CYBERSECURITY

Zero Trust: The Next Evolution of Security Architecture

WHO ARE WE?

Quest Technology Management

Quest *is a trusted name in the Technology Integration industry, with years of experience in helping customers secure their systems, applications, and environments. Our team of certified security experts can help you protect yourself and your company against cyber threats while improving your security posture. We offer our customers consulting and professional services in all security verticals, from access control and network security to cloud computing and security design.*

Security begins with awareness, and we regularly release white papers to help our customers understand common cybersecurity threats like phishing, malware, ransomware, etc., and how to implement controls to protect against them.

Contact Us Today

IN THIS ISSUE

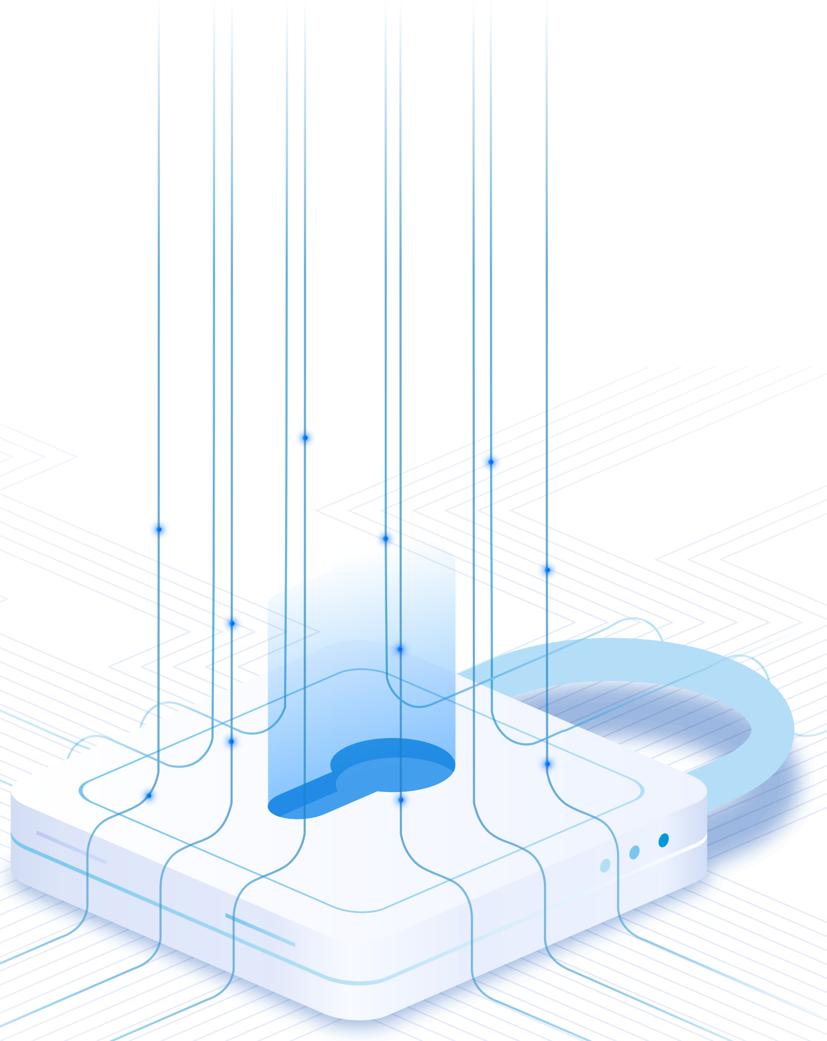
How can we help?

Introduction

The digital landscape has evolved considerably in the past few years, with technologies like Cloud Computing and Artificial Intelligence driving innovation in all spheres. At the same time, cyber threats have kept pace, with newer and more sophisticated attacks emerging regularly. The risks associated with remote working have also forced CIOs, CTOs, and CISOs to take a long, hard look at how they perceive entry points into the corporate network. Due to constantly shifting perimeters, the traditional method of protecting an environment by placing security controls at certain key points is no longer acceptable.

