WHITE PAPER

Symantec® Zero Trust Network Access

Essential Innovations for Secure Private Application Access

TABLE OF CONTENTS

Broadcom Delivers Leading ZTNA Technology

In 2019, Broadcom acquired Luminate Security, an innovative pioneer in Zero Trust Network Access (ZTNA) solutions. This technology, now part of the Symantec® security portfolio, enables security and IT teams to create a Zero Trust application access architecture without traditional VPN appliances. It securely connects any user from any device, anywhere in the world to corporate applications, on-premises, and in the cloud, while all other corporate resources are hidden without granting access to the entire network. This obfuscation prevents any lateral movements to other network resources while eliminating the risk of network-based attacks.

It is also delivered as an agent-based solution through the Symantec Endpoint agent or Cloud Secure Web Gateway (SWG) agent. Any Broadcom customer with one of these agents already deployed can instantly provision Symantec ZTNA. It can also be deployed in minutes to support agentless access for third-party or BYOD devices. Security and IT professionals get full visibility of users' actions when they access corporate resources, as well as real-time governance of these resources.

Analyst firm, KuppingerCole, recognized Symantec ZTNA as an "Overall Leader" in their 2022 Leadership Compass report for ZTNA, and they noted that the Symantec solution "uses Zero Trust Access principles in delivering point-to-point connectivity without agents or appliances, eliminating network attack surfaces and cloaking workloads from the Internet."

ENHANCE YOUR SECURITY WITH OUR BEST-IN-CLASS SYMANTEC THREAT PROTECTION BUILT INTO OUR ZTNA SOLUTION AT NO ADDITIONAL COST

Must-have Elements of an Effective ZTNA Solution

Industry analysts have identified ZTNA as a critical component of a complete SASE solution. ZTNA delivers a simple, secure access method that leverages a software-defined perimeter architecture that blocks users from viewing unauthorized applications or network resources. When searching for a ZTNA solution, understand that some capabilities are critical to a true ZTNA solution. What should you look for?

A Single Agent for All Security Services

Your ZTNA solution must leverage a single agent that is used for Endpoint Protection, Endpoint Detection and Response (EDR), SWG (formerly WSS), Cloud Access Security Brokers (CASB), and soon... Data Loss Prevention (DLP). The last thing you want to do is manage multiple agents that are fighting for the same resources, traffic, and DNS requests; and point fingers at different vendors when there is a problem. Zscaler and Netskope use Crowdstrike for EDR while relying on Microsoft Defender for Endpoint Protection. No other vendor has a single agent that includes network security routing, Endpoint Protection, and EDR. Only Symantec® agents include all these capabilities.

Question to consider: The last time you had an incident, which vendor took accountability for the problem if you have multiple agents?

Full Data Governance and Control

You must have a ZTNA solution that delivers full data governance and data control to keep your consistent compliance policies in place, regardless of the resource location. Zscaler, Microsoft, and Palo Alto Networks do not provide this functionality.

Questions to consider: Do you have multiple data centers? How are you planning to enforce existing DLP rules? When was the last time you made a change or update to your proxy server for DLP inspection?

Comprehensive Malware Inspection for ZTNA Traffic

You must keep your malware inspection in place as part of your ZTNA solution. ZTNA is more than just an access method, it is also a security tool. It must inspect all traffic through the ZTNA solution, and leverage the same multi-layered threat inspection supported by industry-leading threat intelligence. Netskope and Palo Alto Networks do not provide the level of threat protection that Broadcom delivers. We enhance your security with our best-in-class Symantec threat protection built into our ZTNA solution at no additional cost.

Questions to consider: Are you currently using an in-line threat inspection service to inspect your ZTNA traffic? How much does the license, management, and operation cost today? Would you like to entirely remove the cost and effort in its maintenance?

ULTIMATE PERFORMANCE AND THE ABILITY TO SCALE AND SUPPORT ANY NUMBER OF USERS

Native Agentless Access

While agent-based access is ideal for managed devices, your ZTNA solution must also have native agentless access for your resources, including native SSH and RDP access. Customers have invested heavily in their infrastructure and systems. They must be able to use their own tools and scripts and their own working environment, without losing those capabilities. Partners and third parties should be able to access the internal applications with no agent required.

