3 Simple Ways to Start Implementing Zero Trust Security Today

New business initiatives and processes have created broader attack surfaces. Applications, users, and devices are moving outside of the traditional corporate zone of control, dissolving what was once the trusted perimeter, and enterprise security and networks must evolve to protect the business. Taking on a complete Zero Trust security transformation isn't something that most organizations can do overnight. Many companies require time to fully implement major network and security changes, but there are several simple steps you can take today to get started. The following three actions will serve as the foundation of your path to "never trust, always verify" security:

1. Conduct a threat check to gain visibility into your environment and determine devices' current exposure to malware/phishing. Many networks have already been compromised and have active malware that has escaped detection by existing security measures. **Administer a free 30-day Threat Check** to receive a customized report on threats presently active in your environment and tailored suggestions on how to remediate those advanced threats. It's fast and easy to implement, with minimal network changes required. For IT teams, this is typically a quick win to realize operational benefits.

2. Stop giving network access to your users. Full network access increases your threat exposure. User access should be restricted to only the applications an individual needs — not the entire network. For operational efficiency, start simply with the applications that are easiest to transition, such as your web applications and any new applications, and publish those based on Zero Trust security principles. Then **conduct a Zero Trust Architecture Assessment** to develop a comprehensive plan to migrate from your current state to a Zero Trust framework. This includes profiling users and applications, as well as developing a customized phasing plan for all applications (including legacy on-premises applications).

3. Eliminate traditional VPN for specific user groups. A Zero Trust security framework suggests that you stop trusting your endpoints implicitly and work to decommission legacy access — including VPN and privileged corporate Wi-Fi/Ethernet segments — to remove the associated trust at the inner layers. Start by provisioning access based on Zero Trust security principles to high-risk user groups, such as contractors. Then determine a phase-out plan for legacy access for all users.

Continuously adapting your enterprise's approach to security in response to evolving business and threat landscapes is imperative. Transitioning to a Zero Trust security architecture enables you to simply and effectively safeguard your applications, users, and devices. This migration can be achieved through a stepped process, beginning with these three basic and actionable tasks. To learn more about starting your Zero Trust transformation today, **schedule a workshop with an Akamai security specialist.** Together, we'll identify additional opportunities and actions to evolve to a Zero Trust Security model.