McGowanPRO

Professional Liability Insurance

Planning for Zero Trust

Zero Trust Defined

Zero Trust is a term that gets a lot of buzz in the cybersecurity world. But what exactly is Zero Trust? To understand Zero Trust, first imagine airport security. To make it through the checkpoint, passengers must be scanned and present their identification and boarding pass. But once through, these passengers have free reign of the airport. This analogy represents the traditional model of cybersecurity, the so-called perimeter defense.

Now imagine that once passengers are through their first security checkpoint, they must go through the entire process again to enter each restaurant or shop and to board their flight (shoes off and all). While this scene might give frequent fliers a panic attack, it also represents how the Zero Trust cybersecurity model works.

The National Institute of Standards and Technology (NIST) defines Zero Trust as:

> "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."

In simplest terms, Zero Trust means just that — no trust is implicitly given to any user, device, application, workload, or data. Every user is assumed to be a bad actor until they can prove otherwise. Even then, they must re-verify once they move to another part of the network or after a certain amount of time has elapsed.

Zero Trust provides unparalleled protection for organizations' sensitive data and significantly reduces the risk of a data breach. However, implementing Zero Trust can be challenging, as it does not reside in any single technology or service provider. And, like the airport example, fully implemented Zero Trust can impede productivity, as users must constantly re-verify and authorize. That's why strategic implementation of Zero Trust across the most vulnerable areas of a company's network and digital real estate is crucial to the strongest security posture possible that does not cause efficiency backlogs.

This e-book will outline the steps organizations need to advance in their Zero Trust journey. It is intended as a reference only. Teams undergoing Zero Trust transformation should seek the advice of cybersecurity experts or experienced third-party technology vendors.

Common Use Cases

Without thoughtful deployment, Zero Trust can drag down organizational efficiency. However, specific use cases make a lot of sense for many organizations. Below is a list of common scenarios in which an organization should begin implementation of Zero Trust architecture as soon as possible:

- **Hybrid work environments** — VPNs can create a backlog of network traffic, while Zero Trust can authenticate identities from anywhere in the world.
- **Multi-cloud remote access** — Gives admin greater control and visibility into cloud operations across environments.
- **IoT device security** — Closes a common backdoor that bad actors can leverage and ensures visibility into device traffic.
- **Micro-segmentation in a data center** — Minimizes damage in the event of a successful breach by separating IT operations into separate zones or "fortresses".
- **Third-party vendors and software supply chains** — Provides "least privilege access" to outside vendors so they only have the permissions they need to accomplish their function and nothing more.
- **Replacing or supplementing a VPN** — VPNs are rapidly becoming obsolete and can no longer defend distributed workforces. However, VPNs can function concurrently with Zero Trust policies to create a more robust security fabric while organizations transition to Zero Trust.
- **Onboarding new employees** — The principle of "least privilege access" (more on this below) allows growing organizations to add new hires quickly without exposing sensitive data.

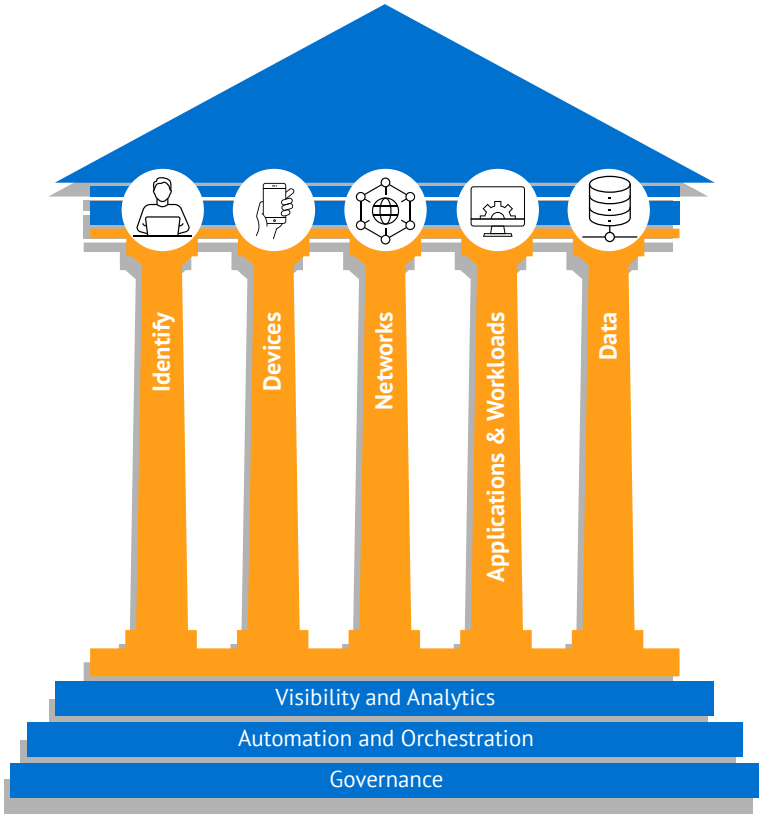
The origins of "Zero Trust"

