TechnologyMatch.com

An essential Zero Trust Access maturity checklist

As an IT leader, you can trust your users' intentions, but you cannot trust their actions. All it takes is a half-minded click on a malicious email before it laterally moves across your network, turning into a ransomware attack. Hundreds and thousands of dollars lost in a disaster that recovers slowly, and the worst part is that you can't even guarantee that it will never happen again. Unless you take action.

A Zero Trust Access (ZTA) infrastructure is not news; it's been around for a while but IT leaders haven't extensively implemented protocols to enable an environment where the possibility of security breaches is minimized.

Contrary to its name, a ZTA infrastructure doesn't not trust the users but rather enforces a least privilege environment where a user's identity is constantly identified. And instead of granting access to the network, a user is connected directly to the application, isolating the risk of any attacks spreading within.

ZTA is not a one-time thing but rather a continuous process and as an IT leader, how mature are you when it comes to implementing these security pillars in your organization?

This assessment helps you go through a necessary checklist for ZTA implementation and figure out where you stand.

To make things more interesting, there's a scoring system to this checklist for a more comprehensive understanding of your ZTA position.

How it works:

- **There are 5 sections with 5 checklists each.**
- **If you've implemented a checklist, assign a "1" to it and if you haven't, assign a "0".**
- **You can have a minimum of 0 points and a maximum of 5 points.**
- **The point you score determines your maturity for that pillar of the ZTA infrastructure.**

Part 1: Who has access to what?

Identity and Access Management

You can have a minimum of 0 points and a maximum of 5 points.

- 0 points: **Immediately implement basic identity management protocols**
- 1 points: **In the right direction. Continue building authentication frameworks**
- 2 points: **Good job. Develop betteridentity protection strategies**
- 3 points: **You're on a roll! Refine access management for higher security**
- 4 points: **Amazing! Implement advanced and dynamic access control**
- 5 points: **You're Yoda. Please teach us the way.**

- [ ] **Comprehensive identity framework and authentication**

  Implemented a robust Identity, Credential, and Access Management (ICAM) framework with Single Sign-On (SSO) and Multi-Factor Authentication (MFA) across all applications and resources.

- [ ] **Privileged access and governance**

  Implemented Privileged Access Management (PAM) with just-in-time (JIT) access, session monitoring, and least privilege principles for all administrative accounts.

- [ ] **Dynamic access control**

  Established dynamic, risk-based access policies that continuously evaluate multiple contextual factors, adapting permissions in real-time based on changing risk levels and automatically revoke access when anomalies are detected.

- [ ] **Credential protection**

  Deployed credential protection including passwordless options, protection against credential stuffing, password spray attacks, and comprehensive monitoring for credential theft or misuse.

- [ ] **Identity analytics and visibility**

  Deployed identity analytics that detect unusual patterns, potential credential compromise, excessive privileges, and access anomalies across the entire identity infrastructure.

Part 2: How quickly can you detect unauthorized devices?

Infrastructure and Access Control

You can have a minimum of 0 points and a maximum of 5 points.

- 0 points: **Urgently address security loopholes in your infrastructure.**
- 1 points: **Replace legacy VPN with Zero Trust Network Access solutions.**
- 2 points: **That's the spirit! Invest in better endpoint security measures.**
- 3 points: **You're doing great. Further protect your network from vulnerabilities.**
- 4 points: **Already amazing! Perhaps you can improve incident response.**
- 5 points: **You're an IT messiah. But also keep optimizing.**

- [ ] **Device trust and endpoint security**

  Implemented mandatory device registration with identity provider for resource access. Deployed endpoint threat detection and response (EDR) capabilities to protect against malware, ransomware, and advanced persistent threats.

- [ ] **Zero Trust Network Access (ZTNA)**

  Replaced traditional VPN infrastructure with ZTNA solutions that provide application-level access rather than network-level access.

- [ ] **Next-generation protection and secure remote access**

  Deployed Firewall as a Service (FWaaS) to control traffic flows based on application needs rather than just ports and protocols.

- [ ] **Asset discovery**

  Maintained a continuously updated inventory of all hardware and software assets with automatic discovery, classification, and security posture assessment capabilities.

- [ ] **Security and incident response**

  Established remediation workflows for common security issues, including quarantining compromised devices, blocking suspicious network traffic, and resetting compromised credentials.

Part 3: Can threats move laterally in your network?

Network Segmentation and Micro-Segmentation

You can have a minimum of 0 points and a maximum of 5 points.

