



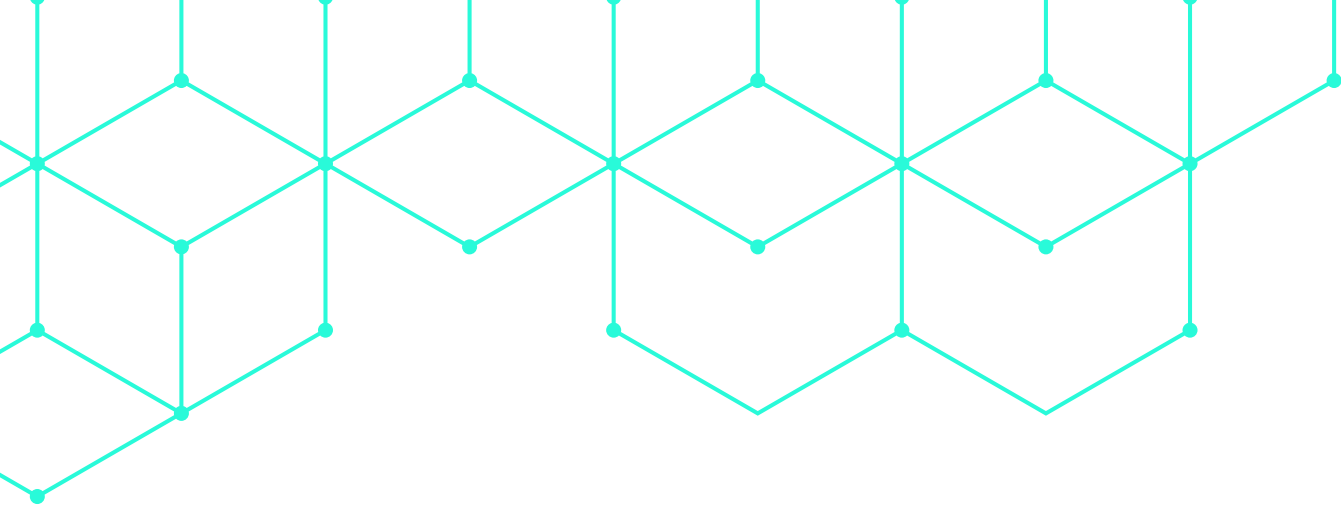
Cyber
Insurance
Academy



Zero Trust & Cyber Insurance

A crash course for the cyber insurance industry





Cyber insurance is a method for organizations to transfer a portion of their liability for cyber risks based on their overall cyber risk management strategy and active mitigations in place. Zero trust security, properly deployed, can provide organizations with better cyber hygiene by improving cyber risk mitigation structures, limiting claims, and reducing the potential for financial loss from cyber-related incidents

This guide, created in conjunction with Zscaler, Inc., will serve as an introduction to zero trust principles, how zero trust differs from traditional IT security practices, and how this risk mitigation approach can benefit policyholders and the cyber insurance industry.

*The **Cyber Insurance Academy** is a 24/7 academy designed to build and expand cyber knowledge in the insurance sector. Our Certified Cyber Insurance Specialist (CCIS) training is accredited by the Chartered Insurance Institute (CII).*

www.cyberinsuranceacademy.com

***Zscaler**, creator of the Zero Trust Exchange™ platform, uses the world's largest security cloud to make doing business and navigating change a simpler, faster, and more productive experience.*

www.zscaler.com



Contents

- The evolution of zero trust
 - A changing digital landscape
 - What is zero trust?
 - How zero trust addresses common security issues
 - Zero trust: No passing fad
- Zero trust and the policy creation process
 - Cyber underwriting with zero trust: What brokers should know
- Conclusion
- Common Zero Trust Terminology Defined

The evolution of zero trust

A changing digital landscape

Technological advances, the growth in cloud computing, and a shifting preference for remote work, largely over the past decade, have profoundly changed how organizations are forced to consider their own digital risk exposure. The most popular business and productivity applications like Office 365, Salesforce, and ServiceNow now reside in “the cloud” – a nebulous term for computing resources at least partially owned and operated by a third party and governed by a [shared responsibility model](#) for secure use.

Employees and third-party individuals who work with an organization are increasingly away from the office for at least a part of the work-week, accessing the organization's sensitive data from numerous locations and devices (personal laptops, phones, etc.).



"An explosion of groundbreaking innovations in recent years – 5G technology, AI and machine learning, the primacy of the cloud – have made necessary a rethinking of the way we conduct business and secure it."

***Kavitha Mariappan,
EVP, Customer Experience & Transformation, Zscaler***

As COVID-19 made remote work a necessity for many workers and the most popular business and productivity applications migrated to the cloud, it has become increasingly risky in how organizations are routing their users and data.

As technologies advanced prior to COVID-19 and organizations quickly adapted to maintain competitive advantage, holistic cybersecurity wasn't always a core focus. Instead, organizations largely focused on protecting their most glaring gaps. Vulnerabilities emerged when security solutions failed to catch up to these new ways of working.

Meanwhile, adversaries were growing more formidable. State-backed groups are increasingly sophisticated and well-resourced. They are often enlisted to conduct corporate espionage, disrupt business operations, launch reconnaissance, or even damage critical infrastructure. Hacking tools, known as exploit kits, are also now widely available and inexpensive for unaffiliated hackers to purchase on the dark web.

These factors have created an environment where breaches abound, risks from cyberattacks are increasingly severe, and regulatory scrutiny can be severe.



Notable cyber attacks involving lateral movement

Target vertical

Retail

Damage

~40M credit & debit records stolen

Attack vector

Compromised third-party contractor

Cost

\$18.5 million USD in fines

Target vertical

Energy infrastructure

Damage

Six-day business disruption, state of emergency declared

Attack vector

Legacy VPN and stolen credentials

Cost

\$4.4 million USD ransom (partially recovered)

Target vertical

Technology

Damage


Stolen account information belonging to ~57M customers and employees

Attack vector

Compromised third-party source code repository

Cost

\$148 million in fines, CSO convicted of obstructing investigation



According to the Zscaler ThreatLabz threat research team, ransomware attacks increased by 80% between February 2021 and March 2022 compared to the previous year, setting new records for both the volume of attacks and the cost of damages.