The term "Zero Trust" was initially introduced by analyst John Kindervag in 2010. However, the concept originates in the "black core" architecture theory of the U.S. Military, which prioritizes the security of individual digital processes over implicit accessibility. The phrase itself comes from the Russian proverb "trust but verify", which gained some infamy as an ironic statement by Ronald Reagan to Mikhail Gorbachev during the Cold War.

Zero Trust initially gained widespread adoption among companies like Google and Akamai. Over the years, it has increasingly become popular among cybersecurity professionals due to market pressures such as high-profile data breaches and the rise of hybrid workforces.

Principles of Zero Trust

NIST identifies five pillars of Zero Trust: Identity, Devices, Networks, Applications and Workloads, and Data. Three cross-cutting capabilities link these pillars: Visibility and Analytics, Automation and Orchestration, and Governance.



Zero Trust can be deployed across each pillar individually or simultaneously.

The Process

Implementing Zero Trust can take several years, as each technology can take months to deploy appropriately. It's best to view Zero Trust as a transformational journey with multiple phases. The overall process looks like this:

1. Create a Zero Trust team
2. Choose an implementation approach
3. Assess the existing environment and security fabric
4. Appraise the appropriate technology
5. Begin implementation
6. Make operational changes
7. Monitor and repeat as necessary

Additionally, CISA defines three levels of Zero Trust maturity for an organization: **Initial**, **Advanced**, and **Optimal**. These maturity levels are measured by the level of automation an organization uses in its security efforts and the degree to which it has integrated Zero Trust into operations.

Step 1. Create a Zero Trust team

Zero Trust is a collaborative effort that requires choosing the right team members. Security teams typically lead and manage Zero Trust initiatives, but if implementing Zero Trust across networking-specific areas first, the networking team should take charge.

Creating dedicated, cross-functional teams to drive implementation efforts is also highly recommended. These teams should include members with expertise in

- user and device identity,
- network and infrastructure security,
- applications and data security,
- and security operations in general.

To fill knowledge gaps and gain specialized expertise, team members can take Zero Trust training courses and certifications from organizations such as (ISC)2, SANS, Forrester, and the Cloud Security Alliance.

Step 2. Choose an implementation approach

Zero Trust has three primary approaches or on-ramps, which focus on different technologies. They are:

- **Identity**
- **Applications and data**
- **Networking**

Zero Trust ultimately encompasses all three approaches when implemented. However, an organization must choose the starting point that makes the most sense for their current environment.

The **Identity** approach includes the following technologies:

- **Biometrics**: Use biometrics such as fingerprints to validate users and tie them to a trust profile.
- **Multifactor authentication (MFA)**: Use MFA to extend trust by tying the user to the device.
- **Identity and access management (IAM)**: IAM provides single-login authentication across cloud platforms and internal systems.
- **Device certification**: Check device configurations to extend trust and ensure applications and operating systems are up to date and properly patched.
- **Zero Trust network access (ZTNA)**: Use ZTNA technology to control access based on user identity, context clues, and enterprise security policies. ZTNA is available as standalone services or as part of broader secure access service edge (SASE) technology and security service edge platforms.

Organizations with many remote users accessing cloud-based applications may find the identity approach a particularly appealing starting point.

