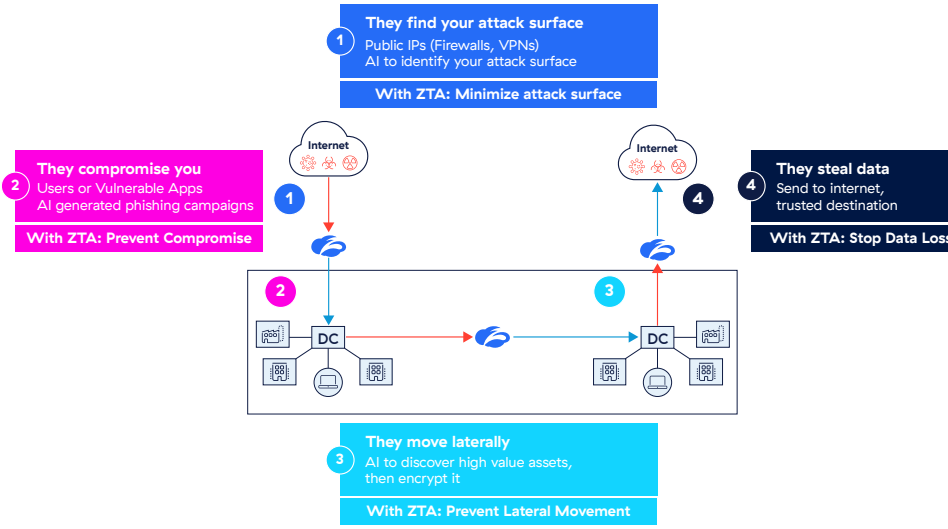
This is what happened with Uber and Colonial Pipeline, among many other examples, where a single machine becomes infected due to the VPN. Since it is on your organization's network, a hacker can traverse laterally across the whole, flat network and bring down every system or application. Or, they can encrypt your data and demand ransom. This is when organizations try doing network microsegmentation, which is extremely difficult. It is like building a highway system of toll booths and toll roads to regulate access. A zero trust architecture, on the other hand, eliminates lateral threat movement.

### 4 – THE BAD GUYS STEAL YOUR DATA AND THE STOLEN DATA IS ALMOST ALWAYS SENT TO THE INTERNET.

Data is the crown jewel of any organization, and the loss of data means a loss of intellectual property, loss of trust among customers, and a blow to brand reputation. Data loss must be prevented.

The figure below depicts a common attack flow for bad actors:




In order to minimize the risk of cyber breaches, organizations should embrace zero trust architecture for protection from cyber breaches by minimizing the attack surface, preventing compromise and lateral movement, and stopping data loss. And this architecture can't be bolted on firewalls and VPNs. However, doing nothing puts organizations at increased risk of attack, while sacrificing user experience.

## How Zero Trust Architecture Provides Better Cyber Protection

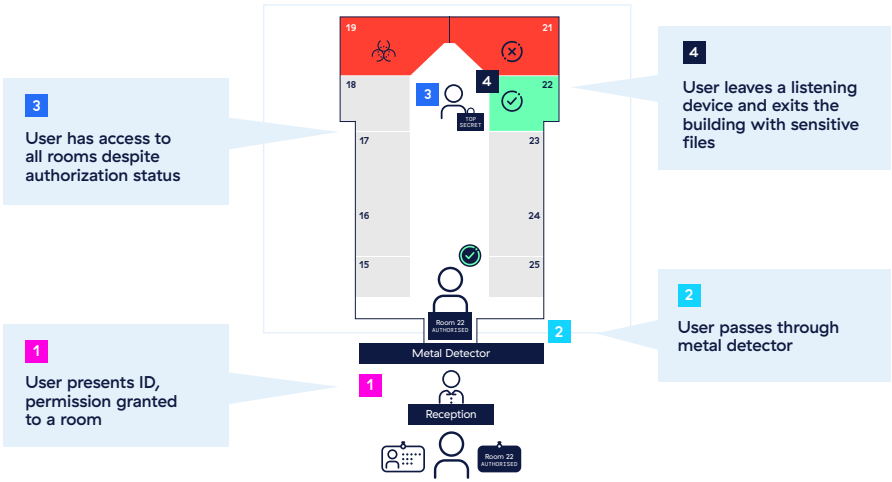
Of the four stages of breach, stage 1 (attack surface) and stage 3 (lateral movement) are the least understood by IT and security professionals. This is because traditional network security using firewalls was never designed to tackle these issues. To illustrate, consider two analogies that describe and contrast the zero trust and firewall–based architectures.

### How to Prevent Lateral Threat Movement on Your Network

The first step is NOT putting users on the network, but instead connecting them directly to applications after performing identity and context verification.

How does one reach an application without being on the network? It sounds a little complicated, so the following is a simple analogy.

If a guest comes to the hospital and enters through the front entrance, they're going to be greeted by the receptionist who will check their ID. If the identity of the visitor is verified, they receive a badge. If they are told to go to a specific patient room without an escort, the visitor may decide to wander around, and go to any room that is unlocked. They may go to an adjacent building since everything is interconnected, then snoop around, steal data, leave behind dangerous material, and depart unnoticed. This is not a good idea. That's why prudent organizations do not allow unescorted visitors.



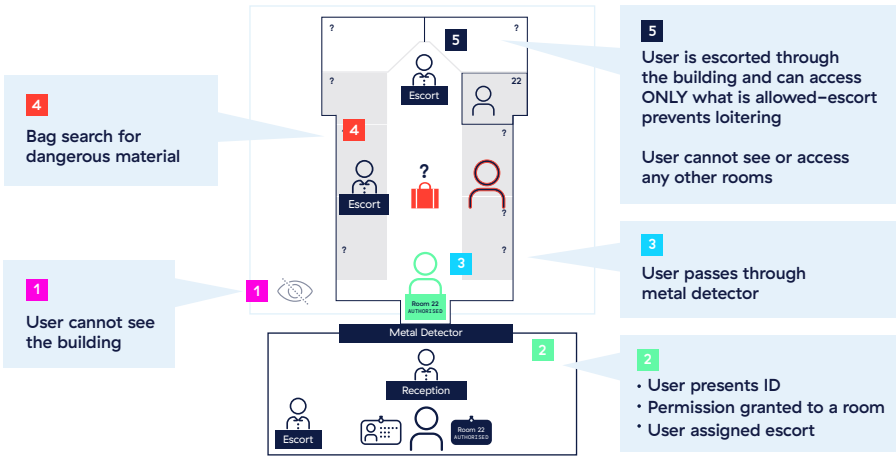

Applying this analogy to lateral threat movement, once the users get on the network (either by being in the hospital or by using a VPN), they can traverse laterally and find hundreds and hundreds of applications and systems. How does one avoid this? The answer is a zero trust architecture. To continue with the visitor analogy from above, ZTA would:

- Remove any identifying health system logos and scrub its location from any internet and map sites so visitors can't even find the hospital.
- Remove the tunnels that connect the buildings on campus so each building is isolated, which prevents lateral movement.

- Move the receptionist far away from the building, so outsiders can't determine which building the receptionist manages.

With ZTA, visitors still stop at the receptionist, have their ID verified, and receive a badge. This time, they'll be taken to a specific room by an escort. Before the visitor enters the room, their bags are checked for dangerous material (malware, from a security standpoint), and if all is good, the visitor is escorted directly to the specifically authorized room, no loitering allowed. Once the meeting is over, the visitor is escorted out. Before the visitor exits, however, their bags are checked for any stolen goods; in ZTA, this translates to data loss prevention (DLP).




In these examples, the first building is like the data center, where the applications are hosted. A room is like an application. The buildings represent public clouds like Azure and Amazon Web Services (AWS). ZTA, by design, acts as a switchboard that connects the user to a particular application within a particular data center or cloud (or a visitor to a room, to extend the analogy).

If a user needs to access a specific file share, that is all that user connects to, not the organizational network. The user can't move laterally to access or try to access the EHR or other applications. This is how lateral movement is eliminated. It is a core principle of ZTA that traditional technology, like firewalls, are not designed to accommodate.