What is zero trust?

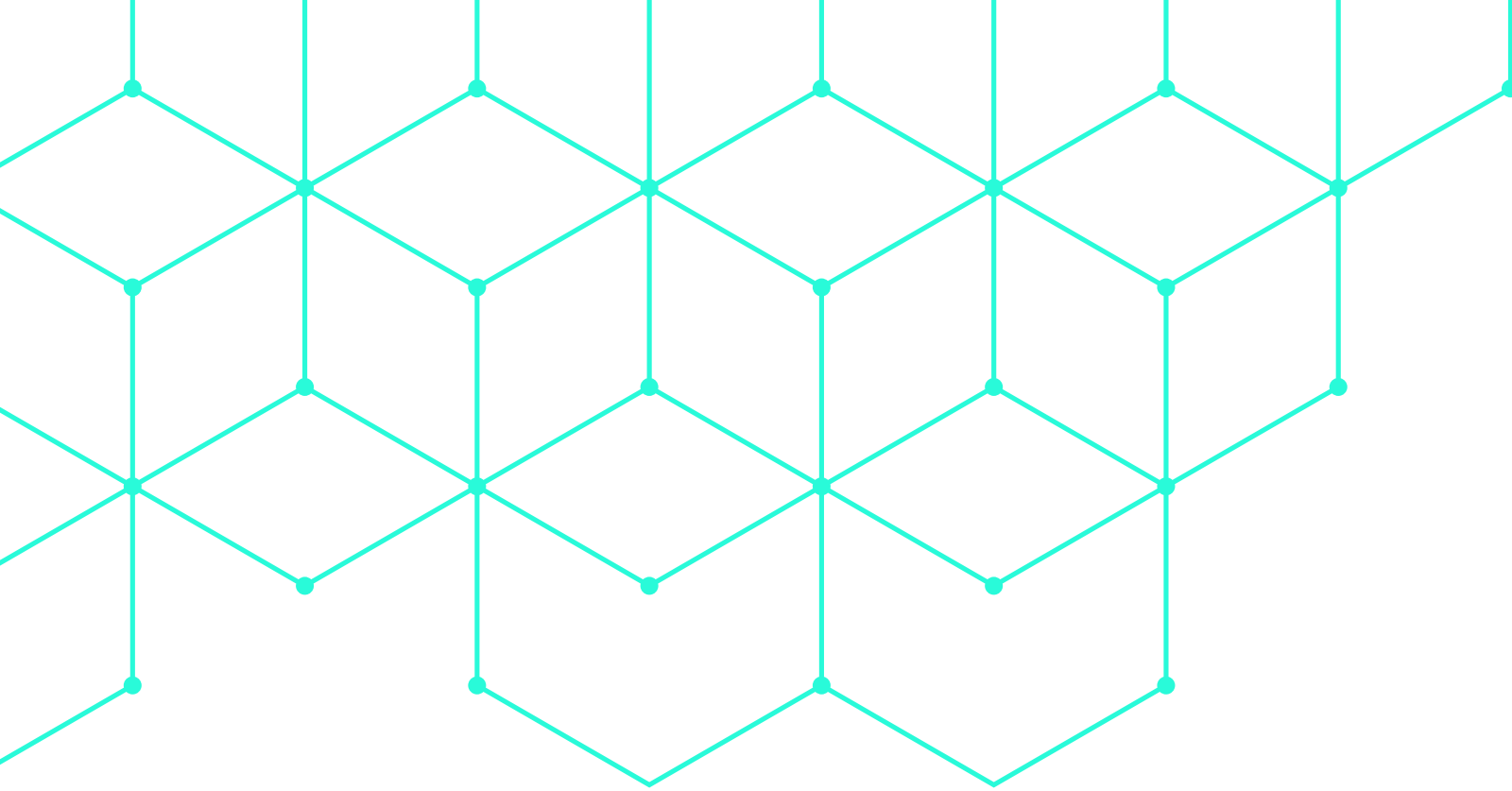
The National Institute of Standards and Technology (NIST) [defines](#) the thinking underpinning zero trust architecture as “no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).” Put another way, “Never trust. Always verify.”

It’s important to remember that zero trust is not a single solution. Instead, it is a set of principles that reassigns security focus from network access (where valuable company data resides) to identity access management (IAM), ensuring no access request is granted by default. A true zero trust ecosystem relies on best-of-breed security vendors for responsibilities, including identity verification, endpoint security for devices like laptops, and security policy enforcement. All have a part to play in ensuring that only the right users have access to the right resources and only under the correct conditions.

That said, many vendors today choose to map their solutions' capabilities onto this zero trust framework because of how it is now widely seen to enhance overall security for users and applications (see Cyber Underwriting for more).

Zero trust, defined:

- *Never trust. Always verify.*
- *Allow access only as needed.*
- *Always verify the user's identity, what they are trying to access, and the context surrounding the request*
- *Lock down access to the organization's "crown jewels" (i.e., most valuable assets)*
- *Limit potential intruders' ability to move around within your organization's network*
- *Prevent cybercriminals from being able to discover your online assets via the open internet*



This approach treats all data movement, user connections, and internal & external interactions with the company data as hostile. Any communications between users, company applications, and protected data are permanently blocked until validated by identity-based policies. An identity-based policy might say, "You are a member of our finance team, and hence need access to QuickBooks," or "You belong to the marketing department and therefore can access Marketo."

Zero trust security can also evaluate the context surrounding an access request. Contextual analysis may determine, "This user does not usually log in at midnight on Sunday, we'd better examine this request carefully," or "We don't have a company presence in this region; perhaps we shouldn't grant access to internal resources."

