Zero Trust Checklist

It's critical to know who's accessing your systems, what level of access each user has, and if you and your team are able to adjust those permissions as necessary. Zero Trust Architecture helps accomplish these tasks in a streamlined and efficient manner.

Trust no one

Zero Trust Architecture or Network Access (ZTNA) is a cybersecurity concept that removes any implicit trust, regardless of who's accessing a network or system and what's being accessed. Since no one is trusted in this model, insider and outsider access need to be verified and authenticated each time a user logs into a system. A Zero Trust model can minimize the risk of a hack by authenticating users to ensure access can be trusted and limiting network exposure through least privilege access.

ZERO TRUST CHECKLIST

Use this checklist to review your current cybersecurity protocol to see how it aligns with Zero Trust principles. You can use the solutions outlined in the checklist to implement Zero Trust within your organization.

- Do you know the different methods of how access is currently being granted to users, especially third parties, vendors, or contractors?
  - Identify all points of access across all users - employees, customers, and third parties (VPN, WebEx, TeamViewer, RDP, Citrix, VDI, etc.), then identify all gaps in security or points of vulnerability within those access points

- Does your solution provide granular access controls and directory-based authentication?

- Do you use multi-factor authentication (MFA) to authenticate the identity of every individual user and third-party/vendor rep?

- Is there a way to prevent lateral movement across the network/system?
  - Implement tools to identify and authenticate each user and access attempt
  - Multi-factor authentication is the bare minimum of authentication methods - implement this at the very least

- Are you able to limit third-party access to:
  - The necessary network segment(s)?
  - Only the specific server/system(s)?
  - The specific application port(s)?
  - The specific periods of time needed for access?
  - Use least privileged access by limiting the scope of what a user can access down to the application, host, system, server, or port level
  - Isolate and limit the movement of a user throughout the network/system to ensure they cannot access what they don’t need.
  - Use time-based provisioning for user sessions

- Are you currently reviewing all access attempts manually?

- Are you inventoring users and auditing user activity manually?
  - Implement regular review of user access and permissions across the organization to verify or adjust permissions as needed
  - Review and monitor user behavior and network activity regularly
  - Streamline this process by using remote access management platforms

- Is there automatic de-provisioning to remove accounts that are no longer needed?

- Is there a workflow process in place for provisioning and de-provisioning accounts?
  - Configure provisioning/de-provisioning processes so access permissions can be changed automatically when needed
  - Work with others within your organization to create processes that adjust access permissions efficiently
  - Install a process or protocol to identify which permissions are appropriate/appropriate on a regular basis

- Do you use VPN?
  - If so, is the VPN always active, or is it authorized on each access attempt?
  - Implement another method of access and remote access to replace less secure, always-on VPN connections

- Does your solution provide granular access controls and directory-based authentication?

- Do you use multi-factor authentication (MFA) to authenticate the identity of every individual user and third-party/vendor rep?

- Is there a way to prevent lateral movement across the network/system?
  - Implement tools to identify and authenticate each user and access attempt
  - Multi-factor authentication is the bare minimum of authentication methods - implement this at the very least

- Are you able to limit third-party access to:
  - The necessary network segment(s)?
  - Only the specific server/system(s)?
  - The specific application port(s)?
  - The specific periods of time needed for access?
  - Use least privileged access by limiting the scope of what a user can access down to the application, host, system, server, or port level
  - Isolate and limit the movement of a user throughout the network/system to ensure they cannot access what they don’t need.
  - Use time-based provisioning for user sessions

- Are you currently reviewing all access attempts manually?

- Are you inventoring users and auditing user activity manually?
  - Implement regular review of user access and permissions across the organization to verify or adjust permissions as needed
  - Review and monitor user behavior and network activity regularly
  - Streamline this process by using remote access management platforms

The days of castle-and-moat cybersecurity strategies are gone. Hackers are becoming too advanced, and threats exist both inside and outside of an organization’s network. The Zero Trust model recognizes that these threats are vulnerabilities and must be addressed. Whether users are internal employees or external third parties, trust must be eliminated, and verification must become the new standard. Watch this webinar to learn why Zero Trust is necessary for third-party remote access management.

About SecureLink

SecureLink, an Imperva company is the industry leader in critical access management, empowering organizations to secure access to their most valuable assets, including networks, systems, and data. By leveraging Zero Trust principles, machine learning, and artificial intelligence, SecureLink provides comprehensive security solutions to govern, control, monitor, and audit the most critical and highest risk access points. Organizations across multiple industries – including healthcare, manufacturing, government, legal, and gaming – trust SecureLink to secure all forms of critical access, from remote access for third parties to access to critical infrastructure, regulated information, IT, and OT.