So how do attackers get into an organization's network in the first place? Let's look at the top attack vectors as reported across industries.

## Top Attack Vectors

### Phishing

Phishing remains a predominant threat, luring even the most vigilant employees into divulging sensitive information. The harvested credentials are then used to infiltrate legacy internet–exposed appliances, allowing attackers to traverse the network with ease. This lateral movement can go unnoticed, enabling the attacker to compromise multiple systems and exfiltrate data over extended periods and eventually encrypt sensitive data.
Bad actors are leveraging AI to craft more sophisticated phishing attacks and hide behind encryption.

A common misconception is that multifactor authentication (MFA) is enough to thwart attacks which use harvested credentials, however, MFA has been proven to be bypassed utilizing a number of tactics and techniques plus older applications may still not yet support MFA. Email protections are not enough to prevent phishing attacks. Phishing websites are difficult to detect by traditional means because they use encryption and are hosted by legitimate hosting providers like Amazon and Microsoft cloud environments.

### Internet–Exposed Network/Security Devices

Legacy network and security devices, many of which are publicly accessible via the internet, are fraught with vulnerabilities. These devices have historically and consistently been found to have many new zero–day vulnerabilities released throughout the year. They often operate on outdated software, lack essential security patches, and are inherently insecure by modern standards. Attackers can exploit these weaknesses to gain a foothold within the hospital's network, bypassing traditional security measures. Once inside the network, bad actors have free reign to move to critical applications, steal data, and encrypt sensitive information. This legacy infrastructure significantly increases your attack surface with internet exposure.

### Internet-Exposed Cloud and Distributed Applications

Healthcare providers have been adopting cloud over the years—both SaaS applications as well as applications hosted in private clouds (IaaS). While this has been another technology the industry has embraced, this also opened the doors to even more attacks as your attack surface has spread further into the open internet. Deploying applications into the cloud, while aiding significantly with modernization of patient care, also adds security complexities often overlooked.

## How Zero Trust Helps Prevent / Contain Breaches

In the analogies described above to explain zero trust architecture, think of applications as the destination. These applications fall in two buckets:

### Private Applications

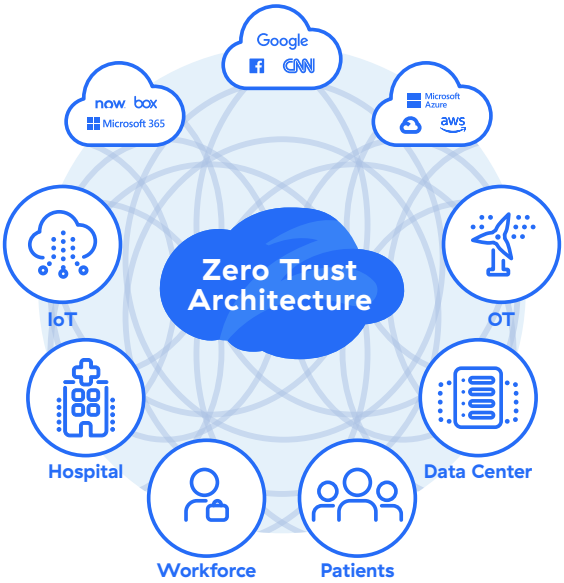
Private applications are applications managed internally by the IT department. These are often hosted in a an organization's data centers, satellite facilities, or in IaaS/PaaS public clouds like Azure, AWS, or GCP.

### Public Applications

Public applications are applications managed by others. These are SaaS applications hosted and secured by companies like Microsoft 365, Salesforce, ServiceNow, or Workday. This also includes destinations such as LinkedIn, BBC, Facebook, and Google Search accessed on the open internet.

Both of these application types are simply destinations. Users/devices, things (IoT/OT), and workloads need to access them. By default, they're all untrusted. The biggest difference between a zero trust architecture and traditional network security architecture is that with ZTA there's no routable network between the user and the application. How do they connect? They go through a zero trust policy engine, which acts as a switchboard for various entities (users, devices, and applications) to communicate with each other over any network.

When entity A tries to reach entity B, the connection is directed through the zero trust policy engine. The first thing that happens is that the connection is stopped.



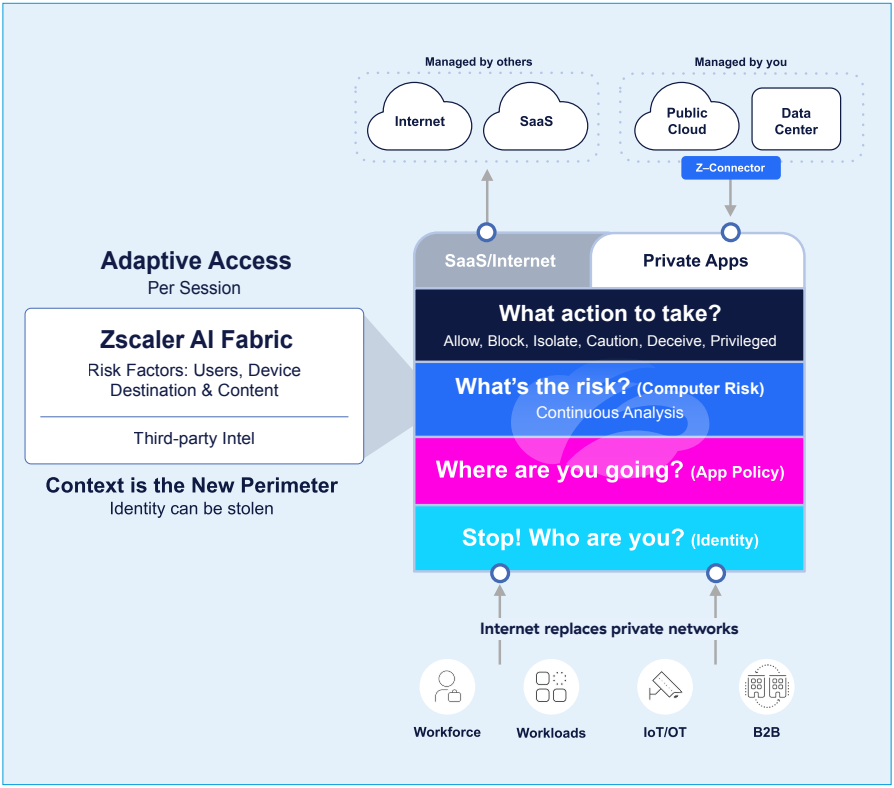

The ZTA proxy architecture also allows an enterprise to inspect all traffic, identify and isolate threats, prevent data loss, and prevent the execution of malicious code. This proxy architecture is important because it functions as a proper ZTA 'switchboard' and terminates all traffic. This ensures that:

- All traffic, including encrypted traffic, can be scanned in a single pass for malware and threats
- The corporate network IP address range is no longer visible to hackers

ZTA also verifies identity using an integrated identity and access management (IAM) system. But, since an identity can be stolen, the ZTA also considers the properties of the device in use. Is it managed? Is it unmanaged? Is it BYOD? Where is its geographic location? What is the user trying to do? This context is very important. The proper policy is determined and applied based on all of these factors.