The critical distinction between an organization taking a zero trust approach versus one that does not is that the latter typically focuses on enforcing security policies only at the perimeter of a company's assets, allowing for one single breach into the organization to have the potential for complete data access and loss. Meanwhile, when deployed correctly, zero trust locks down the entire organization's data and assets and heavily monitors access, data visibility, movement, and activity deemed suspicious.

The term "zero trust" was coined in 2010. But the push to move away from perimeter-based security is older than that. [Click here](#) for a brief look at the origins of zero-trust thinking.

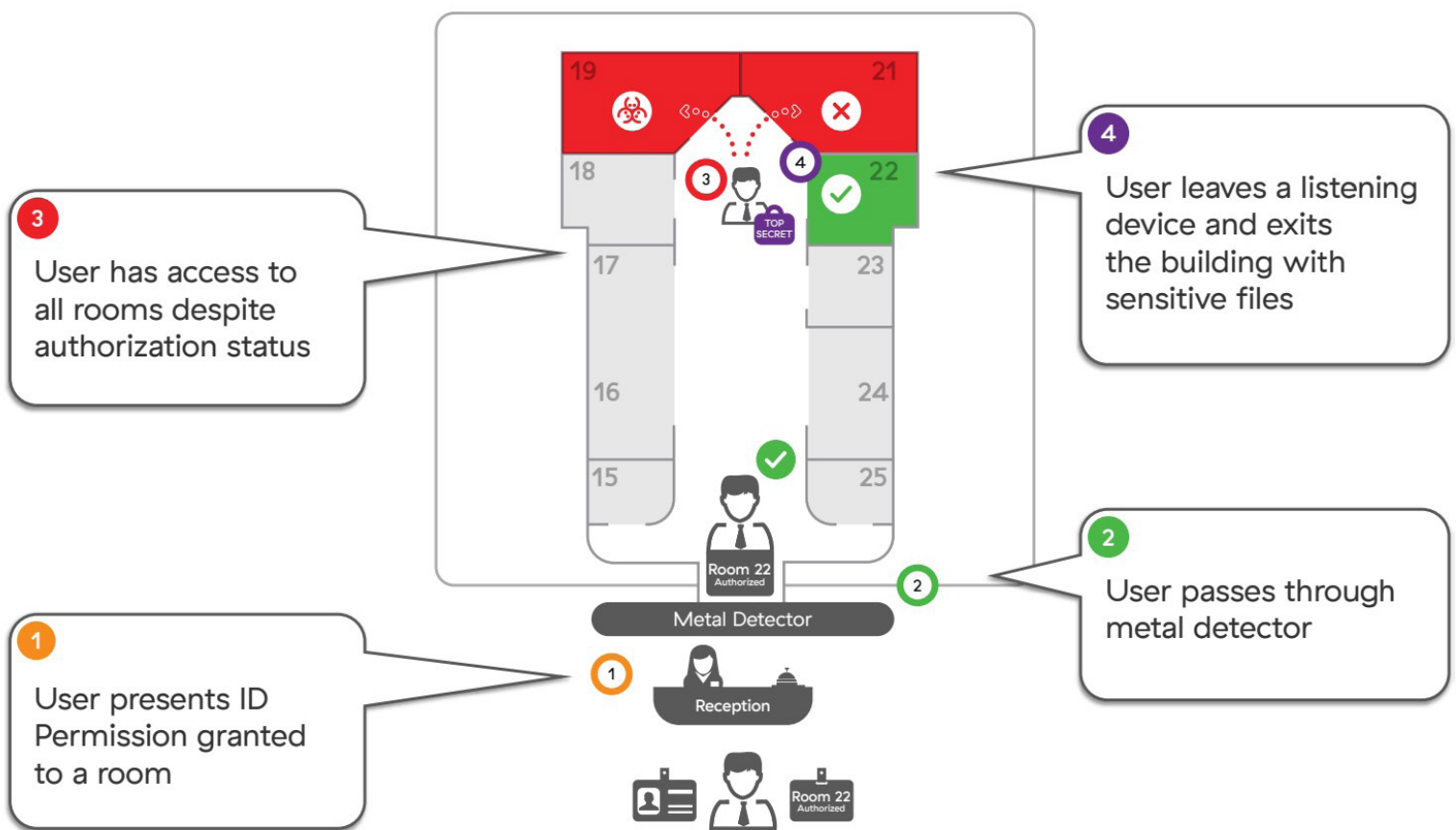
How zero trust addresses common security issues

For decades, cybersecurity controls have focused on enforcing protection at the network's perimeter, akin to building a giant wall around any assets of value. We call this "castle-and-moat" security. The issue with this approach is that once castle walls are breached, cybercriminals have more or less free reign to roam the network they've just infiltrated – nothing on the inside is fully protected any longer.

In the typical cyber incident attack chain, a threat actor will:

- 1. Discover the attack surface – Often a trivial step for cybercriminals, any IP address that resolves to the open internet is discoverable. This could be a printer, internet-enabled machinery, VPN, or personal computer on the corporate network.*
- 2. Gain entry through initial compromise – This can be done by entering a user's stolen credentials, exploiting an unpatched vulnerability, or by taking advantage of a previously unknown vulnerability.*
- 3. Move laterally to locate valuable resources – Once on a network, cybercriminals begin to snoop around for valuable data like intellectual property or payment information.*
- 4. Exfiltrate data for extortion or sale – Once it's located, data can either be encrypted and held for ransom or stolen and sold on the dark web.*

Imagine a guest arrives at a company's headquarters for a scheduled meeting. The visitor checks in at reception, proves his identity by providing ID, passes through a metal detector, and is then admitted to the building.



In cybersecurity, this ability to wander unchecked through an environment is known as "lateral movement." Cybercriminals rely on lateral movement to locate valuable company data once they've bested perimeter-based defenses.

In legacy networking

Our visitor is able to monitor the building from the outside before deciding how to gain entrance

Once the visitor has access to HQ, he is able to travel to other buildings on the business's campus without additional security checks.