An **application and data** approach includes:

- **Data classification**: Associates security levels with specific types of data.
- **Data loss prevention (DLP)**: Tools that track and log access to data. Creates visibility for Zero Trust security teams.
- **Authentication and authorization of microservices**: Foundational for advanced security initiatives, particularly Zero Trust security.
- **Container security**: Automated management and securing of groups of containers.
- **Cross-system integration via APIs**: Integrating various components of a cybersecurity infrastructure with automation.

When working in a cloud environment that prioritizes applications and data protection, it might be beneficial to begin the process by focusing on the applications and data approach.

The **networking** approach includes:

- **Automation**: Automating network controls enables dynamic revocation of authorization mid-session.
- **Micro-segmentation**: Approving data flows based on user and resource type rather than port, IP address, and traffic type enhances security.
- **Stateful Session Management**: This capability allows for individual session management and tracking.
- **Cloud-based firewalls and centrally managed firewalls**: These technologies make implementing and managing zero-trust processes easier.
- **Software-defined WAN and SASE**: These technologies provide network endpoints for zero-trust policies.

If an enterprise has an established internal network with network-based controls and many workloads still being processed in an on-premises data center, then the network approach for Zero Trust can be a suitable solution for them. Additionally, if the network is currently the cybersecurity platform, then it might be a wise decision to upgrade network-based controls to Zero Trust.

Step 3. Assess the existing environment and security fabric

After choosing the appropriate approach, it's vital for Zero Trust teams to consider current security policies and controls. It's possible that aspects of Zero Trust security are already active or lying dormant, waiting to be configured.

The goals of this phase are:

- To locate existing security controls. Based on the lists above, determine what technologies are already operational.
- To determine the gaps. Which technologies must be upgraded, replaced, reconfigured, or added to the environment to move closer to Zero Trust principles?

TechTarget has a helpful cybersecurity audit checklist that teams can reference during this phase.

Step 4. Appraise the appropriate technology

Once your team pinpoints gaps, the next step is to assess which technology can address those gaps. Most modern technology tools are built with Zero Trust architecture in mind. For example, virtualized networking like SD-WAN and SASE features Zero Trust tools like micro-segmentation. Choosing the appropriate technology to advance your organization's Zero Trust journey will depend on your team's chosen approach, technology budget, and timeline for Zero Trust implementation.

Step 5. Begin implementation

At this point, it's time to pull the trigger. Take the necessary steps to ensure that upgrades to infrastructure, systems, and applications minimize the disruptions to your organizational workflow. Monitor new systems during and after implementation to confirm that there are no negative interactions with your system.

Step 6. Make operational changes

As organizations advance in Zero Trust maturity, they necessarily must lean on automated processes. This development means that your team may need to update associated tasks to be automated and update training to reflect the changes.

Step 7. Monitor and repeat as necessary

The key to successful Zero Trust implementation is constant monitoring, evaluating, and configuring Zero Trust technologies to accomplish security objectives. As your organization moves through each pillar of Zero Trust (Identity, Devices, Networks, Applications/Workloads, and Data), your Zero Trust team will undoubtedly gain new insights and experience. It may be necessary to evaluate the steps you have already taken and update them as necessary. And as technology advances, new tools may become available that aid the process.

Managing the Security Journey

Zero Trust, and cybersecurity in general, is not a "set it and forget it" situation. Developments in technology, both for security and for bad actors, continuously drive the search for streamlined approaches to keeping your organization's data safe. But cracks can appear in even the most robust security fabric.

McGowan PRO offers comprehensive Cyber Liability and Data Breach Response Insurance. A successful breach can cost an organization dearly in regard to litigation, fines and fees, and reputational damage. But efforts like Zero Trust, when paired with a Cyber Liability policy, can help to prevent and minimize damage, as well as keep your organization compliant with evolving regulations. Our experienced professionals can guide your path in protecting your organization from economic harm.

Get in touch to learn more about our cyber insurance policies.

McGowanPRO
Professional Liability Insurance

Contact us:

McGowanPRO
150 Speen St., Suite 102, Framingham, MA 01701
Phone: +1 866 262 7542 | Fax: +1 508 656 1399

Rob Ferrini | Program Manager | McGowanPRO
Phone: 508 656 1327 | Fax: 508 656 1399 | Mobile: 508 330 0454
RFerrini@mcgowanprofessional.com

https://mcgowanprofessional.com/