Zero Trust checklist

imprivata®

It is 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. A 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 is accessing a network or system and what is 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 in to a system. A Zero Trust model can minimize the risk of a hack by authenticating users to ensure access can be trusted and by limiting network exposure through least privilege access. Zero Trust is not a single set of technologies an organization can purchase – it's a guiding set of principles that organizations are gradually adopting to protect their organization.

The main goal:

> **"Prevent unauthorized access to data and services, coupled with making the access control enforcement as granular as possible..."**
>
> **– NIST SP 800-207,** Zero Trust Architecture 2020

Zero Trust checklist

Use this checklist to review your current cybersecurity protocol to see how it aligns with Zero Trust principles and to understand where there might be security gaps in your strategy.

Do you know the different methods of how access is currently being granted to users, especially third parties, vendors, or contractors?

- ☐ Yes
- ☐ No

Strategy: 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

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

- ☐ Yes
- ☐ No

Strategy: Require tools to identify and authenticate each user and access attempt. Implement multifactor authentication for access to internal systems, applications, and even data.

Do you have solutions in place that can help your organization prevent lateral movement across the network/system?

- ☐ Yes
- ☐ No

Strategy: Enforce the principle of least privilege. If a user does not need access to systems, applications, or data, remove it. As a first step, remove administrator rights on desktops for all users. Implement strong password policy management. Solutions like privileged access management (PAM) or identity governance and administration (IGA) can help you accomplish this task.

Are you able to limit privileged users or third-party access to:

- The necessary network segment(s)?
  - ☐ Yes
  - ☐ No
- Only the specific server/system(s)?
  - ☐ Yes
  - ☐ No
- The specific application port(s) and specific periods of time needed for access?
  - ☐ Yes
  - ☐ No

Strategy: 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 do not need. Use as a solution with time-based provisioning for user sessions like vendor privileged access management (VPAM) or PAM for internal privileged users.

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

- ☐ Yes
- ☐ No

Strategy: An IGA solution provides fast, secure role-based access to systems and offers capabilities such as automated provisioning and de-provisioning, access request management, and detailed event logging.

Is there a workflow process in place for provisioning and de-provisioning accounts?

- ☐ Yes
- ☐ No

Strategy: Configure provisioning and 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. Create policies and protocols to determine which permissions are appropriate/inappropriate on a regular basis.

Do you use VPN?

- ☐ Yes – And if "yes," is the VPN always active, or is it authorized on each access attempt?
- ☐ No

Strategy: Implement a secure remote access solution like VPAM or a PAM solution as an alternative method of access to replace less secure, always-on VPN connections which do not scale and are a risk to your organization.

Are you currently reviewing all vendor access attempts, privileged user access requests, and employee access to applications or your network manually?

- ☐ Yes
- ☐ No

Strategy: Implement cybersecurity solutions that are fully integrated to conduct a regular review of user access and permissions across the organization to verify or adjust permissions as needed.

Are you conducting reporting and auditing around vendor access, privileged user access, and application access?

- ☐ Yes
- ☐ No

Strategy: Review and monitor user behavior and network activity regularly. Streamline this process by using access management platforms as well as identity governance solutions that already have session management and reporting to make your auditing process an easier one and help you maintain compliance.

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.

When it comes to implementing Zero Trust in your organization, Imprivata is your partner with the tools required to protect access and control identities – the very core of an effective security strategy. If you checked "no" to any of the above questions, **contact us** to help you change your answer to "yes."