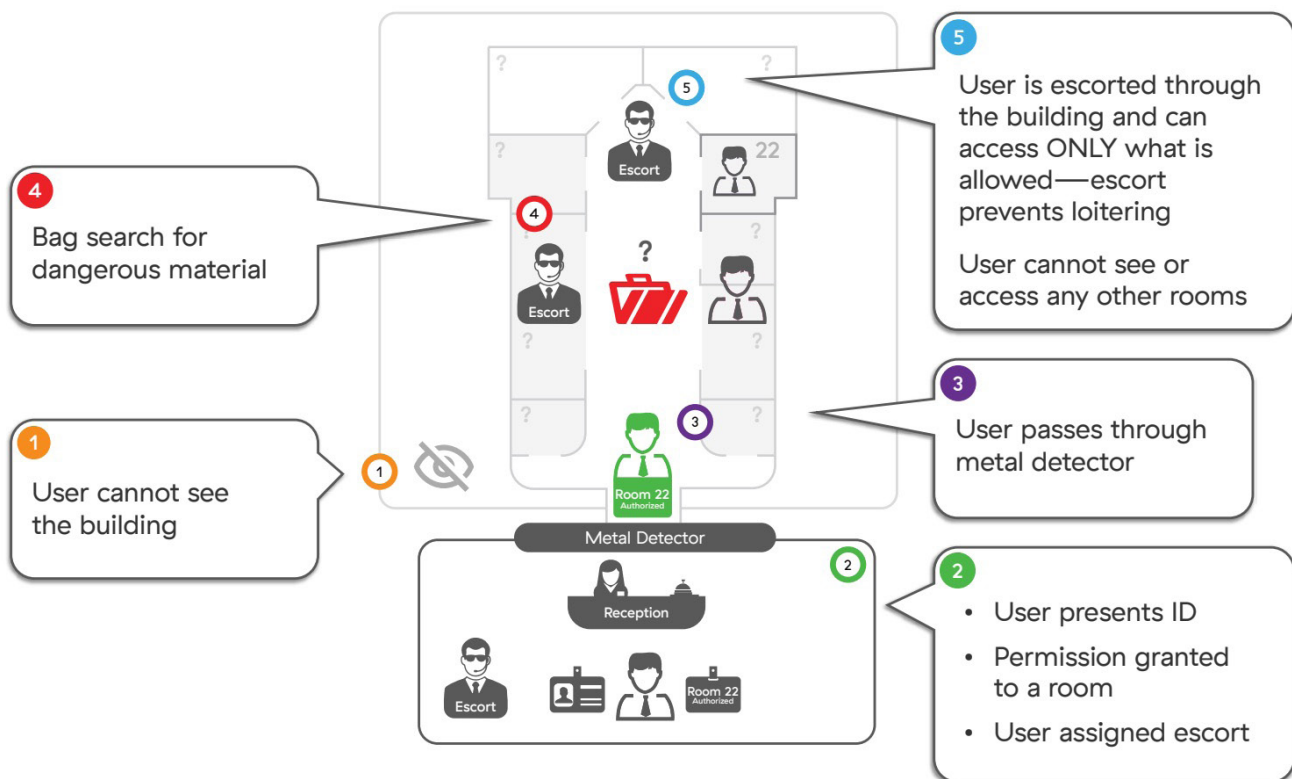
The sly visitor knows he only needs to bypass the receptionist to gain entry into the building.

With zero trust

All signage is removed from the building, and its location is scrubbed from the internet, so the visitor doesn't know the location of the building until his identity is verified

Doors to rooms are locked, so the user can only access the room of his scheduled appointment.

The receptionist works from a third-party site, so visitors are not certain which building she controls access to.



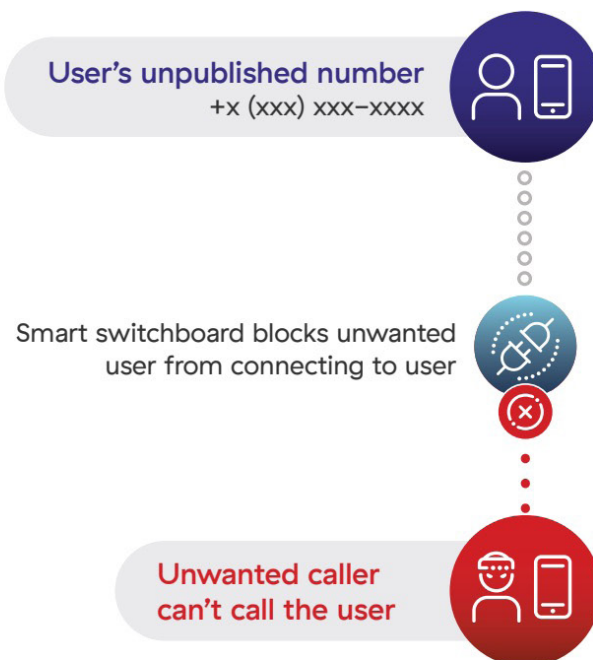
With zero trust, visitors still check in at reception, have their ID verified, and receive a badge. But this time they will also be escorted to their specific room (direct to resource connections). Before the visitor enters the room, their luggage is checked for dangerous material (malware). If it checks out, the visitor is escorted directly to their specific, authorized meeting room with no option to enter any other (lateral movement prevention). Once the meeting is over, the visitor is escorted out. Before the visitor exits, however, their suitcase is checked for any stolen goods (data loss prevention).

This is how zero trust addresses the common security issue of lateral movement. Next, let's look at how it can stop cybercriminals from finding protected resources entirely, a practice known as managing the "attack surface."

A user with a **published** phone number



A user with an **unpublished** phone number



To understand attack surfaces and how zero trust helps manage them, let's journey back in time to the days of phone books and switchboards. Imagine Sue has a publicly available phone number anyone can use to reach her. This is good in the sense that Sue's friends can look her up and give her a ring anytime they'd like. Unfortunately, it's also easy for scammers and thieves to find her as well.