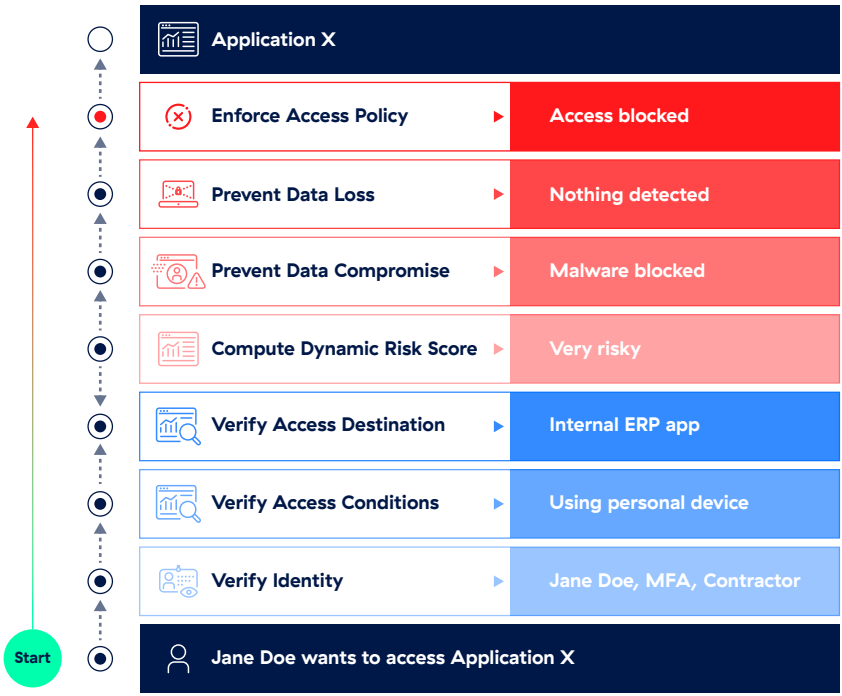
If a connection looks valid, the ZTA takes steps to measure and control risk, prevent compromise, and stop data loss. To do so, the ZTA inspects all inbound and outbound traffic for malware and outbound sensitive data.




Beyond this, the ZTA leverages adaptive control, continuously assessing changes in the user's risk. If it sees anomalous behavior of traffic or the user, it can terminate any suspicious connections. Next, the ZTA enforces policy, which is done per user–initiated session. The enforced policy could be Allow, Block, Caution, Isolate, and Stream Pixels, Prioritize, or Deceive. The ZTA grants users access only to certain applications, and prevents lateral movement.

Finally, if all checks are in good standing, the ZTA takes the final step to connect the user to the authorized application. For external applications, this is a simple connection. For internal applications, the ZTA establishes an inside–out connection using a lightweight software component on the server side. This way, internal applications only resolve to the ZTA cloud and not to the internet; that's how the ZTA hides the attack surface.




How does this work in practice? Consider the figure above where Jane Doe is requesting to access Application X. ZTA first verifies identity to learn that Jane is a contractor. Next, it looks into how Jane is connecting and sees that she is on a personal device. The application she wishes to access is a sensitive, internal ERP application. These conditions deem her request to be "very risky," and while there is no record of data loss, there is a history of malware downloads that had to be blocked. Based on these factors, the ZTA decides to enforce an access policy by blocking access.

Contrast this method with the traditional architecture of firewalls and VPNs. This is important because many legacy architectures falsely claim to be zero trust architecture. Fundamentally, a firewall is not a proxy architecture. It is categorized solely as pass–through architecture because it can only perform limited inspection and it connects users to the network. By doing this, it enables lateral threat movement. A firewall is facing the internet and basically announces, "I am here, connect with (and attack) me."

Zero trust is designed to dramatically reduce the risk of breaches with both prevention as well as containment of breaches. Simply hiding your internet-exposed network/security appliances and applications removes the vast majority of your attack surface—removing many of the common attack vectors. Remember – if you're reachable, you're breachable.


Phishing attempts can be thwarted with the use of decryption. Once you uncover attacks hidden inside encryption, they can be more easily identified and blocked. Even if someone's credentials are phished and compromised, a bad actor won't be able to make use of them if there is nothing exposed to the internet to log in with them.

Should a bad actor somehow still manage to get inside, other security measures can be implemented within a zero trust architecture in order to minimize the blast radius of damage. This includes deployment of deception decoys in order to keep the bad actor busy while alerting the security team of an intrusion. Segmentation is an essential element to prevent any kind of lateral movement of both the bad actor and any kind of malware deployed.

Finally, should a bad actor somehow still make it all the way through to your data, a robust data protection strategy built into zero trust will save your organization from the devastation of lost patient data. This includes safeguarding data at rest and in motion, data in your data center, your private cloud, public cloud, and on devices.


CHAPTER 4

# Common Misconceptions: Mythbusting Zero Trust

In the journey towards implementing zero trust in hospitals, several myths and misconceptions can create hesitation and/or resistance among decision-makers and/or technologists. These myths often stem from a lack of understanding or the complexities associated with the implementation process. In this chapter, we aim to debunk some of the most common myths about zero trust, providing clarity and confidence for CXOs considering this transformative approach.

## Myth 1: One Brand/Vendor Partner for Zero Trust

### Reality: Zero Trust Requires an Ecosystem of Partners

A prevalent myth is that zero trust can be effectively implemented through a single brand or vendor. This is not true. Zero trust is a comprehensive security paradigm that requires integration across various layers of an organization's IT infrastructure. Successful zero trust implementation involves an ecosystem of partners, each contributing specialized solutions that work seamlessly together.

### Ecosystem of Partners

To operationalize zero trust, hospitals need to collaborate with multiple vendors specializing in different aspects of cybersecurity. This collaborative approach ensures that all facets of security are covered, from identity management to endpoint detection and response. Putting all your eggs in one vendor basket can be very risky as this is the same idea of having the fox guarding the henhouse.

**Identity management:** Partners specializing in identity management, such as Okta, Microsoft Azure AD, and Imprivata, play a crucial role in ensuring that only authorized users have access to critical systems and data. They provide robust authentication and authorization mechanisms that are central to zero trust.

**Endpoint detection and response (EDR):** Vendors like CrowdStrike and Carbon Black offer advanced EDR solutions that monitor and protect endpoints from threats. Integrating these solutions into a zero trust framework ensures that devices accessing the network are secure and compliant with security policies.

**Security information and event management (SIEM) and security orchestration, automation, and response (SOAR):** Solutions from vendors like Splunk and IBM QRadar provide the necessary tools for continuous monitoring, threat detection, and automated response. These tools are essential for maintaining the zero trust principle of continuous verification and real-time threat mitigation.

## Myth 2: Hard to Deploy—Taking Years of Effort

### Reality: Zero Trust is More Accessible Than Ever

Another common myth is that deploying zero trust is a lengthy and complex process that takes years to complete. This is far from the truth. With the right strategy and partners, hospitals can implement zero trust incrementally and achieve significant milestones within months.

### Customer Stories: Rapid Implementation

Consider the case of a mid-sized hospital that partnered with Zscaler to implement zero trust. By leveraging Zscaler's cloud native platform and following the structured guidance from the *Zero Trust Hospital: An Architect's Approach to Achieving Zero Trust in a Clinical Setting* (see Additional Resources), the hospital achieved a secure zero trust environment in less than six months. The phased approach allowed them to start with critical systems and gradually expand the scope, ensuring minimal disruption to operations.

Another large sized provider partnered with Zscaler and deployed to 70,000 users over a weekend to immediately achieve a significant milestone of protecting users. They then took another two weeks to hide their assets from the internet—dramatically reducing risk in a short period of time. While the assets were hidden, they were able to spend the next several months further defining segmentation rules for users and applications.

### Operationalizing Zero Trust—Day 2: How-To

Operationalizing zero trust is not a one-time event but an ongoing process. The *Zscaler Zero Trust Hospital: An Architect's Approach book* offers a comprehensive roadmap for this journey. Day 2 operations focus on maintaining and optimizing the zero trust framework, ensuring continuous protection, and adapting to evolving threats.

## Myth 3: Disruptive to the Organization

**Reality: Zero Trust Can Be Seamlessly Integrated**
There is a misconception that transitioning to zero trust is highly disruptive to an organization's daily operations. In reality, a well-planned zero trust implementation can be conducted with minimal disruption, enhancing security without hindering productivity.

**Customer Story: Seamless Integration**
A large healthcare network implemented zero trust with the help of Zscaler and experienced minimal disruption. By conducting thorough planning and involving cross-functional teams, the implementation was aligned with the hospital's operational workflows. Continuous communication and training ensured that staff were well-prepared, resulting in a smooth transition that enhanced security without compromising daily operations. Implementing the integration with other vendors, like Imprivata, allowed for that seamless adoption by the care providers as this did not hinder their workflows (and on most occasions, actually made it faster/easier.)

