SONICWALL PERSPECTIVES

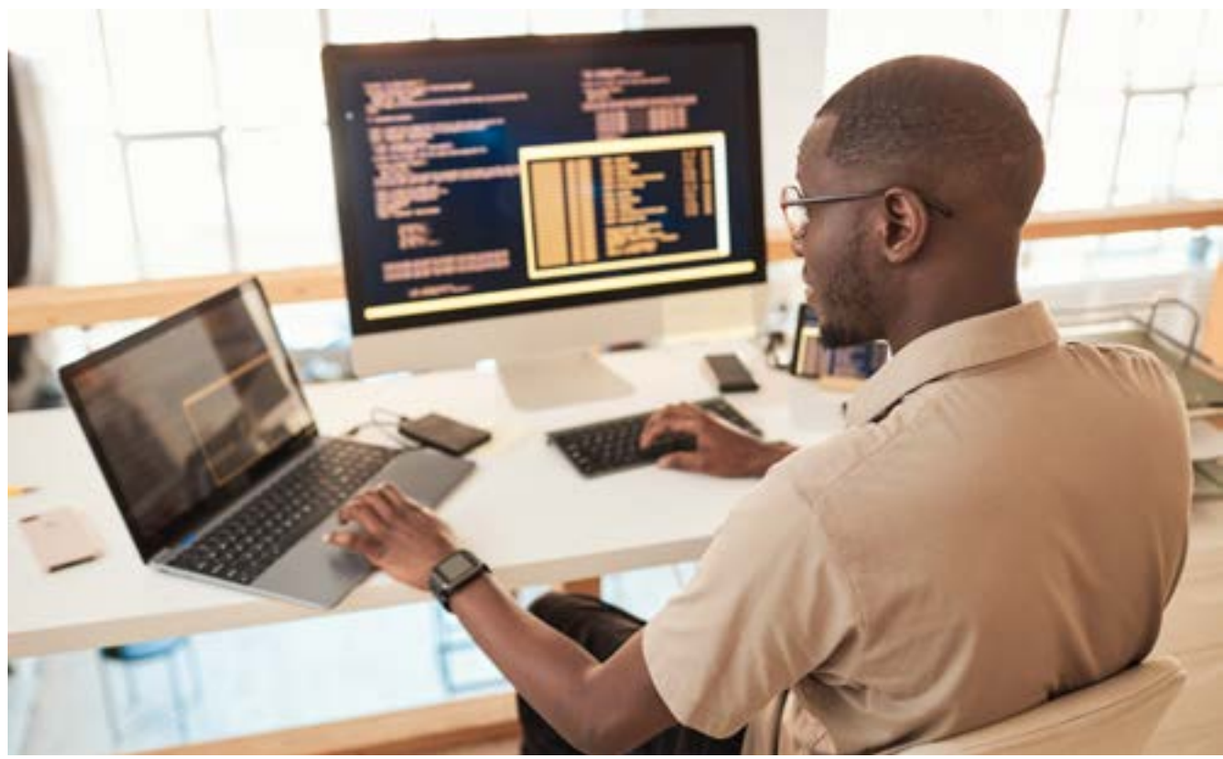
Zeroing In on Zero Trust: A Streamlined Strategy for a Secure Pivot

Organizations looking at the shift to zero-trust network architecture (ZTNA) should consider this five-step strategy.

By James Whewell, Senior. Solutions Architect, SonicWall

For organizations aiming to rapidly adapt their cybersecurity strategies to suit the evolving IT landscape while upholding utmost security, pivoting to zero trust is the optimal solution. By eradicating the antiquated notion of blindly trusting based on user location, zero trust requires thorough verification and authentication of all network traffic — be it internal or external — before granting access. This empowers organizations to uphold a resilient security posture and ensures data and devices are safeguarded against potential threats, no matter who is using their data, what device they are using, or where they are located.

While the shift to zero-trust network architecture (ZTNA) is recent, the ideas behind it are not.



A Quick History of Zero Trust

A lot has changed in the last 25 years or so, but the core principle of distrust remains. Even the marketing messages surrounding the topic are largely unchanged. A popular vintage marketing tag line, “Detect — Protect — Connect,” has the same essence as today’s “Don’t trust but verify.”

The 2000s gave birth to the SSL VPN revolution, which celebrated the death of VPN while

Previous Next

amplifying the benefits of clientless remote access rules. Twenty-plus years later, we're seeing this again with SASE/SDP. It comes down to crypto, packet encapsulation, and routing: When to route direct versus when to proxy versus when to do backhaul tunnel — these are all questions of trust. There is no one-size-fits-all answer to this. To build a highly resilient and scalable service, you must do all three (often, together) within a single session using just-in-time logic.

Streamlining the Zero-Trust Journey in Five Steps:

1. **Agile asset identification:** The first step in streamlining zero-trust adoption is to identify and assess assets with agility. This includes endpoints, networks, and cloud environments. By understanding the location and importance of assets, organizations can prioritize security efforts effectively.
2. **Reimagining the security perimeter:** Zero trust challenges the notion of a static security perimeter. Instead, organizations must redefine their security perimeters to encompass all critical resources, regardless of their location. This ensures that access is strictly verified and authenticated for every user and device, preventing unauthorized entry.
3. **Rapid implementation of multifactor authentication:** An integral aspect of zero-trust adoption is swift implementation of multifactor authentication. MFA fortifies security by requiring users and devices to provide multiple forms of identification before gaining access. By promptly adopting MFA, organizations can safeguard data and devices against potential threats.
4. **Seamless network segmentation:** The zero-trust model advocates for granular network segmentation to control access and reduce the attack surface. Organizations must ensure seamless and swift network segmentation to limit lateral movement within the network, mitigating potential risks.
5. **Continuous monitoring and adaptive assessment:** Streamlining zero-trust adoption involves embracing continuous monitoring and adaptive assessment. By deploying sophisticated security tools like security information and event management (SIEM) and user and entity behavior analytics (UEBA), organizations can quickly detect anomalies and respond proactively to potential threats.

As organizations embrace the fluidity of modern IT environments, zero-trust adoption emerges as a pivotal security strategy to protect data and devices from potential threats. Streamlining zero-trust adoption empowers organizations to swiftly transition to a dynamic cybersecurity approach without compromising on security measures.

By reimagining the security perimeter, implementing MFA, segmenting networks, and continuously monitoring, organizations can ensure a smooth transition while enhancing their security posture. By leveraging solutions that offer end-to-end remote access and granular access control, organizations can confidently pivot toward a zero-trust future, safeguarding their data and devices irrespective of user identity or physical location.