Akamai

WHITE PAPER

Roadmap to a World-Class Security Posture

Get a customized transformation plan with Zero Trust at its core

To ensure Akamai stays protected in an evolving security environment — and avoids complacency — we recently visualized our security performance using the Zero Trust Maturity Model (ZTMM). Here, we share how doing that for your own organization can highlight critical areas for improvement and create a clear roadmap to achieving a world-class security posture.

Simplify the journey to Zero Trust

Enterprise access and security are complex and constantly changing. Against this backdrop, it can be challenging to know where to concentrate efforts when moving toward a Zero Trust security posture.

That's why we recommend using the ZTMM as a tool for assessing and visualizing your current security posture. We've used it to assess our own corporate security posture at Akamai, as well as to assess the security postures of several customers. At the end of the process, you'll have a roadmap of practical actions to move you closer to a Zero Trust architecture. (See Appendix A for more information about the Zero Trust concept.)

Why the Zero Trust Maturity Model makes sense

We think the most critical step on the road to implementing a stronger security posture is the first one: getting started. However, when it comes to the complex, ever-changing topic of cybersecurity, starting is easier said than done. We've seen many organizations struggle with decisions regarding what to do, how much to do, and the order in which they should make changes to achieve Zero Trust.

This is where the ZTMM shines. It creates a framework around Zero Trust, providing a sense of linearity, which makes it easier to implement. It helps organizations create a plan for change and budget for updates. It also explains Zero Trust concepts to decision-makers who aren't IT specialists, which helps IT teams get the buy-in they require.

The ZTMM is tried and tested. It was developed by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and has been widely adopted within U.S. federal agencies.

The five pillars and three capabilities of the Zero Trust Maturity Model

The ZTMM represents a gradient of implementation across five distinct pillars, so minor advancements can be made over time. The pillars ask you to consider Identity, Devices, Networks, Applications and Workloads, and Data (Figure 1). The ZTMM also requires you to think about three capabilities that traverse all five pillars:

- Visibility and Analytics
- Automation and Orchestration
- Governance

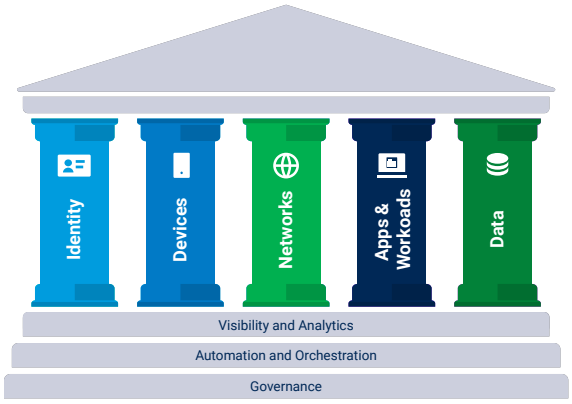


Fig. 1: CISA's ZTMM is one of many paths to support the transition to Zero Trust (Source: CISA)

Each of these areas is assigned a maturity status that describes how close an organization is to achieving a Zero Trust approach. The four maturity stages (Traditional, Initial, Advanced, and Optimal) describe the journey from manual configuration and VPNs toward the ideal "perimeterless security" setup (Figure 2). At the Optimal end of maturity, organizations grant applications minimum privileges, deny authentication and access to vulnerable devices, prevent internal threats from spreading, and instantly detect and respond to security incidents. (See Appendix B for a more detailed description of the ZTMM framework.)

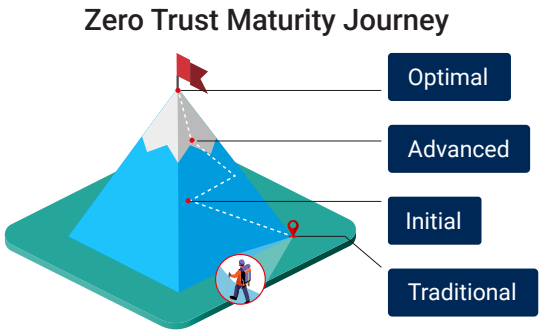


Fig. 2: The Zero Trust maturity journey (Source: CISA)

By highlighting areas where maturity is lowest, the ZTMM helps organizations develop a more balanced security environment. Akamai's industry-leading suite of security solutions, combined with our expertise, is making it easier than ever to move toward a mature security posture.

Are your teams struggling to implement Zero Trust? You are not alone.

The responsibility of creating a Zero Trust architecture doesn't sit with just one department. It requires buy-in, flexibility, and approval from a range of stakeholders at all levels of an organization.