A prominent strategy that's been rising in importance in the cybersecurity community is the Zero Trust Architecture. This isn't just a trendy phrase used for marketing security tools but represents a transformative shift in network defense. Adopting a Zero Trust methodology means reimagining the entire structure of the network to bolster defenses against cyber adversaries. Moreover, the Zero Trust model has the agility to seamlessly integrate with modern tech evolutions, be it diverse cloud services like IaaS and SaaS or innovative realms like DevOps and AI.

The following sections will delve into the nuances of the Zero Trust approach. It's essential to recognize that Zero Trust isn't just another checkbox or a fleeting trend, but a profound evolution in how we approach security. Upon finishing this guide, readers will have a comprehensive understanding of Zero Trust's foundational principles, its functional aspects, and the steps towards building a Zero Trust-centric infrastructure.



What is Zero Trust?

A Zero Trust Architecture, at its core, adopts the principle of "Never Trust, Always Verify". In other words, every request is assumed to be potentially malicious unless verified. This means there is no implied trust, even if the request is coming from a previously authenticated device or person. By continually verifying every request based on certain criteria, Zero Trust can prevent attackers from compromising and laterally moving within a network, as each request is validated on its own security merits instead of a previously established trust—hence the name "Zero Trust."

This core tenet represents a dramatic shift from the traditional way of assessing security requests, in which external requests are assumed malicious but internal requests still carry an implied trust. In traditional security architectures, attackers can compromise a network and then move laterally within it by abusing the established authorized access. Zero Trust assumes that everything in the network is potentially compromised. So no request, be it from a user or device, can be trusted.

What Zero Trust is Not

Despite its many benefits, Zero Trust also carries certain misconceptions that must be clarified. By clearly understanding what Zero Trust is and what it is not, CISOs and other C-level executives can set themselves up for a successful journey toward this concept.

Zero Trust is not:

- **A Product:** Zero Trust is not a software or appliance that can be implemented. CISOs should be wary of any tool that promises to immediately make your environment "Zero Trust compliant." Zero Trust is a strategic approach to how the environment is architected and how security controls are implemented. Provided this understanding exists, it is possible to even start a Zero Trust journey by leveraging existing security tooling.
- **A Certification:** Zero Trust is not a certification against which you need to get annually audited. While standards like NIST are present that can serve as guiding documents, Zero Trust is a continual process that is different for every environment.
- **Static:** While the current tenets of Zero Trust have remained stable, it acknowledges how rapidly the threat landscape changes, with new tenets being added regularly.

The Need for Zero Trust

Zero Trust resulted from several factors that necessitated the move away from traditional security architecture. Its visibility has increased in recent years due to several reasons:

The Increasing Threat Landscape

The rising adoption of cloud computing and remote work means that the attack surface for environments has drastically increased within the last couple of years. CISOs find it incredibly difficult to secure a perimeter in constant flux, with new entry points constantly added. Sophisticated cyber threats like malware and ransomware can compromise an environment from multiple areas, such as the cloud, remote devices, IoT, etc., making the perimeter-based model obsolete. Zero Trust, on the other hand, acknowledges this and assumes that the perimeter does not exist, making it a far better choice.

The Impact of Cybersecurity Incidents

The industry itself has been wracked with significant security incidents such as SolarWinds, Capital One, and Log4J, in which attackers could leverage previously established trust to increase the blast radius of their attacks. The damages from these attacks have reached into the millions—and that excludes additional costs due to reputational damage and loss of trust. A change in mindset is needed to combat threats like supply chain compromises and advanced malware.

Executive Order 14028

Zero Trust also received a significant endorsement, with the Biden Administration issuing **Executive Order (EO) 14028** in May 2021, instructing federal agencies to adopt Zero Trust principles to harden them against attacks. This greatly boosted the popularity of the model, with other companies also adopting it as the de-facto standard to aim for regarding future security improvement.

These factors have enhanced the profile of Zero Trust. **Gartner** estimates that by 2025, 70% of companies will have replaced their existing Virtual Private Networks (VPNs) with a Zero Trust network approach.