"What used to take weeks to accomplish with on-premises infrastructure and staff support can now be achieved in a matter of hours with Zscaler, without the need to be on-site."

**MANI MASOOD** | Head of Information Security, AMN Healthcare

## Myth 4: Expensive

### Reality: Zero Trust is a Cost-Effective Investment

Many CXOs believe that adopting zero trust is prohibitively expensive. However, when considering the potential costs of data breaches, regulatory fines, and reputation damage, zero trust is a cost-effective investment that delivers significant long-term value. If you also account for the benefits referenced in the earlier "Do more with less" chapter, you can see there is a strong ROI with zero trust. Countless healthcare providers have also reduced their cybersecurity insurance premiums (by a significant margin) by providing auditors proof of a zero trust architecture implementation.

### Business Value Assessment (BVA) Customer Story

A leading hospital conducted a business value assessment with Zscaler to evaluate the financial impact of zero trust. The assessment revealed that the hospital could achieve a substantial return on investment (ROI) by reducing the risk of breaches, lowering both capital and operational costs, and improving workforce efficiency. Within the first year, the hospital realized significant cost savings, which far outweighed the initial investment. Subsequent years also show more ROI as other vendor renewals have been stopped or reduced by removing overlapping point products. Subsequent BVR (business value realization) after deployments show these cost savings have been realized.

### Conclusion

Debunking these myths is crucial for CXOs to make informed decisions about zero trust. By understanding the reality behind these misconceptions, hospitals can confidently embark on their zero trust journey, knowing that it is a strategic, achievable, and cost-effective approach to securing their digital environments. As we continue to explore the implementation and benefits of zero trust in subsequent chapters, it becomes increasingly evident that this paradigm is not only essential for modern healthcare but also within reach for organizations willing to embrace it.

## Business Value Assessment (BVA) Example

| 197%+ Return on investment | <12 month Payback period |
|---|---|

**ROI for ACME (3 year totals)**

| | |
|---|---|
| **COST SAVINGS** | |
| **Product Savings** Eliminate point products | $4.20M |
| **Operational Savings** | $0.84M |
| **Network Savings** | $1.80M |
| **COST AVOIDANCE** | |
| **Risk Reduction** | $1.5M |
| **User Experience** | $2.7M |
| **Remote Radiology Efficiencies** (not calculated) | $0K |
| **TOTAL** | $11.0M |

CHAPTER 5

# Where to Begin with Zero Trust

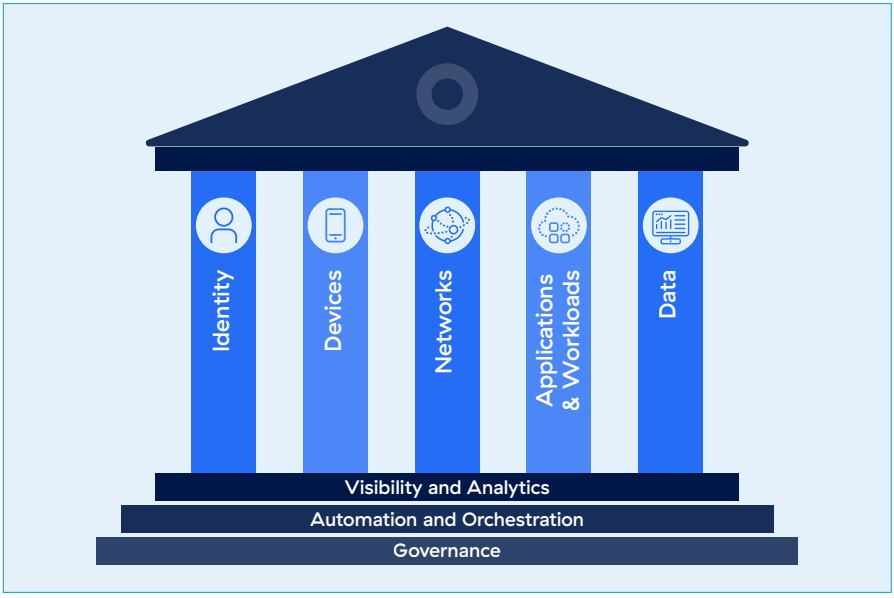
 

Embarking on the journey towards zero trust can seem daunting, especially in the complex and high-stakes environment of a hospital. However, understanding where to start is crucial for a successful implementation. This chapter focuses on two fundamental elements: the importance of identity management and prioritizing users and internet exposure. By addressing these areas first, hospitals can lay a solid foundation for a comprehensive zero trust architecture that enhances security and operational efficiency. But first, let's briefly explore zero trust frameworks.

## Zero Trust Frameworks: A Comparative Overview

### CISA's Zero Trust Maturity Model

The Cybersecurity and Infrastructure Security Agency (CISA) offers a Zero Trust Maturity Model designed to be CXO-friendly. This model provides a high-level roadmap for organizations to follow, emphasizing the importance of adopting zero trust principles without being overly prescriptive. It serves as a strategic guide, helping CXOs understand the broad strokes of zero trust adoption and the key milestones along the journey.



CISA's model is particularly valuable for its approachability. It breaks down the complex zero trust concept into digestible segments, making it easier for executive leaders to grasp the strategic benefits without delving into technical minutiae. This framework focuses on:

1. **Identity:** Ensuring that all users are authenticated and authorized
2. **Devices:** Keeping track of all devices accessing the network and ensuring they meet security standards
3. **Network:** Implementing network segmentation and microsegmentation to contain potential breaches
4. **Applications and workloads:** Securing applications and ensuring they are accessed securely
5. **Data:** Protecting data at rest and in transit, ensuring it is accessible only to authorized users

CISA also defines various stages of the zero trust journey from traditional manual efforts through to optimal automation.

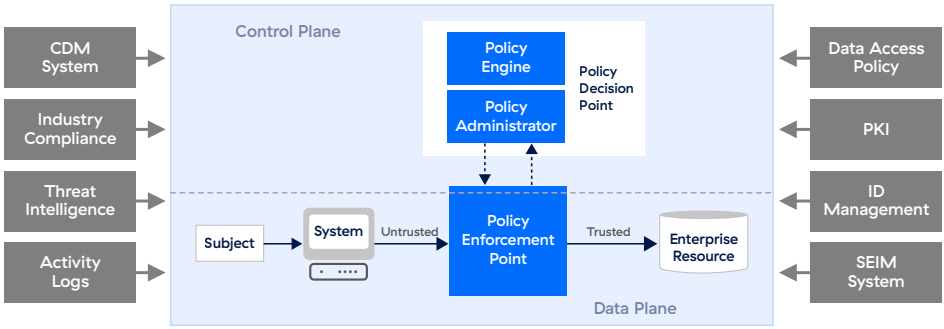
### NIST's Zero Trust Architecture

For those seeking a more detailed and technical guide, the National Institute of Standards and Technology (NIST) offers a comprehensive special publication on the zero trust architecture (ZTA) framework. The NIST SP 800–207. This reference guide delves into the specifics of what to do and how to do it, making it an invaluable resource for practitioners and IT teams responsible for implementing zero trust principles.

NIST's framework is less CXO–friendly due to its technical depth but is crucial for translating strategic vision into actionable steps. Key components of the NIST ZTA include:

1. **Policy engine (PE):** Responsible for making access decisions based on policy rules
2. **Policy administrator (PA):** Enforces the decisions made by the PE
3. **Policy enforcement point (PEP):** The gatekeeper that grants or denies access based on instructions from the PA
4. **Continuous diagnostics and mitigation (CDM):** Ongoing monitoring and assessment of the network and endpoints to ensure compliance with security policies




### Zscaler's Zero Trust Hospital: An Architect's Approach

The accompanying book in this series, *Zero Trust Hospital: An Architect's Approach to Achieving Zero Trust in a Clinical Setting* (see Additional Resources) is a pivotal resource that bridges the gap between high-level strategy and technical implementation. This comprehensive guide provides actionable insights and detailed blueprints for deploying a zero trust architecture tailored to the specific needs of hospitals. The guide cross-references both the CISA and NIST frameworks, offering a holistic approach that combines strategic vision with technical rigor.