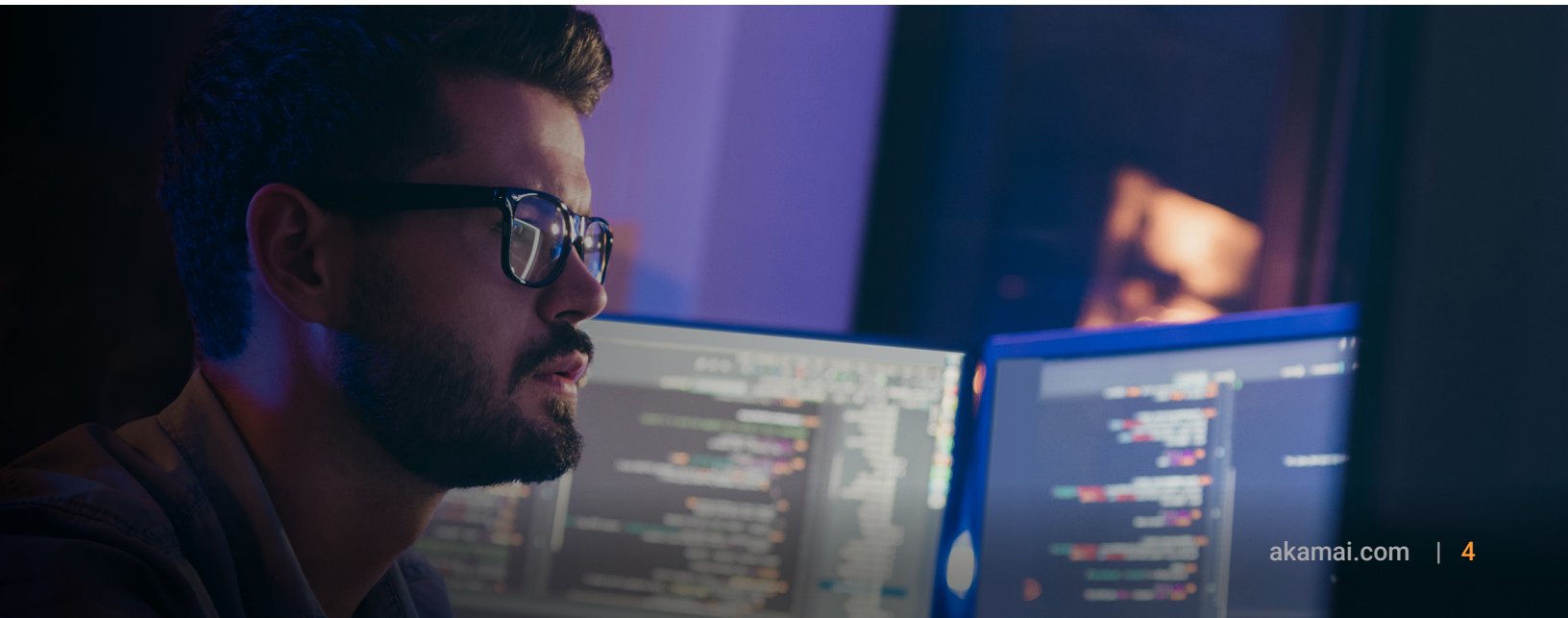
Akamai is the cybersecurity and cloud computing company that powers and protects business online. Our market-leading security solutions, superior threat intelligence, and global operations team safeguard critical data and applications at every touchpoint, all across the globe. This bird's-eye view means we understand the most common challenges when it comes to moving toward a Zero Trust security posture — and we can help you find solutions.

Three common Zero Trust challenges

1. *Knowing where to start.* We usually recommend starting with workload visibility and reducing the attack surface to bolster cyber resiliency — but that depends, of course, on the organization's current security posture.

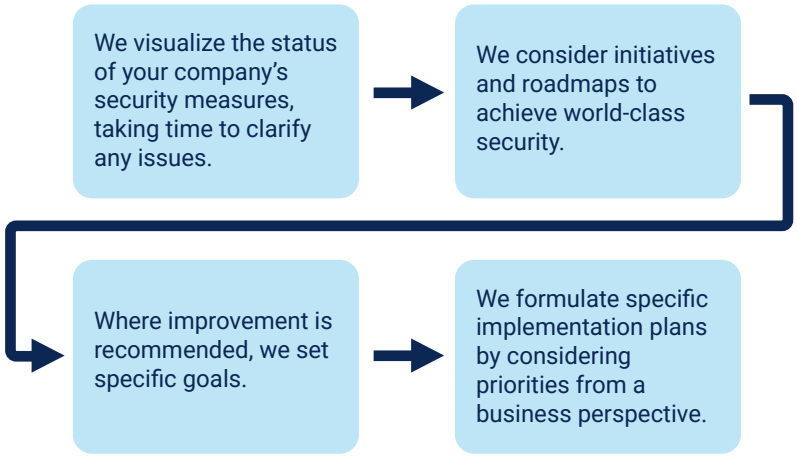
2. *Achieving success quickly.* Achieving Zero Trust can seem like such an enormous undertaking that it's difficult for teams to focus on any one thing or to celebrate the small steps taken toward the goal.