It would be better for our user to hide her number behind an intelligent switchboard. This switchboard could broker connections between Sue and an approved list of contacts. With zero trust, all connections between users, apps, and OT/IoT devices are routed through this intelligence switchboard, or security cloud, where permissions can be checked and security policies applied.

In legacy networking

Sue's phone number is publicly available so her friends and scammers can reach out to her at any time.

Callers are put through to Sue, regardless of whether or not they are authorized to contact her.

With zero trust

Sue's phone number is hidden behind a trusted, intelligent switchboard hosted in the cloud and unavailable publicly.

Callers with the correct permissions are patched through by the switchboard, while those without the correct permissions are dropped.

Another important differentiator of zero trust to note is that it is a framework rather than a product. It's a way of thinking about a number of security and networking disciplines. No single vendor sells "zero trust." Instead, they build products that satisfy core principles of zero trust, such as no connection shall be established until the requestor's identity is verified. Once implemented, zero trust secures users, things (smart devices), and workloads (communication between apps) to public or private destinations.

Zero trust: No passing fad

Zero trust is catching on, which could benefit both underwriters and policyholders. Implementing zero trust architecture is a priority for IT and security leaders, given the changing landscape discussed above.

Zero trust network architecture can help eliminate the attack surface, prevent compromise, stop lateral movement, and prevent data loss. This leads to fewer cyber incidents, claims, and losses so organizations that have adopted zero trust can reduce their limits and lower their premiums, and carriers are exposed to less risk.

90%

90% of organizations migrating to the cloud have implemented or are implementing a zero trust strategy in the next 12 months

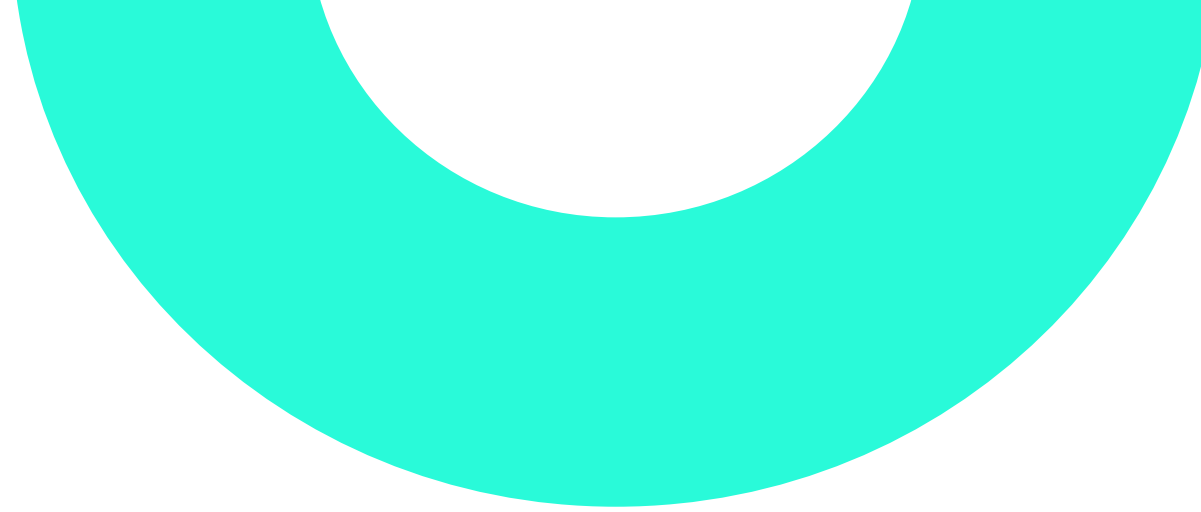
68%

68% of IT leaders agree that secure cloud transformation is impossible with legacy security models

#1

Zero trust network access (ZTNA) is the #1 priority for zero trust technology investment over the next 12 months

Source: The State Of Zero Trust Transformation 2023, Zscaler ([full report here](#))




"Zero trust provides an elevated level of hygiene that can help to mitigate these risks even more effectively and improve underwriting. It can be used in collaboration with cyber insurance providers to identify coverage and potential financial loss."

Stephen Singh, VP, Outsourced Projects and M&A Integration, Zscaler

While, in reality, no one can be 100% certain never to suffer a cyber incident, an adequately deployed zero trust model can also help limit "blast radius." This means it reduces an organization's overall exposure if, say, an employee's laptop were to become compromised. As with legacy security, an attacker can not traverse the entire network from a single compromised device.

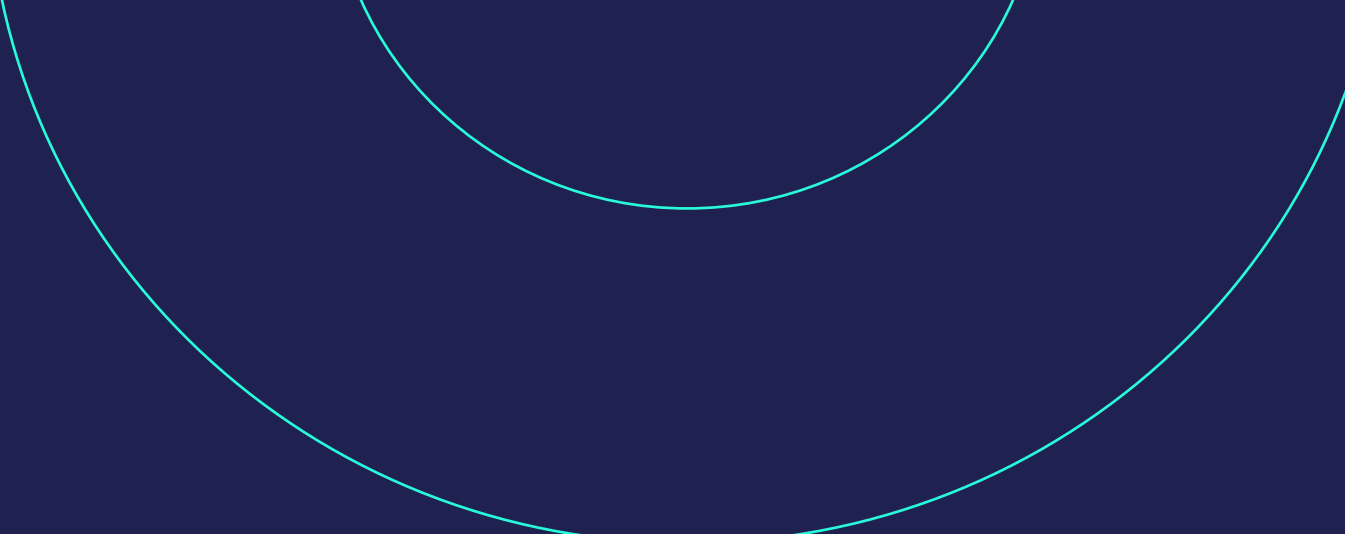
True Story: The CISO of a family of large apparel brands was preparing to renew his cyber insurance policy. Before negotiations, he was uncertain of how to best demonstrate the controls he had initiated to curtail risk. However, his ability to establish inside-out controls for reducing his attack surface and preventing lateral movement allowed him to gain more favorable coverage that was better aligned to his risk profile.