## Identity Management as the Cornerstone of Zero Trust

At the heart of zero trust lies the principle of "never trust, always verify." This principle is fundamentally tied to identity management. Ensuring that you have a robust identity management system in place is the first and most crucial step in implementing zero trust. Without accurate and reliable identity management, it is impossible to enforce the strict access controls and continuous verification that zero trust demands.

### Key Components of Identity Management

Authentication and authorization: Robust authentication mechanisms, such as multifactor authentication (MFA), ensure that only legitimate users can access critical systems and data. Authorization processes further define what each authenticated user is allowed to do within the network, based on their role and responsibilities.

**Identity governance:** Identity governance involves managing and monitoring user identities and access rights throughout their lifecycle. This includes onboarding new employees, adjusting access as roles change, and promptly revoking access when employees leave the organization.

**Single sign-on (SSO):** Implementing SSO simplifies the user experience by allowing users to access multiple applications with a single set of credentials. This not only enhances productivity but also reduces the risk of password fatigue and the likelihood of users employing weak or reused passwords.

**Zero trust network access (ZTNA):** ZTNA solutions provide secure, granular access to applications based on user identity and context. Unlike traditional VPNs, ZTNA ensures that users are only granted access to specific applications they need, rather than broad network access.

### Why Identity Management Is Critical for Hospitals

For hospitals, effective identity management is critical not only for security but also for ensuring uninterrupted patient care. Medical professionals need quick and reliable access to patient records and clinical applications. A robust identity management system ensures that this access is secure and efficient, preventing unauthorized users from gaining access to sensitive information while enabling legitimate users to perform their duties without delay.

### Prioritizing Users and Internet Exposure Identifying and Securing High-Risk Users

In any organization, certain users pose higher security risks due to the sensitivity of the data they access or the roles they perform. In a hospital setting, these high-risk users typically include:

**Senior executives:** Access to strategic and financial data makes them prime targets for cyber attackers.

**Medical staff:** Doctors, nurses, and other clinical staff access critical patient data that must be protected.

**IT administrators:** They have broad access to the hospital's IT infrastructure, making them key targets for cyberthreats.

Prioritizing these high-risk users involves implementing stricter access controls, continuous monitoring, and regular audits to ensure that their access remains secure and appropriate.

## Managing Internet Exposure

Another critical aspect of zero trust is minimizing internet exposure. Internet-exposed systems and applications are prime targets for cyber attackers. Reducing this exposure involves:

**Removing or hiding internet exposed network security appliances:** Internet exposed appliances like VPN and VDI should be removed or at least hidden behind the zero trust proxy. These are often attacked by bad actors because they provide very broad/wide access to critical systems internally.

**Remove applications from visibility:** Applications should not be visible by anyone on the internet nor should they be fully visible to all users. Users should only be able to not only access the applications they are authorized, but only even see those said applications.

**Network segmentation:** By segmenting the network into smaller, isolated segments, hospitals can contain potential breaches and limit lateral movement. This makes it harder for attackers to move from one compromised system to another.

**Application access controls:** Implementing strict controls over which applications are accessible to users and ensuring that these applications are secured with up-to-date patches and configurations.

**Web isolation:** Web isolation technologies can help protect users from internet-based threats by isolating web traffic and preventing malicious content from reaching the endpoint.

**Continuous monitoring:** Continuous monitoring of network traffic and user activity helps detect and respond to suspicious behavior in real-time, reducing the risk of breaches.

## Practical Steps to Get Started

### Transformation: Overcoming Inertia

As business and technical leaders define digital transformation roadmaps, there are unprecedented opportunities to enhance patient care resulting in better outcomes, improve data accessibility, and streamline healthcare delivery. Breaking the chains of technical debt can be difficult and migrating away from legacy network security architectures is often a first hurdle that needs to be cleared. As these infrastructures have grown over the years so have the attack surfaces and the level of risk involved in maintaining these environments.

Transforming legacy security architectures to meet the demands of distributed applications, mobile users and devices, connected medical devices, internet of things (IoT), and cloud models can help to not only reduce risk but deliver the agility needed to accomplish larger digital transformation initiatives. Zero trust is a methodology that can help transform security by shrinking the attack surface resulting in reduced risks facing today's healthcare organizations.

The question that many leaders face is where to start on their journey to zero trust. For many it starts with securing the workforce and protecting the mission critical assets the business cannot do without. If we move one layer deeper, this often starts with remote users and devices. Focusing on a specific use case creates an achievable goal while addressing one of the biggest attack surfaces. This doesn't require a lift–and–shift of an entire infrastructure and can be accomplished without any significant changes to existing infrastructure. Instead of focusing all efforts securing users connecting to a network, the focus can become the identity of users and devices, and connecting them only to the applications and services they are allowed to access – regardless of the underlying network infrastructure. This starts to separate the dependency on hardware while modernizing security.

Many network security vendors have a product or solution they claim to help achieve zero trust. The issue is most of these are simply legacy security technologies being offered in a different footprint, i.e., firewalls are now virtual firewalls. While there can be a place in a security architecture for some of these, they were not designed on a zero trust model.

It is critical for executives and practitioners to agree on a definition of zero trust and to ensure their security vendor is able to help achieve the goal of implementing a zero trust framework.

The question that often comes up within healthcare organizations is how do you operationalize zero trust and how will it affect the business and day two operations. It is important to first define a transformation roadmap that articulates the phases and goals of each step along a journey to zero trust. Creating this playbook is an important reference for leaders to set clear goals within their functional areas. Involving the right technology areas early–on in discussions and planning often shortens the deployment cycle and results in a successful rollout.

While each organization differs, the following functional areas are seen as critical to this process: Identity, networking and security architecture, security operations, desktop team, and cloud architects. Each of these roles should have an understanding of any requirements needed, operational workflow changes, and the end–user experience. When these roles are involved from the initial planning to the production rollout the knowledge gap shrinks, the technical requirements are understood early, all resulting in shorter project timelines and positive outcomes. Here are some practical steps we see leading healthcare organizations taking to start the transformation to zero trust.

**Assess current state:** Conduct a thorough assessment of the current identity management and internet exposure landscape. Identify high–risk users, systems, and applications that require immediate attention.

**Develop a roadmap:** Create a detailed roadmap for implementing zero trust, starting with identity management and prioritizing high–risk users and internet–exposed systems. This roadmap should include milestones, timelines, and key performance indicators (KPIs) to measure progress.

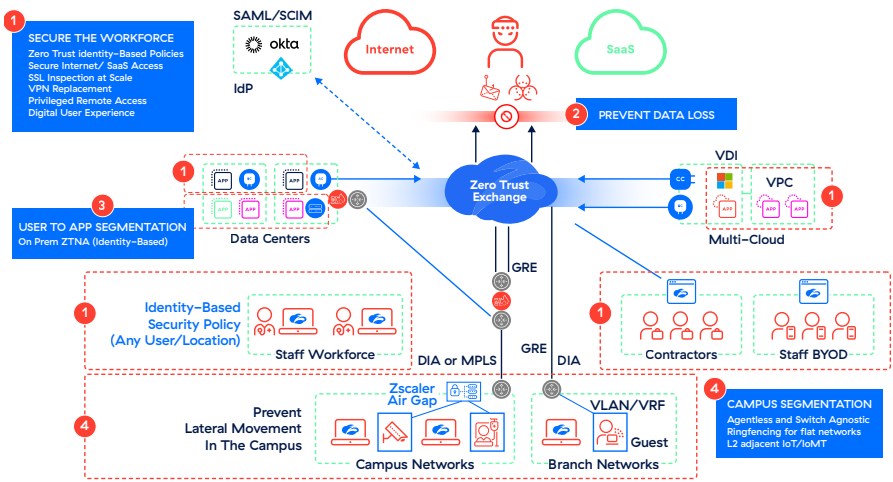
**Implement key technologies:** Deploy the necessary technologies for robust identity management, such as MFA, SSO, and ZTNA. Additionally, implement network segmentation, web isolation, and continuous monitoring solutions to manage internet exposure effectively.