Questions to consider: What are your plans to allow third-party partners, contractors, and consultants to access critical applications? Have you had security concerns about this? Are you aware that the number one attack vector in 2022 was through third-party partner access (60% of attacks)? - *2022 Verizon DBIR*

A ZTNA Solution that Improves the User Experience

Your ZTNA solution requires ultimate performance and the ability to scale and support any number of users. Broadcom runs our Symantec ZTNA solution on Google Cloud, along with the rest of our security stack. Our customers do not experience performance issues, problems scaling to a larger user base, or outages as other vendors have had. When a vendor manages their own PoP environment, they are responsible for creating optimized routing and building up data centers with more hardware to scale. The vendor must also manage their own failover capabilities. Other vendors, such as Zscaler, have experienced outages that have disrupted service. We are powered by Google to deliver a reliable and smooth user experience. Customers can proceed with confidence!

Questions to consider: Do you have multiple data centers across the globe? What are your plans to guarantee the best possible user experience?

Roll-Based Access Control (RBAC) and Automated Setup

Your ZTNA solution must simplify the effort of configuration and granting secure access. It must eliminate bottlenecks, not create them. It must support RBAC administration and provisioning automation. You need the ability to delegate access management or automate the process. Other ZTNA vendors do not have solid RBAC administration.

Questions to consider: How much time have you spent in the last month on VPN configuration? What are the costs for managing your VPNs?

Resources

- Product Brief: Symantec Zero Trust Network Access
- IDC Webinar: Security Transformation Enabling Remote Work
- Video: ZTNA with the Symantec Cloud SWG Agent (WSS)
- Report: KuppingerCole Leadership Compass, Zero Trust Network Access
- Blog: From Symantec's ZTNA Team: Planning to Replace Your VPN?

How are Organizations Using Symantec ZTNA?

As a cornerstone of a complete SASE solution, Symantec ZTNA delivers simple, secure access that prevents users from viewing unauthorized applications or network resources. It is available through Symantec Network Protection at no additional cost, and it is instantly deployed through existing Symantec agents. As a global technology leader, Broadcom uses our own Symantec ZTNA solution to deliver secure, smooth, and reliable application access to over 20,000 global users. You can also see immediate return for deploying ZTNA in your environment. Contact your Symantec product representative and create a plan for getting Symantec ZTNA set up.

Global Digital Services and Business Consulting

An international services organization of over 300,000 users had to immediately shift from on-premises work to remote work at the onset of the COVID-19 pandemic. With Symantec ZTNA, they were able to replace on-premise authentication, provide native RDP access, simplifiy their maintenance effort, and improve the user experience.

International Technology and Engineering

An engineering company with more than 60,000 employees had a growing demand to support remote work and BYOD. They needed secure access to sensitive applications from any device, managed or unmanaged. With Symantec ZTNA, they replaced 90% of their VPN use cases and delivered 24/7 access to global data centers, supporting hundreds of applications for thousands of users.

Online Marketplace for Freelance Services

The company delivers a multi-billion dollar marketplace for freelancers in 160 countries, and it had to provide granular access to internal cloud resources while allowing only specific actions when using an unmanaged device. With no change to the user experience, they provided seamless implementation of Symantec ZTNA for simple, secure access with no VPN. Onboarding was fast and they increased their visibility and data governance.

Electronic Commerce and Online Retail

The retailer was undergoing a digital transformation project while supporting over 20,000 employees. They wanted to get rid of their dated VPN technology, yet still, provide secure access to internal resources and applications for managed and unmanaged devices across the globe. They used Symantec ZTNA and rapidly onboarded thousands of users accessing multiple apps. With a one-step rollout, they met the objectives of the security operations center and network teams, with no business impact.

For more information, visit our website at: www.broadcom.com

EI-ZTNA-WP100 February 28, 2023