3. *Demonstrating ROI.* Zero Trust projects are not cheap, and they usually require cultural changes, as well as technological changes, within an organization. The ability to demonstrate the return on investment — whether that's a reduced attack surface, a mitigated breach, a secured vulnerability, or a financial win— is critical, especially for decision-makers and security leaders.



Ready to begin your Zero Trust journey and visualize your security posture?

As we did at Akamai, you can use the ZTMM to visualize the maturity status of your organization's current security measures. Doing so will help highlight how you can bring more balance to your process and what needs to change in order to achieve a Zero Trust architecture.



How Akamai can guide you toward a Zero Trust security posture

A successful Zero Trust architecture uses a variety of controls and principles to address security challenges.

We'll consider initiatives and roadmaps to help you create an implementation plan that takes your entire business and its goals into account to achieve world-class security. This approach allows us to work with you to build security systems and processes that are effective and sustainable in the long term.

Alongside Akamai Cloud, our suite of security products — including an advanced distributed ZTNA solution, industry-leading microsegmentation, phish-proof multi-factor authentication (MFA), and a proactive DNS firewall — will move your security posture toward the Optimal end of the Zero Trust maturity scale. Moreover, the entire system can be run by a single agent using a single console (Figure 3).

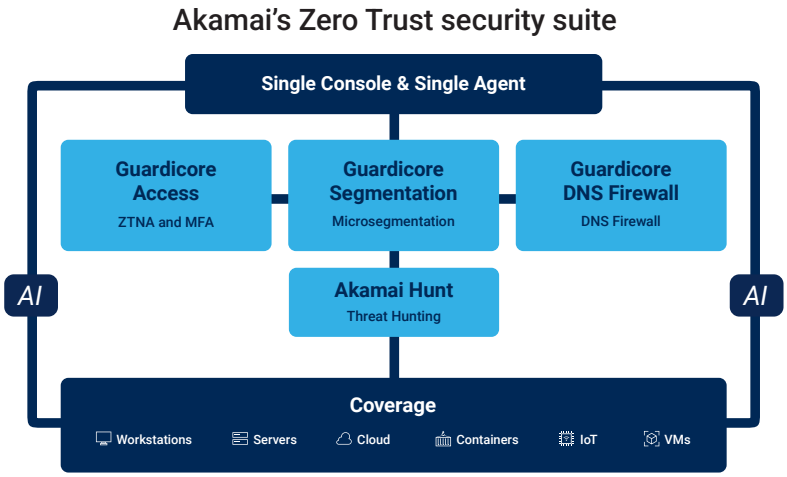


Fig. 3: Akamai's suite of security products can be run by a single agent using a single console

Case study

Visualizing a multinational retailer's ecommerce security posture using the Zero Trust Maturity Model

We recently analyzed a multinational retailer's ecommerce security posture, visualizing its security status and providing a corresponding roadmap to move it closer to a world-class security posture. Our team of experts identified areas for improvement across the ZTMM, which we ranked in importance from high to low. Here, we share the results.

An unbalanced system with variation in implementation

In each pillar, we found that some functions were implemented at the highest (Optimal) level of maturity, such as mobile device management and automation of application deployment. However, some functions in each pillar remained at the Traditional level, which presented serious risks.

In particular, important functions in the Identity and Network pillars had not been strengthened; these pillars are the foundation of a Zero Trust architecture. These functions included MFA, integrated management of identity infrastructure, context-based access control, and microsegmentation.

Risky ID infrastructure

Our analysts discovered that ID and password authentication was the standard within the retailer; the use of MFA was limited to a few systems. This created a high risk for the authentication information to be abused. Additionally, multiple ID infrastructures existed, such as Microsoft Entra ID, on-premises Active Directory (AD), and Lightweight Directory Access Protocol (LDAP). Since the retailer's management was not integrated, there was a risk of a breach starting from an ID infrastructure with weaker security measures, such as LDAP.