**Educate and train:** Ensure that all staff, especially high-risk users, are educated about the principles of zero trust and trained on the new security protocols and technologies. Regular training and awareness programs are essential to maintain a strong security culture.

**Continuously improve:** Zero trust is not a one-time project but an ongoing journey. Continuously review and improve your security posture based on emerging threats, technological advancements, and feedback from users and stakeholders.

The *Zero Trust Hospital: An Architect's Approach* book is a source of information with detailed step-by-step actions which can be referenced by the technical teams. The guide walks your teams through the steps as outlined below:

## Security Initiatives | Risk-Based Prioritization



## Conclusion

Starting with robust identity management and prioritizing users and internet exposure sets a solid foundation for zero trust. These initial steps are critical for building a secure, resilient, and efficient hospital environment. By focusing on these areas first, hospitals can significantly enhance their security posture, protect sensitive patient data, and ensure that healthcare professionals can deliver the highest standards of care without compromising security. As we continue to explore the principles and implementation of zero trust in subsequent chapters, it becomes clear that taking these foundational steps is essential for achieving long-term success in the zero trust journey.

CHAPTER 6

# How to Promote a Zero Trust Culture

Implementing zero trust in a hospital setting requires not only technical expertise but also the ability to effectively communicate its benefits to various stakeholders within the organization. This chapter provides a roadmap for CXOs on how to internally sell zero trust, from presenting to the board to engaging internal stakeholders and addressing the concerns of users, clinicians, and radiologists.

## Gaining Board Support

Securing buy–in from the board is a critical step in the journey towards implementing a zero trust architecture. As CXOs, presenting a compelling case to the board involves articulating the strategic benefits, financial implications, and risk mitigation aspects of zero trust. This section provides guidance on effectively presenting to the board, focusing on risk reduction, cost/benefit analysis, and considerations during mergers and acquisitions.

### Risk Reduction: Safeguarding Brand and Avoiding Costly Spend

When presenting to the board, it is essential to highlight the significant risk reduction that zero trust offers. Boards are acutely aware of the potential damage that data breaches can inflict on an organization, not only in terms of direct financial loss but also in terms of long–term reputational damage.

**KEY POINTS TO COMMUNICATE:**

#### Safeguarding the Brand

**Reputation management:** Emphasize how zero trust protects the hospital's reputation by significantly reducing the risk of data breaches. A strong security posture reassures patients and stakeholders that their data is safe.

**Patient trust:** Highlight that maintaining the confidentiality and integrity of patient data is crucial for sustaining trust. Any breach can erode patient confidence and loyalty, impacting the hospital's ability to attract and retain patients.

### Avoiding Costly Spend

**Breach costs:** Provide data on the average costs associated with data breaches, including regulatory fines, legal fees, and the expenses related to breach remediation and recovery. The current average costs of breaches for healthcare providers (at the time of this book publishing) is well over $10,000,000.

**Proactive investment:** Explain that investing in zero trust is a proactive measure that can prevent these costly incidents. The cost of implementing zero trust is often significantly lower than the potential costs of dealing with a major breach.

### Cost/Benefit Analysis of Replacing Legacy Technology with Zero Trust

A thorough cost/benefit analysis is crucial for demonstrating the financial viability of transitioning to a zero trust architecture. This involves comparing the costs associated with maintaining legacy technology against the benefits of adopting a modern zero trust approach.

**KEY POINTS TO COMMUNICATE:**

### Costs of Legacy Technology

**Maintenance and upgrade costs:** Highlight the ongoing costs associated with maintaining and upgrading legacy systems, which often require significant resources without providing commensurate security benefits.

**Vulnerability management:** Legacy systems are frequently targeted by cyber attackers due to their known vulnerabilities. The costs of managing these vulnerabilities, including patching and incident response, can be substantial.

## Benefits of Zero Trust:

**Enhanced security:** Zero trust provides a modern, comprehensive security framework that reduces the attack surface and prevents unauthorized access, thereby lowering the risk of breaches.

**Operational efficiency:** Zero trust streamlines access management and reduces the complexity of security protocols, leading to increased productivity and lower operational costs.

**Scalability and flexibility:** Zero trust solutions are designed to scale with the organization, providing the flexibility to support future growth and technological advancements.

**Quantifiable savings:** Present a detailed analysis of the potential savings from reduced breach incidents, reduced capital and operational costs, lower maintenance costs, and improved operational efficiency.

**Long-term value:** Emphasize the long-term value of zero trust in terms of sustained security, compliance with regulatory requirements, and the ability to adapt to evolving threats.

**Cybersecurity insurance premiums:** Providing evidence to auditors of a zero trust implementation reduces premiums significantly.

# Creating Organization Support via Specific Events: The M&A Risk Example

Mergers and acquisitions (M&A) present unique security challenges, as integrating disparate IT systems and security protocols can introduce vulnerabilities. A significant proportion of breaches occur in acquired entities due to weaker security postures or unaddressed vulnerabilities.

**KEY POINTS TO COMMUNICATE:**

**Due diligence:** Emphasize the importance of conducting thorough cybersecurity due diligence during the M&A process. Identifying potential vulnerabilities in the acquired entity is crucial for preventing breaches post–acquisition.

**Zero trust integration:** Explain how zero trust can be integrated into the M&A strategy to ensure that acquired entities adhere to the same stringent security standards. This reduces the risk of breaches originating from newly acquired systems and can be implemented Day 1.

## A Unified Security Framework

**Seamless integration:** Highlight how zero trust provides a unified security framework that simplifies the integration of acquired entities. By enforcing consistent security policies and continuous monitoring, zero trust ensures a smooth and secure transition.

**Scalability:** Zero trust solutions are scalable, allowing the organization to expand and integrate new entities without compromising security. This scalability is essential for supporting growth through acquisitions.

## Protecting Shareholder Value

**Financial impact:** Present data on the financial impact of breaches originating from acquired entities. Explain how zero trust mitigates these risks, protecting shareholder value and ensuring a smooth, secure integration process.

**Confidence in growth:** Communicate that a robust zero trust strategy not only protects the organization's current assets but also supports future growth by providing a secure foundation for acquisitions.

### Conclusion

Effectively presenting the case for zero trust to the board involves clearly articulating the strategic, financial, and risk mitigation benefits. By focusing on risk reduction, cost/benefit analysis, and M&A considerations, CXOs can demonstrate the value of zero trust in safeguarding the hospital's brand, reducing costs, and supporting growth. There is a companion book you may also be able to deliver to your board members to help understand zero trust and its benefits: *Cybersecurity: Seven Steps for Board of Directors* (see Additional Resources).

## Building Support with Department Leaders and Other Stakeholders

Implementing a zero trust architecture in a hospital environment is not just an IT initiative—it requires the engagement and support of various internal stakeholders and business owners. Successfully selling the concept of zero trust internally involves clear communication, demonstrating value, and addressing specific concerns of different departments. This chapter section focuses on strategies for engaging internal stakeholders and business owners to ensure a cohesive and supportive approach to zero trust implementation.

### Identifying Key Stakeholders

The first step in selling zero trust internally is to identify the key stakeholders and business owners whose support and buy-in are crucial for successful implementation. These typically include:

**Executive leadership (CXOs):** The CEO, CFO, CIO/CDIO, CMIO, CMO, CNO, and other senior executives who are responsible for the overall strategic direction and financial health of the hospital.

**IT department:** The CIO/CDIO, CTO, CISO, IT managers, and IT staff who will be responsible for implementing and maintaining the zero trust architecture.

**Clinical leadership:** Heads of clinical departments, including Chief Medical Officers, Chief Nursing Officers, department heads, and senior clinicians.

**Compliance and legal teams:** Professionals responsible for ensuring the hospital meets regulatory and legal requirements.

**Human resources (HR):** HR leaders who will need to manage the impact on staff training and adherence to new security protocols.

### Communicating the Vision and Benefits

To gain the support of these stakeholders, it is essential to clearly communicate the vision and benefits of zero trust. Tailor the message to address the specific concerns and priorities of each group.