A Brief History of Zero Trust

The term "Zero Trust" was initially introduced by John Kindervag in 2010 when he recognized that traditional network approaches towards security no longer sufficed. This resulted in the proposal of a new approach towards security architecture, where instead of trying to keep cyberattacks out of the network, it was assumed that everything in the network was already compromised and needed to be verified. This was a significant rethink of how security was traditionally approached, and the concept grew in popularity with the increase in cloud adoption and remote working.

Tech giants like Google showcased their own internal initiatives like **Google BeyondCorp**, which was their internal implementation of a Zero Trust architecture with a long-term vision of completely replacing their perimeter.

NIST contributed to Zero Trust by releasing publication 800-207, "**Zero Trust Architecture**," which guided the design and implementation of this model within different environments. NIST publications typically become industry standards due to the high scrutiny and review they undergo from various industry leaders and experts. This guide has contributed to Zero Trust maturing over time and becoming a long-term strategic goal for most companies.

Principles of a Zero Trust Implementation

Along with its core tenet, Zero Trust has several principles that all work together to form a secure network. It is important to note that these principles are not static and evolve to accommodate new types of attacks and threats.

1. Robust and Adaptive Authentication

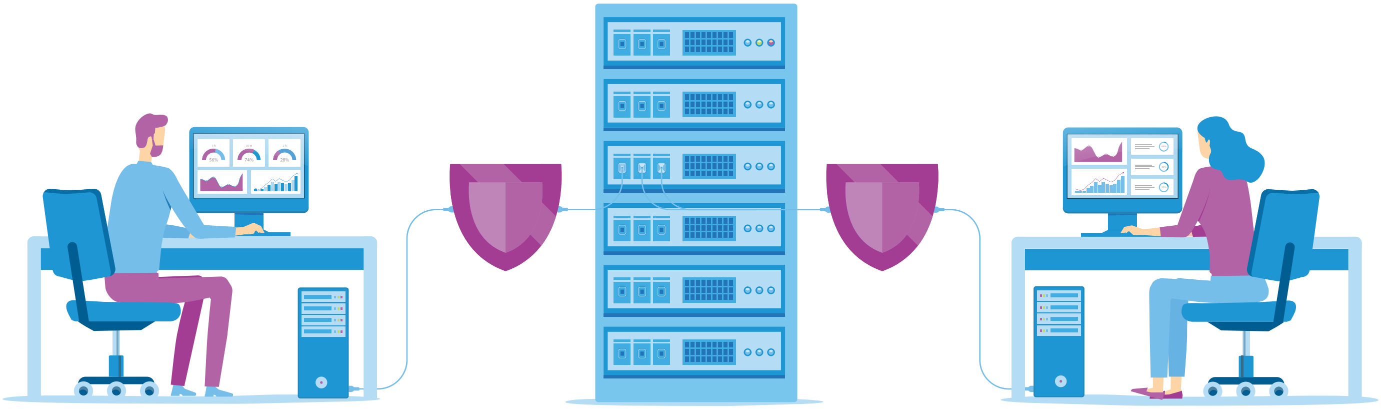
Identity is the heart of Zero Trust, as we will see in the next section, and it is essential to set up a strong foundation from the start. The model dynamically adapts authentication requirements based on the risk profile of a request. For example, a user's risk score may require standard password authentication; however, the following request might require multi-factor authentication for further verification. The Zero Trust engine analyzes each request uniquely and increases the level of authentication based on its criteria.

2. Continuous Approval and Authorization

Many cyber attacks succeed as the user or device is compromised after the established session. Zero Trust continually approves and authorizes requests so it can defend against an attacker who compromised a previously authorized device. By constantly monitoring requests, the model can pick up malicious activity much sooner than other approaches.

3. Least Privilege Access

Zero Trust works with the security principle of least privilege and tools like Privileged Access Management (PAM) that control administrative access within an environment. The principle of least privilege is not unique to Zero Trust; however, the model extends this to the network architecture instead of restricting it to systems or applications.