Zero trust and the policy creation process

A number of factors, including a relatively immature market, an overreliance on policies rather than controls, and supply/demand imbalances, have caused cybersecurity premiums to skyrocket in recent years. Surging ransomware and business email compromise tactics have expanded the scope, severity, and speed cyber insurers were forced to pay out.

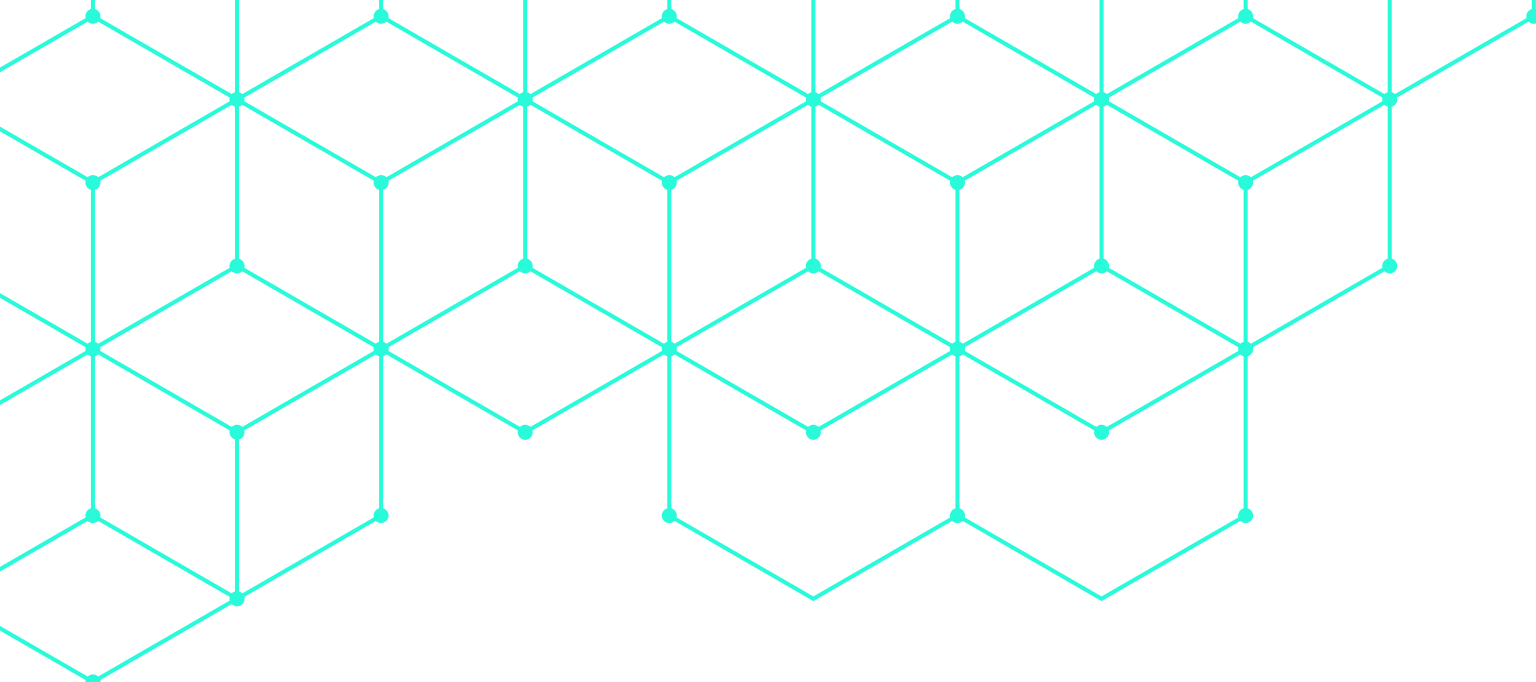
According to [industry reports](#), loss ratios for cyber insurers in 2020 were approximately 70%, up from around 45% in 2019. This, along with recent court rulings, has led many issuers to carve out exemptions for instances of state-sponsored hacking and ransomware. While reports suggest loss ratios [fell](#) in 2021 for the first time in five years, insurers still face a dangerous cyber threat landscape that is unlikely to improve in the face of war in Europe, escalating political tensions,



the profitability of cybercrime, and ever-increasing digitization.

Current cybersecurity policy requirements entail multi-page, check-box questionnaires about mitigation techniques – SIEMs, MFA, firewalls, awareness training – with minimal to no consideration for how they are implemented or administered. "Outside-in" risk assessments are point-in-time, provide limited visibility, and offer no ongoing evaluation of organizations' cyber risk posture.

The ability to monitor real-time information on controls implemented, telemetry data from those controls, and a 360-degree view of the organization's attack surface allows underwriters a far more holistic and up-to-date understanding of the IT estate during policy creation. This "inside-out" view takes a process that was once static and makes it dynamic.