### Executive Leadership

**Strategic alignment:** Explain how zero trust aligns with the hospital's strategic goals, such as enhancing patient care, improving operational efficiency, and safeguarding the hospital's reputation.

**Risk mitigation:** Highlight the importance of zero trust in mitigating risks associated with data breaches, regulatory non–compliance, and cyberattacks.

**Financial benefits:** Emphasize the cost savings and economic value of zero trust, demonstrating how it enables the hospital to do more with less by streamlining security processes and reducing inefficiencies.

### IT Department

**Technical advantages:** Discuss the technical benefits of zero trust, such as improved network security, enhanced visibility, and streamlined access management.

**Simplified management:** Highlight how zero trust simplifies security management through automation and continuous monitoring, freeing up IT resources for other strategic initiatives.

**Support and training:** Reassure the IT team that they will receive comprehensive training and support throughout the implementation process. These teams may also benefit from reading the additional book: *Seven Elements of Highly Successful Zero Trust Architecture* (see Additional Resources).

### Clinical Leadership

**Patient safety and care:** Emphasize how zero trust enhances patient safety by protecting sensitive health information and ensuring continuous access to critical systems.

**Operational continuity:** Explain how zero trust minimizes disruptions and outages, allowing clinicians to focus on providing high-quality patient care.

**Ease of use:** Address any concerns about the complexity of new security measures by demonstrating how zero trust solutions, such as single sign-on (SSO) and multifactor authentication (MFA), improve the user experience.

### Compliance and Legal Teams

**Regulatory compliance:** Highlight how zero trust helps the hospital meet regulatory requirements, such as HIPAA, by ensuring robust access controls and continuous monitoring.

**Audit readiness:** Explain how zero trust provides detailed logs and reports, making it easier to demonstrate compliance during audits.

**Data protection:** Reassure compliance and legal teams that zero trust provides comprehensive protection for sensitive patient data, reducing the risk of data breaches and legal liabilities.

### Human Resources (HR)

**Training and awareness:** Discuss the importance of staff training and awareness programs to ensure that all employees understand and adhere to new security protocols.

**Change management:** Highlight the role of HR in managing the cultural shift towards a zero trust mindset and ensuring that staff are supported throughout the transition.

**Employee experience:** Emphasize how zero trust solutions, such as SSO, can enhance the employee experience by simplifying access to applications and reducing password fatigue.

## Building a Business Case

To secure buy–in from internal stakeholders and business owners, it is essential to build a strong business case for zero trust. This involves:

**Cost–benefit analysis:** Conduct a thorough cost–benefit analysis to demonstrate the financial value of zero trust. Compare the costs of implementation with the potential savings from reduced breaches, lower capital and operational expenditure, improved efficiency, and compliance with regulatory requirements.

**Risk assessment:** Perform a risk assessment to identify the potential risks and vulnerabilities in the current security infrastructure. Use this assessment to highlight the importance of zero trust in mitigating these risks.

**Case studies and success stories:** Share case studies and success stories from other hospitals or healthcare organizations that have successfully implemented zero trust. This provides tangible evidence of the benefits and feasibility of zero trust.

**Pilot programs:** Propose a pilot program to demonstrate the effectiveness of zero trust in a controlled environment. Use the results to build confidence and support for a broader rollout.

## Creating a Collaborative Approach

Engaging internal stakeholders and business owners requires a collaborative approach that involves regular communication, feedback, and collaboration. Here are some strategies to achieve this:

**Create a steering committee:** Establish a steering committee comprising representatives from key stakeholder groups. This committee can provide oversight, guidance, and support throughout the zero trust implementation process.

**Perform regular updates:** Provide regular updates to all stakeholders on the progress of the zero trust implementation. Use these updates to highlight successes, address challenges, and gather feedback.

**Have workshops and training sessions:** Conduct workshops and training sessions to educate stakeholders about zero trust principles, technologies, and best practices. Use these sessions to address concerns and build a shared understanding of the benefits.

**Open the door for feedback:** Create feedback mechanisms, such as surveys or focus groups, to gather input from stakeholders and address any concerns or suggestions they may have.

### Conclusion

Successfully selling zero trust internally requires a clear and compelling vision, tailored communication, and a collaborative approach. By addressing the specific concerns and priorities of different stakeholder groups and demonstrating the strategic, operational, and financial benefits of zero trust, CXOs can build the support and momentum needed for a successful implementation. Additionally, CXOs have access to the accompanying book: *Seven Questions Every CXO Must Ask About Zero Trust* (see Additional Resources).

## Addressing End-User, Clinical, and Radiology Concerns Head-On

Implementing a zero trust architecture in a hospital setting requires not only technical acumen but also the ability to effectively communicate its benefits and address concerns across various stakeholders. Users, clinicians, and radiologists each have unique perspectives and potential apprehensions about such a significant shift in security strategy. This chapter section provides guidance on how to address these concerns and garner support for zero trust within the organization.

### Addressing Concerns of Users

**Concern:** Increased complexity and inconvenience
**Response:** A common concern among general users is that enhanced security measures will complicate their workflows and make it more difficult to access necessary resources. It's essential to highlight how zero trust, when implemented correctly, actually simplifies access through solutions like SSO and MFA.

## KEY POINTS TO COMMUNICATE:

**Ease of access:** SSO allows users to access multiple applications with a single set of credentials, reducing the number of passwords they need to remember.

**Enhanced security with convenience:** MFA adds an extra layer of security without significantly complicating the login process. Modern authentication methods, such as biometrics, tap–and–go or push notifications, are user–friendly and quick.

**Seamless experience:** Emphasize that zero trust is designed to work in the background, providing robust security while ensuring that users can continue their work without interruption.

**Concern:** Training and adaptation
**Response:** Users may be concerned about the need for extensive training and the time required to adapt to new security protocols. Address these concerns by providing a clear training plan and demonstrating the intuitive nature of the new tools.

## KEY POINTS TO COMMUNICATE:

**Comprehensive training:** Offer detailed training sessions and resources to ensure users understand how to use new systems effectively.

**User support:** Provide ongoing support and a helpdesk to assist users with any issues they encounter during the transition.

**Gradual rollout:** Implement the zero trust model in phases, allowing users to adapt gradually rather than being overwhelmed by sudden changes.

## Addressing Concerns of Clinicians

**Concern:** Impact on patient care
**Response:** Clinicians are primarily concerned with how security measures might impact their ability to provide timely and efficient patient care. It's critical to reassure them that zero trust enhances security without hindering their workflows.

KEY POINTS TO COMMUNICATE:

**Uninterrupted access:** Zero trust ensures that clinicians have continuous, secure access to patient records and clinical applications, regardless of their location.

**Improved response times:** By reducing the risk of breaches and system downtimes, zero trust actually improves the overall reliability of IT systems, leading to fewer disruptions in patient care.

**Patient safety:** Emphasize that robust security measures protect patient data from unauthorized access, thereby safeguarding patient privacy and enhancing trust in the hospital.

**Concern:** Balancing security and usability
**Response:** Clinicians may worry that stringent security protocols will complicate their already demanding workflows. Address these concerns by demonstrating how zero trust can be seamlessly integrated into their daily routines.

KEY POINTS TO COMMUNICATE:

**Streamlined processes:** Highlight how technologies such as SSO and role-based access control streamline access to necessary information without compromising security.

**Flexibility:** Zero trust allows secure access from any device and location, providing clinicians with the flexibility to work efficiently, whether they are on-site or remote.

**Minimal disruption:** Reassure clinicians that the implementation process will be managed carefully to minimize any disruption to their day-to-day activities.

## Addressing Concerns of Radiologists

**Concern:** Access to large data files
**Response:** Radiologists frequently work with large medical images and data files. They may be concerned that zero trust will slow down access to these critical resources.

### KEY POINTS TO COMMUNICATE:

**Optimized performance:** Explain that zero trust solutions are designed to optimize network performance and ensure that large data transfers are secure and efficient.

**Reliable access:** Zero trust provides reliable, uninterrupted access to medical imaging systems, ensuring that radiologists can quickly retrieve and analyze images.