- 0 points: **Immediately transition from traditional network perimeters**
- 1 points: **Begin implementing identity-based network security model**
- 2 points: **A good first step. Develop granular network segmentation strategies**
- 3 points: **Great! Improve or implement better lateral traffic movement.**
- 4 points: **Your network is pretty much fool proof. Perhaps SASE?**
- 5 points: **Look at you, smart ass!**

Identity-based segmentation and Zero Trust network

Transitioned from traditional network perimeters to identity-based network security model where access is determined by user identity and context rather than network location.

Micro-segmentation and lateral movement controls

Monitored and controlled lateral traffic between network segments with default-deny policies and explicit permission for legitimate communications only.

Software-Defined Networking (SDN) and Visibility

Utilized SDN capabilities to implement granular, policy-based network controls that dynamically adjust based on real-time security telemetry.

Secure Access Service Edge (SASE)

Deployed SASE architecture that combines network security functions with WAN capabilities to support access from any location to applications in any environment.

Network Access Control (NAC)

Leveraged NAC that validates device security posture, user identity, and other contextual factors before allowing any device to connect to the network infrastructure.

Part 4: How quickly can you respond to incidents?

Security and Monitoring

You can have a minimum of 0 points and a maximum of 5 points.

- 0 points: **Rapidly deploy enterprise-wide security monitoring solution**
- 1 points: **If you're completely on-prem, consider moving operations to cloud**
- 2 points: **Things are improving. Develop better CASB capabilities.**
- 3 points: **Can you improve on things like DLP and prevent Shadow IT?**
- 4 points: **Perhaps monitoring efforts can be better automated.**
- 5 points: **You're good. But security and monitoring is a constant process**

- [ ] **Comprehensive security monitoring and SIEM**

  Deployed an enterprise-wide Security Information and Event Management (SIEM) solution that collects, correlates, and analyzes security data from all environments.

- [ ] **Cloud access security**

  Deployed Cloud Access Security Brokers (CASB) for visibility and control over all cloud services, providing data security, threat protection, and access control across a multi-cloud architecture.

- [ ] **Behavioral analytics and anomaly detection**

  Implemented User and Entity Behavior Analytics (UEBA) that establishes baseline behavior patterns for users, devices, and applications, then automatically detects anomalous activities indicating compromise.

- [ ] **Shadow IT discovery management**

  Implemented Shadow IT discovery and risk assessment that continuously monitors for unauthorized cloud services, applications, or resources, then applies appropriate controls or integration into security framework.

- [ ] **Data Loss Prevention (DLP)**

  Deployed DLP controls across all channels (email, web, endpoints, cloud, removable media) with content inspection and automated policy enforcement.

Part 5: Is security embedded in your culture?

Employee Awareness Programs

You can have a minimum of 0 points and a maximum of 5 points.

- 0 points: **Seriously think of a security awareness training program.**
- 1 points: **You need to be more proactive about awareness.**
- 2 points: **In the right direction but lacks consistency.**
- 3 points: **Good. Look more vigorously into contextual training programs.**
- 4 points: **Your organization is pretty aware but needs constant reminders.**
- 5 points: **Hats off! Your organization and employees are smarter than most.**

- [ ] **Phishing Defence**

  Implemented phishing simulation program that regularly tests employees with realistic scenarios, provides immediate feedback and education, and tracks improvement over time.

- [ ] **Contextual security guidance**

  Implemented context-sensitive security guidance that provides relevant information to users at the moment of decision (e.g., warnings when opening suspicious attachments or visiting potentially dangerous websites).

- [ ] **Remote work security**

  Established dedicated training for secure remote work practices covering home network security, public Wi-Fi risks, physical security of devices, and secure collaboration practices outside the corporate environment.

- [ ] **Reporting channels**

  Established accessible channels for employees to report security concerns, suspicious activities, or potential incidents with protection from retaliation and recognition for proactive reporting.

- [ ] **Emerging Threat Education**

  Educated employees about emerging threats, including new phishing techniques, social engineering tactics, or ransomware distribution methods.

Conclusion

If you haven’t thought about implementing a ZTA infrastructure, you’re exposing your organization to great risks.

Zero Trust is an ongoing process and it’s not something you can do on your own; you need the right partners and vendors to help you transition gradually with state-of-the-art solutions and expertise.

- **Zero Trust has become one of the most important pillars of successful IT initiatives in the past decade.**
- **Organizations with ZTA are exponentially less susceptible to network vulnerabilities and more prepared for modernization.**
- **More than 90% of enterprises are considering or implementing Zero Trust for important use cases like IAM, micro-segmentation, incident response, CASB, and DLP.**