Unintegrated authorization controls

Authorization controls had not been integrated, so each application was being handled individually. It was not possible to block access from vulnerable devices or suspicious access: If the PC of an employee or partner with access to the company network became infected with malware, there was a high risk of unauthorized access to systems and resources via lateral movement.

Inadequate segmentation

We found that the retailer's security measures were heavily focused on external threats, overlooking the risks posed by attackers who had already breached the network. Without robust internal segmentation, an intrusion via the Wi-Fi network at a warehouse or via vulnerabilities in the VPN could lead to uncontrolled lateral movement. This lack of internal barriers significantly increased the risk of widespread system compromise, data leakage, and operational outages, as the attack could move freely across the network without containment measures in place.

Insufficient vulnerability management and response

The retailer did not have a management system that linked a software bill of materials (SBOM) to vulnerability information. This meant it was unable to quickly identify and respond to application vulnerabilities, which posed a high risk.

Our recommendations

We advised the retailer to take the following five steps to strengthen their security posture:

1. Take proactive measures to reduce the risk of unauthorized intrusion and lateral movement that exists with the current setup
2. Continue to integrate Identity infrastructure into their existing tech stack
3. Develop a plan to expand authentication and authorization capabilities, in conjunction with Zero Trust Network Access
4. Decide on the most effective way to implement granular workload and application protection
5. Build a response system and process for unknown future threats, develop a system and process to strengthen vulnerability management and response, and formulate a plan

If you are interested in embarking on your Zero Trust journey, contact us for a complimentary security assessment.

Appendix A: An overview of the Zero Trust concept

Zero Trust is a security philosophy based on the idea that no user, device, or system — inside or outside of an organization's network perimeter — should be trusted.

Instead, verification processes and monitoring are used to minimize risk. This includes approaches like enforcing strict identity and access management (IAM) policies, using multi-factor authentication (MFA), and prioritizing role-based access control (RBAC).

The Zero Trust concept has been around for 15 years, but it became more important during the COVID-19 pandemic when organizations faced increased remote access requirements. Many companies realized their existing security measures didn't hold up when users and devices were scattered rather than centralized.

Today, there are many implementations of Zero Trust principles, including Zero Trust architecture, Zero Trust Network Access (ZTNA), Zero Trust secure web gateway (SWG), and microsegmentation.

Read more about Zero Trust

Appendix B: The ZTMM 2.0 framework

The five pillars

Each pillar can progress at its own pace and may progress more quickly than others — until cross-pillar coordination is required.

Pillar	Description
Identity	An attribute or set of attributes that uniquely describes an agency user or entity, including nonperson entities
Devices	Any asset that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, Internet of Things (IoT) devices, networking equipment, and more
Networks	An open communications medium, including typical channels, such as agency internal networks, wireless networks, and the internet, as well as other potential channels used to transport messages
Applications and Workloads	Agency systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments
Data	Structured and unstructured files and fragments that reside or have resided in systems, devices, networks, applications, databases, infrastructure, and backups, as well as the associated metadata

Cross-pillar capabilities

These three capabilities support the entire Zero Trust framework, ensuring that security measures are integrated, responsive, and consistent.

Capability	Description
Visibility and Analytics	Organizations should have a clear, real-time view of all user activities, device states, and network interactions. Threats are detected and responded to quickly, which reduces risk. Organizations make informed, proactive security decisions.
Automation and Orchestration	Human error is a common cause of security issues. When automation and orchestration are optimized, the chances of this are minimized. Automation simplifies routine tasks, and orchestration organizes security actions across different systems. This creates the right conditions for quicker, more coordinated responses to threats.
Governance	Good security governance creates accountability, ensuring everyone follows the same security practices and regulations. This builds a strong foundation for safe operations. It also sets clear Zero Trust guidelines and helps organizations meet compliance standards.

The maturity aspect of the Zero Trust Maturity Model

ZTMM 2.0 defines four maturity levels for each function. The goal is to determine the current maturity level of the five pillars and three capabilities and then create a plan to move each one toward the highest maturity level.

Maturity level	Description
Traditional	Manual configuration, response, and mitigation; static and siloed policies and solutions
Initial	Starting automation; initial cross-pillar solutions; some responsive changes to least privilege; aggregated visibility for internal systems
Advanced	Automated controls where applicable; cross-pillar policy enforcement; least-privilege changes based on risk/posture; response to predefined mitigations
Optimal	Automated controls where applicable; cross-pillar policy enforcement; least-privilege changes based on risk/posture; response to predefined mitigations