**Data integrity:** Emphasize that zero trust protects the integrity of medical images and data, ensuring that they cannot be tampered with or accessed by unauthorized individuals.

**Concern:** Specialized software and tools
**Response:** Radiologists often use specialized software and tools that are integral to their diagnostic processes. They may worry that these tools will be affected by new security measures.

### KEY POINTS TO COMMUNICATE:

**Compatibility:** Ensure that all specialized software and tools are compatible with the zero trust framework. Conduct thorough testing and provide assurances that their workflows will not be disrupted.

**Vendor collaboration:** Work closely with software vendors to ensure that security protocols are integrated smoothly and that any potential issues are addressed proactively.

**Continuous support:** Offer dedicated support to radiologists to address any technical issues that arise, ensuring that they can continue their work without interruption.

## Conclusion

Successfully implementing zero trust in a hospital requires addressing the concerns of diverse stakeholders, including users, clinicians, and radiologists. By clearly communicating the benefits, providing comprehensive training and support, and demonstrating how zero trust enhances security without disrupting workflows, CXOs can build a strong case for zero trust adoption.

Gaining the support and buy-in of these key groups is essential for a smooth transition and the long-term success of the zero trust initiative. As we continue to explore the principles and implementation of zero trust, it becomes increasingly evident that addressing stakeholder concerns is a critical step in achieving a secure, resilient, and efficient hospital environment.

CHAPTER 7

# Final Thoughts

As we reach the end of this exploration into the transformative potential of a zero trust architecture in healthcare IT, it's important to reflect on the critical insights and strategies discussed. The healthcare industry stands at a pivotal moment where the integration of advanced security frameworks can fundamentally improve patient care, safeguard sensitive information, and streamline operations.

## Recap of Key Points

Throughout the book, we've navigated the complexities and benefits of adopting a zero trust approach in the healthcare sector. Here are the key takeaways:

- **Improved patient safety and care outcomes:** Cyber care is patient care, as implementing zero trust ensures patient information is protected at every access point, reducing the risk of breaches that can deeply impact patient outcomes, and ensuring compliance with stringent regulatory standards.
- **Heightened operational efficiency:** Zero trust models streamline IT operations by simplifying network structures and enhancing transparency, enabling more efficient management of resources and workflows.
- **Scalability and flexibility:** The modular nature of zero trust allows healthcare organizations to scale their IT infrastructure seamlessly, adapting to evolving technological needs and patient care demands.
- **Enhanced user experience:** By providing seamless, fast and secure access to necessary resources, zero trust enhances the experience for both healthcare providers and staff, fostering a more responsive and effective care environment.

In summary, the adoption of a zero trust architecture in healthcare IT is not just a security measure, but a comprehensive approach to modernizing and optimizing the entire healthcare delivery system.

## The Future of Healthcare IT with Zero Trust

Looking ahead, the future of healthcare IT is intricately linked with robust security frameworks like zero trust. As the digital landscape continues to evolve, the need for a security model that can adapt to new threats and operational changes is paramount. Zero trust stands out by offering a proactive stance on security, one that continuously verifies and validates every access request, regardless of where it originates.

The integration of zero trust with emerging technologies such as artificial intelligence, machine learning, and the Internet of medical things (IoMT) will further revolutionize healthcare delivery. These technologies, supported by a zero trust framework, will enable more accurate diagnostics, personalized treatment plans, and real-time monitoring of patient health, all while ensuring the highest standards of data security and privacy.

## Call to Action for Healthcare CXOs

For healthcare CXOs, the imperative to modernize IT infrastructure and security with a zero trust architecture is clear. The stakes are higher than ever, with cyberthreats becoming increasingly sophisticated and the demand for secure, efficient healthcare delivery growing.

- **Evaluate your current security posture:** Conduct a thorough assessment of your existing IT infrastructure and security measures to identify risks and areas for improvement.
- **Develop a strategic plan:** Create a comprehensive roadmap for implementing zero trust, including timelines, resource allocation, and key milestones.
- **Invest in training and education:** Ensure that your IT staff and healthcare providers are well-versed in zero trust principles and practices, fostering a culture of security awareness and proactive defense.
- **Leverage advanced technologies:** Integrate emerging technologies that complement zero trust, enhancing your organization's ability to provide cutting-edge care while maintaining robust security.
- **Engage with stakeholders:** Collaborate with all stakeholders, such as the board and clinical leaderships, to ensure a smooth transition to a zero trust architecture and to address any concerns or challenges that may arise.

By taking these steps, healthcare CXOs can lead their organizations into a future where security and efficiency go hand in hand, ultimately delivering better patient outcomes and a more resilient healthcare system.

In closing, the journey towards a zero trust architecture is not just a technological upgrade; it's a fundamental shift towards a more secure, efficient, and patient-centric healthcare environment. As the Department of Health & Human Services reminds us, "cyber care is patient care." Embrace this change, and lead your organization into a future where healthcare IT is both innovative and impervious to the ever-evolving landscape of cyberthreats.

# Additional Resources

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

**Seven Questions Every CXO Must Ask About Zero Trust**

**CXO Revolutionaries**

Created for CXOs by CXOs. Learn from IT leaders bringing a new wave of cloud- and mobile-first technology to major enterprises globally. The website publishes the latest insights by digital transformation pioneers and thought leaders.

**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**

Tamer Baker (Zscaler CTO, Healthcare, Government & Education) and David Anderson (Zscaler Senior Director, Transformation Architecture) bring a wealth of expertise and innovation to the forefront of cybersecurity. With extensive backgrounds in companies such as Cisco, VMware, Forescout Technologies and the Department of Defense, their combined experience spans over two decades in the industry. Tamer's strategic vision in healthcare, government, and education sectors and David's deep knowledge in transformation architecture have been instrumental in driving advancements in cloud security and zero trust architecture. Together, their thought leadership and practical insights make them key figures in shaping the future of secure digital transformations in healthcare.

**Special Thanks**

We sincerely thank Cris Ross for his compelling foreword and Drex DeFord for his invaluable feedback and insights during the book's development. We greatly appreciate the time they dedicated and the perspectives they shared.

# What industry leaders are saying:

*"This easy-to-digest book for healthcare technology and business leaders provides a clear and compelling overview of zero trust and a roadmap for how to get started and make a case for zero trust. For business leaders frustrated by the cost of defending against crime and vandalism, this book describes how zero trust has the promise to not only improve security but also to improve user experience."*

**Cris Ross, Former CIO, Mayo Clinic**

*"While zero trust might be a difficult task to accomplish in a hospital environment, this book provides a very methodical approach to understanding and applying the concepts within the enterprise."*

**Christian AbouJaoude, Associate CIO & CTO, Keck Medicine of USC**

*"Cybersecurity in healthcare is not a challenge CISOs can face alone. **Zero Trust Hospital: The CXO Vision** lays out an understandable and actionable starting point to bring an organization together through a zero trust transformation."*

**Nate Couture, Network AVP – CISO, The University of Vermont Health Network**

*"Kudos to the **Zero Trust Hospital: The CXO Vision** for bringing timely health sector awareness and education around the benefits of zero trust, its ability to shrink attack surface, improve identity management, and appropriately segment critical assets in what should become an imperative to safeguarding critical infrastructure healthcare."*

**Carter Groome, CEO, First Health Advisory, CHIME Foundation Board Member**

*"Digital transformation brings with it a lot of known and unknown risks — we need to do everything possible to insulate ourselves and our patients from that risk — Zero trust isn't just a marketing phrase, it's a real strategy that can help us create better, faster, cheaper, SAFER, easier-to-access care for patients and families."*

**Drex DeFord, President, This Week Health, Former Industry CIO**

*"As organizations who care for people in their most vulnerable moments, we make an implicit contract – a commitment – that not only will we ensure the highest quality of care, but deliver this with confidence that everything you share with us remains secure. **Zero Trust Hospital** is an impeccable resource for all CXOs desiring to fulfill this promise."*

**Edward Marx, CEO, Marx Advisory & Former Industry CIO**