Outside-in analysis

Point-in-time risk assessment	Opaque visibility limits exposure awareness	Ignores access to critical assets (data, systems, applications)	Response and remediation limitations
-------------------------------	---	---	--------------------------------------

Inside-Out analysis

Attack surface exposure assessments	Internet threat exposure analysis	Ransomware and data loss prevention risk assessment	Intelligent signals and analysis
-------------------------------------	-----------------------------------	---	----------------------------------

Rather than prioritizing only the external dimensions of the cyber threat landscape, an inside-out analysis also considers telemetry being generated by the organization's security controls. When evaluated this way, policy creation considers typical cyber hygiene controls plus tenets of zero trust known to reduce the chances of a breach occurring and to limit the damage (blast radius) should one occur.

Hygiene

- Multi-factor authentication (MFA) for remote access and admin controls
- Endpoint Detection and Response (EDR) Secured, encrypted, and tested backups
- Privileged Access Management (PAM)
- Email filtering and web security
- Patch/vulnerability management
- Cyber incident response planning and testing
- Cybersecurity awareness training and phishing testing
- Hardening techniques, including Remote Desktop Protocol
- Logging and monitoring/ network protections
- End-of-life systems replaced or protected
- Vendor/digital supply chain risk management

Hygiene+

- All hygiene controls, plus:
 - Least privileged access
 - Obfuscated attack surface (not discoverable from the open internet)
 - No lateral movement (connect users directly to resources)
 - Eliminate data loss (by preventing the exfiltration of sensitive data)

This type of assessment provides underwriters with a significantly improved understanding of the coverage, limitations, risk, and potential financial loss compared to previous methods. Organizations leveraging advanced zero trust network architecture can more readily prove their enhanced cyber maturity and reduced risk posture on an ongoing basis.

Cyber underwriting with zero trust: What brokers should know

Many underwriters and brokers may wonder how zero trust capabilities map onto their current assessment questionnaires. The honest answer is that it is not a one-to-one relationship. Some zero trust principles address a number of assessment topics, while others fall outside its purview.

To illustrate, here are questions taken from representative questionnaires and responses to their relevance provided by an experienced team of CISOs familiar with both legacy cybersecurity and modern, zero trust approaches.

Cyber Insurance Underwriting Topic Area	Common Cyber Insurance Underwriting Question	Zero Trust Relevance and Application
Account Access	Are administrator accounts separate and distinct from non-privileged accounts?	Zero trust tenants are based on providing least-privilege access to all data and key assets. An organization properly implementing zero trust principles will have clear and transparent account designations for administrators' enhanced access versus minimal access, where rules will differ based on the data and systems. Organizations also have stronger visibility of levels of access using the right zero trust solutions.
Account Access	Do you allow remote access to your network?	Zero trust, by definition, does not allow remote or non-remote access to the network for any users. Remote access is controlled and monitored through a set of rules, policies, and controls. A zero trust organization enhances its security by never allowing blanket network access.
Account Access	Can users access the network with their own device ("Bring Your Own Device")?	Zero trust, by definition, does not grant access to networks regardless of device. Users only access applications directly based on privileged access rules, policies, and controls. Organizations committed to zero trust have the ability to enforce limited access to applications from unmanaged devices, resulting in heightened security.

Cyber Insurance Underwriting Topic Area	Common Cyber Insurance Underwriting Question	Zero Trust Relevance and Application
Account Access	Do employees or third parties have remote access to your OT environment?	Zero trust tenants are based on providing least-privilege access to all data and assets, including OT environments. Zero trust limits the type of visibility and access a user has to OT environments. Access from the OT environment to other company applications or networks is denied by default, preventing illicit access and lateral movement.
Antivirus	Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise?	NGAVs only protect against known threats attacking endpoints, not new or unknown ones. Zero trust organizations augment these capabilities with both endpoint and in-line defenses, behavioral analytics, and heuristics to minimize risk from a broader range of suspected threats.
Antivirus	Are all connecting devices required to have an antivirus installed in accordance with your company policy for updates and patching?	Zero trust principals focus on enforcing connecting devices through means above and beyond antivirus software, by relying on a set of checks unique to each request - who is accessing, what is being accessed, where it is being accessed from, the requestor's permissions, device status, and more. While endpoints like laptops should have antivirus software installed, this is insufficient to provide against the full range of threats facing organizations.

Cyber Insurance Underwriting Topic Area	Common Cyber Insurance Underwriting Question	Zero Trust Relevance and Application
Centralized Management & Controls	Do you actively monitor all administrator access for unusual behavior patterns?	Continuous, active monitoring is a key tenet of zero trust. Admin access, critical data, and other mission-critical assets receive the highest level of scrutiny in terms of behavioral analysis and activity monitoring to detect unusual behavioral patterns when requests for these resources are involved.
Centralized Management & Controls	Do you monitor perimeter network traffic, including internet traffic into and out of your organization?	Monitoring perimeter network traffic, including internet traffic, is a key zero trust principle. Zero trust organizations should have the ability to not only authenticate this traffic but also monitor and inspect analytics on that traffic regardless of encryption status.
Data Loss Prevention	Is critical data encrypted at rest?	Zero trust principles exceed data encryption to include tokenization and controls over data and application access. There are numerous methods used to protect data at rest beyond encryption that better protect against cyber threats. An organization leveraging a proper zero trust strategy will have a more robust data encryption capability in place.

Cyber Insurance Underwriting Topic Area	Common Cyber Insurance Underwriting Question	Zero Trust Relevance and Application
Endpoint Detection and Response (EDR)	Do you use an EDR tool that includes centralized monitoring and logging?	EDR is another critical tenant of zero trust. Organizations employing zero trust properly surpass traditional EDR capabilities by identifying, authenticating, and remediating cyber threats on endpoints.
Encryption	Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? Is electronic data stored in an encrypted format? (i.e. data in servers, laptops, computers, portable media, wireless networks, backup media, etc.)	Zero trust principles exceed encryption to include tokenization and other data access controls. By replacing personal data with random symbols during the tokenization process, that data retains no intrinsic, exploitable meaning or value. Zero trust organizations go beyond encryption to better protect against cyber threats and data loss.
Firewalls	Do you use a commercially available firewall for all your computer systems?	A cornerstone concept of zero trust is that firewalls are ill-suited to securing today's organizations due to the lateral movement they can potentially enable. Rather than enforcing controls only at the perimeter, zero trust states requestors should only be given access to applications, not networks, on a least-privileged basis after identity has been verified.

