Symantec by Broadcom | Carbon Black. by Broadcom | ARROW

GUIDE

A Practical Guide

Security and Resiliency with Symantec ZTNA

Your Virtual Private Network (VPN) promises secure remote access, but what it really delivers is an open door to your network. Traditional VPNs assume that anyone inside the network perimeter can be trusted, and that's a problem. It turns every contractor, partner and third-party vendor into a potential breach vector.

When attackers compromise a single contractor's credentials, they don't just access one application; they can move freely across your entire network. Recent high-profile breaches have shown that third-party access has become the weak link in enterprise security.

Symantec Zero Trust Network Access (ZTNA) changes this equation, replacing blind trust with continuous verification and network-wide access with precise application-specific connections.

Why it's time to address the third-party access crisis

Traditional VPNs hand out full network access by design because they can't predict which applications users will need. This "all or nothing" approach means that a remote worker, consultant, or contractor hired to update your website can potentially access your financial systems, customer databases and intellectual property. Vulnerability scans and mapping techniques expose your entire network topology to anyone with basic credentials.

A visibility gap compounds this risk. Essential data for compliance and incident response sits scattered across multiple servers, appliances and locations in different formats. This leaves security teams struggling for information during incident response because user activities span disconnected systems. You can't defend what you can't see.

Bring-your-own-device (BYOD) access presents another problem. Contractors and partners often bring their own devices. Their company rules might not allow those devices to use your VPN, or your VPN might not support them.

Finally, VPN support means deploying complex DMZ configurations and firewall rules that drain IT resources. This also forces traffic through central data centers, creating bottlenecks that hinder remote work.

Building resilience with ZTNA

Zero trust flips the script on network security. Instead of assuming everyone inside the perimeter is trustworthy, it operates on a simple principle: never trust, always verify.

Every access request faces scrutiny under ZTNA. Systems evaluate user identity, device health, location, authentication method and even the specific application URI in an access request.

This software-defined perimeter approach focuses on protecting individual applications and hiding them altogether from unauthorized users. It follows a "least-privileged" access model and only allows access to applications to which the user has permission.

Symantec ZTNA replaces broad network access with point-to-point connections, creating secure tunnels between specific users and specific applications. **This helps deliver three key benefits:**

Performance

Point-to-point connectivity removes bottlenecks and reduces latency. Symantec's tests showed users enjoying 62% faster transaction times compared to traditional VPN connections. And with Symantec ZTNA running on Google Cloud, users can expect faster performance and improved scalability to address all users' needs.

Security

ZTNA limits the blast radius of a compromise by cloaking unauthorized parts of the network from the user. If an attacker compromises one credential, they gain access to exactly one application and nothing more. Lateral movement becomes impossible when there's no network to move through.

Resilience

Symantec's systems use Google Cloud infrastructure to deliver three availability zones per point of presence and one-click failover across global regions. That keeps it operational, even during natural disasters.

Security and Resiliency with Symantec ZTNA

Your phased roadmap to ZTNA implementation

Implementing ZTNA doesn't have to be disruptive. Symantec recommends a three-phase approach to unlock its benefits and deliver capabilities not found in a VPN.

Phase 1 – Deliver least-privilege access for remote users

Symantec ZTNA's least-privilege access model gives everyone access to only the applications they have permission to use. These applications are cloaked from the rest of the network, preventing malicious or unintentional access to sensitive applications and data.

Start with your remote workforce, including employees working from home, travelling sales teams and distributed staff who need secure application access. These users represent your largest attack surface and highest productivity impact. Enable agent-based access for managed devices and agentless access for BYOD scenarios. Symantec ZTNA supports web applications, native SSH for DevOps teams, RDP for remote desktop and TCP for legacy applications.

Once employees have secure access, extend the same protection to contractors, partners and suppliers. This approach proves value quickly with your core users while addressing third-party risks. It is also effective for mergers and acquisitions, as during the process the new organization may need to access the parent company's resources.

Your existing VPN can continue running during this transition, eliminating disruption while you validate the zero trust model.

Phase 2 – Enhance security controls by adding threat and data protection

This phase sees the addition of threat and data protection. VPNs create a security blind spot. They can't inspect traffic for threats or enforce data protection policies. Symantec ZTNA changes this completely.

Every connection to private applications now receives the same security inspection as any other traffic. Symantec ZTNA integrates directly with Symantec Threat Intelligence Service, which scans all files for malware and malicious content, as well as Web Isolation, which automatically protects users from unknown or suspicious sites.

Symantec ZTNA also syncs with Symantec Data Loss Prevention (DLP), so any existing DLP policies can be applied to ZTNA traffic, ensuring the same protections and restrictions are enforced.

Phase 3 – Roll out ZTNA to entire organization

This phase sees the deployment of Symantec ZTNA to the entire organization, not just to remote users. It gives everyone, including on-premises staff, a more secure method to access applications and resources.

With Symantec ZTNA, the same compliance rules that govern SaaS and web access now protect internal applications. Traffic inspection happens in the cloud without deploying proxies or backhauling through data centers, ensuring consistent protection whether users access cloud or on-premises resources. Application-level policies ensure that all users only see what they're authorized to access, with everything else remaining cloaked and invisible. Every access attempt generates centralized audit logs, giving you the visibility that VPNs didn't.

Also, you can deploy a single agent that handles ZTNA alongside existing Symantec tools, such as Cloud SWG, Cloud Access Security Broke, DLP and Web Isolation. This greatly simplifies deployment and management, with one agent used for multiple different use cases.

As you see positive results, you'll be ready to phase out your VPN infrastructure. It's no coincidence that 80% of concept pilots convert to purchases.

Security and Resiliency with Symantec ZTNA

Realizing the SSE advantage for modern enterprises

Consolidation eliminates tool sprawl. Combining ZTNA with Cloud SWG and DLP/CASB under the Security Service Edge (SSE) framework strengthens, streamlines and simplifies your security operations.

Symantec SWG customers already have a critical component of a Zero Trust framework. Now they can integrate it seamlessly with ZTNA, using the same agent, same management console and same policy framework.

The operational gains are immediate:

Deploy Quickly

Roll out the system in minutes instead of weeks.

Protect Everything

Symantec's Threat Intelligence Service and Remote Browser Isolation work across all services, providing unified protection against malware and emerging threats.

Simplify Management

Manage one security stack instead of juggling multiple vendors with different interfaces, licensing models and support processes.

Conclusion

ZTNA deployment is an effective way to remove transformational risk. It isn't just about saving money (although reducing vendor sprawl certainly helps the budget). It's about building a security architecture that scales with your business while actually reducing complexity.

Organizations clinging to "good enough" VPNs are accepting unnecessary risk. The technology exists today to eliminate lateral movement, secure third-party access and improve user experience and performance simultaneously.

The question isn't whether to implement Zero Trust Network Access; it's how quickly you can move.