4. Continuous Monitoring

For Zero Trust to be effective, it requests continuous visibility into the security posture and risk profile of the devices and users connecting to the environment. This enables it to detect anomalies in real-time and assess the security posture of users and devices before granting them access. AI and Machine Learning tools can be useful here as they can baseline what is expected from what is malicious within an environment.

5. Microsegmentation

Organizations typically implemented network segmentation as a security control in which sensitive workloads were kept in separate network subnets for additional control and security. Yet the concept of least privilege was not fully applied, as traffic within network subnets is typically not restricted or inspected by firewalls, which have visibility into "north-south" traffic that crosses the perimeter. Microsegmentation helps to protect the "east-west" by further breaking down the subnets into smaller and more isolated segments restricting lateral movement.

In addition to these principles, a crucial pillar of Zero Trust is identity. Identity is often referred to as a new perimeter in Zero Trust environments—for a good reason. Most of the principles we discussed, such as continuous monitoring, adaptive authentication, least privilege, etc., revolve around establishing a strong identity foundation. Technologies like Single Sign-On (SSO) and Multi-Factor Authentication (MFA) all help to dynamically enforce intelligent policies required for Zero Trust. These controls extend beyond human users and also encompass machine-based identities as well. By moving controls away from the perimeter and focusing on identity as the core, organizations can adapt to environments in which the network perimeter is in constant flux.

Embarking on Your Zero Trust Journey

Having grasped the core concepts of Zero Trust, it's time to delve into its practical application within a setting. Remember, Zero Trust isn't just a singular initiative, but a continuous process that evolves and refines with time.

Key activities for a successful Zero Trust journey are:

- **Setting expectations:** Management must understand that Zero Trust takes time and effort to implement. It is not a plug-and-play solution. There are many success stories (such as Google's BeyondCorp initiative, which we discussed earlier) that can be used to show the long-term benefits of Zero Trust and get management's support. Tools like SSO and microsegmentation require resources and budgeting, so it is essential to acquire management support at the start.

- **Upskilling of existing staff:** Adopting Zero Trust alters the authentication and access procedures, necessitating proper training for personnel. A significant cause of Zero Trust initiatives falling short is due to insufficient understanding, which can result in opposition and uncertainty.
- **Understanding the Environment:** Zero Trust doesn't follow a universal blueprint. Organizations need to grasp their specific risk landscape and pinpoint their primary concerns. From there, they should craft a tailored Zero Trust approach that addresses these specific security challenges using its foundational principles.
- **Deployment/Upgrade of Technologies:** Once a company has decided on which principles to implement, it can start translating them into the technical and policy level. Implementing new technologies is not mandatory; existing ones can also be leveraged and modified. It is also possible that current versions of firewalls and other security products might not be able to support Zero Trust tenets and require replacement or upgrades. This can be done in a phase-wise manner to minimize disruption to the environment.

- **Maturing the Model:** Like any project, Zero Trust must be matured and improved upon over time. Its effectiveness must be monitored and reported to senior management for effective governance. Similarly, policies must be fine-tuned as more data is gathered on what is working and what needs improvement.
- **Future improvements:** As technology evolves, companies must reassess their controls to ensure that the Zero Trust Model has visibility and control over new and emerging technologies. For instance, companies might adopt biometric authentication for some applications that would require policy updates within the Zero Trust engine. Another potential change would be the adoption of AI and Machine Learning systems that can baseline and detect security anomalies.

Conclusion

Zero Trust is playing an essential role in the evolution of cybersecurity. As threats become increasingly advanced, it is apparent that the solution lies not in implementing more and more security products, but in fundamentally rethinking how we approach security. By following the principles outlined in this ebook, CISOs and other thought leaders can set themselves up for long-term success in their Zero Trust journey.

Want to learn more?

Let's have a conversation.

How can we help?®

www.questsys.com
1.800.326.4220

Quest®
TECHNOLOGY MANAGEMENT