Cyber Insurance Underwriting Topic Area	Common Cyber Insurance Underwriting Question	Zero Trust Relevance and Application
Multi-factor Authentication (MFA)	Where in your environment is MFA enforced? Do you use MFA to secure all cloud provider services that you utilize (e.g. AWS, Microsoft Azure, Google Cloud) to protect all local and remote access to privileged user accounts?	While important, MFA is only one control that should be used to enforce access to sensitive data. Zero trust principles augment this control by continuously verifying access requirements are met. Proper zero trust solutions add adaptive controls such as behavioral analysis to exceed protection offered by MFA controls.
Privileged Access Management (PAM)	Is the principle of least privilege enforced through technology-based restriction	Least privilege is enforced continuously in zero trust environments. "Never trust, always verify" as a guiding tenet means access controls are applied for each application request, regardless of a user's circumstances or position on the network. A user on an unmanaged device, for example, may have access to public-facing applications, but no internal ones.
Privileged Access Management (PAM)	Do you have a PAM solution in place?	Zero trust based on least privileged access, visibility, and context should utilize a PAM solution provider to support providing administrative access to relevant applications.

Cyber Insurance Underwriting Topic Area	Common Cyber Insurance Underwriting Question	Zero Trust Relevance and Application
Segmentation	Do you utilize segmentation for the purposes of protecting mission-critical or high-value assets or systems? Are your networks and systems segregated as opposed to residing on a flat network?	Segmentation is the practice of dividing up an organization's data that flows inside and outside to other organizations, to reduce and minimize its susceptibility for attacks. Zero trust principles go beyond traditional segmentation to include implementation by least privileged access, therefore reducing the overall attack surface and resulting in advanced segmentation.
Security Information & Event Monitoring (SIEM) & Security Operations Center (SOC)	Is an SIEM tool used to correlate the output of multiple security tools? Do you utilize a SOC?	Monitoring events and key security controls within the organization's cyber environment is a key principle of zero trust. A zero trust organization will have the ability to monitor the security events and output from the control. A SOC is one implementation use case of that 24x7 monitoring capability.

Conclusion

Castle-and-moat-style security worked well when the data center was the heart of the organization. But today, workers have moved off the corporate network and applications have migrated to the cloud, requiring new ways of protecting company assets. Zero trust responds to these new realities by de-emphasizing perimeter-based security, focusing instead on connecting users directly to resources, after and only after verifying identity and enforcing security controls.

By shrinking the attack surface and eliminating lateral movement, zero trust frameworks frustrate the attack chain that currently enables threat actors to cause organizations millions of dollars in damage due to business disruption, extortion by cybercriminals, and fines from regulators. This in turn, can lead to better loss ratios for cyber insurance underwriters and more satisfied clients. Cyber insurers are also better informed about the true nature of an organization's cyber risk maturity, so they can better underwrite and grant policies for those organizations implementing zero trust strategies.

Policyholder benefits

- Controls are easier to demonstrate, so policies are easier to secure
- More favorable terms for policies, including fewer carve-outs
- Reduced or eliminated premium hikes during the renewal process
- Potential to reduce limits as less coverage may be needed

Underwriter benefits

- A more accurate understanding of the types and extent of controls deployed
- Ongoing assurance of compliance by policyholders
- Better loss ratios resulting from addressing common breach enablers

Common Zero Trust Terminology Defined

Attack surface – A measure of an organization's overall risk exposure gained by determining which of its assets are publicly locatable from the open internet.

Attack vector – The means by which a threat actor goes about exploiting gaps in an organization's risk mitigation strategies.

Browser isolation – A method for limiting organizational exposure to threats like data loss by streaming a pixel rendering of a web browser window to a requesting user, due either to that user's risk profile or other policy red flag.

Cloud access security broker (CASB) – A set of tools for ensuring the proper provisioning and configuration of cloud-native assets.

Firewall-as-a-Service (FWaaS) – A network security technology that delivers advanced threat protection capabilities, including access controls, URL filtering, advanced threat prevention, intrusion prevention systems (IPS), and DNS security.

Lateral movement – The ability of a threat actor to traverse a network in light of a successful initial compromise.

Perimeter-based security – A focus on threat prevention at the network's edge, common to decades of IT security thinking but one that is increasingly outdated given the global nature of today's workforce, a preference for the ability to work from anywhere, and the rise in cloud-native business productivity applications.

Sandbox – A security capability focused on isolating potential negative effects of an unknown or uncategorized asset such as a file or application.

Secure Service Edge (SSE) – A Gartner-defined term for a set of solutions that house security enforcement tools, including secure web gateways, CASBs, FWaaS, and others closer to the end user in order to capitalize on performance and usability benefits.

Secure web gateway (SWG) – A security solution used by enterprises to protect employees and users from accessing or being infected by malicious websites and web traffic, internet-borne viruses, malware, and other online cyber threats.

SSL inspection – The practice of intercepting and reviewing SSL-encrypted internet communication between the client and the server.

Zero trust – Zero trust is a framework for securing organizations in the cloud and mobile world, asserting that no user or application should be trusted by default.

Zero trust network access (ZTNA) – Zero trust network access (ZTNA), also known as the software-defined perimeter (SDP), is a set of technologies and functionalities that enable secure access to internal applications for remote users. ZTNA gives remote users secure connectivity to private apps without placing them on the network or exposing them to the internet.



Bringing Cyber Insurance **Down To Earth**

www.cyberinsuranceacademy.com

 @CyberInsuranceAcademy

 @CyberInsAcademy

 @CyberInsAcademy