Symantec by Broadcom | Carbon Black. by Broadcom | Arrow

ZTNA vs VPN

Why Zero Trust Network Access Wins

With the rise of remote and hybrid work, cybercriminals are targeting the growing attack surface. To counter this, enterprises must deploy solutions that follow and protect users everywhere. When evaluating remote access options, understanding the differences between VPN and ZTNA is crucial to find the best fit for your organization.Arrow Intro

Replace your costly VPN with a modern technology such as Symantec ZTNA. Understand why organisations are choosing ZTNA over VPN.

What's the difference between ZTNA and VPN?

Use Case	ZTNA	VPN
Security	✓ ZTNA provides secure, segmented access, providing employees access to the resources they need, preventing lateral movement throughout the network. That access is constantly controlled through policy and audited in real-time for every user, device and action. ✓ ZTNA keeps IPs hidden from the internet, making the corporate network invisible to unauthorized users.	✗ VPNs increase the potential exposure of sensitive data by granting full access to the entire network surface. Without just-in-time privileged access, resources are left vulnerable to potential attacks. ✗ VPNs expose ports to the internet to enable network access, which makes them a target for malware and ransomware attacks.
Trust & Access	✓ ZTNA operates on a Zero Trust model: no implicit trust, continuous verification of users and devices. ZTNA enforces secure access to only what a user needs and has been provisioned to access, otherwise known as "least-privileged" access. ✓ Native Agentless Access – so partners & third parties can access apps.	✗ VPNs reinforce the traditional perimeter-based security model, which grants implicit trust within the network: once connected, users have broad access to the network. This makes it easier for malicious entities to access the network and exploit critical data and resources.
Control & Visibility	✓ ZTNA provides full visibility of users' actions when they access corporate resources, and enforces governance of those resources.	✗ VPNs lack the granular control and visibility needed to effectively secure remote access. VPNs primarily provide network-level access. Activities performed by users connecting to applications make end-to-end tracing extremely difficult.
Ease of Use	✓ ZTNA provides seamless user experience –allowing users to access applications without having to worry about setting up a connection or knowing where an application is located.	✗ VPNs can negatively impact organizations by reducing productivity and overall operational efficiency. Connecting to a VPN can be time-consuming, and if the VPN is slow or frequently disconnects, it can significantly disrupt business operations, leading to slow connections and frequent interruptions.
Scalability	✓ ZTNA enhances performance by utilising a cloud-based architecture, providing the nearest access path to both the user and the application, and benefiting from the cloud's scalable capacity.	✗ VPNs are difficult and cumbersome to scale, often leading to increased management complexity and operational maintenance costs, while also suffering from performance issues due to bandwidth limitations, network congestion, and latency.

Benefits of Symantec ZTNA

Reduce your attack surfaces and risk of data breaches.

With Symantec ZTNA, access is granted at the application level rather than the network level, restricting access to necessary applications and resources and stopping authorised users from moving laterally beyond their approved applications, minimising the risk to sensitive data and enhancing overall security.

Full Data Governance and Control

Do you have multiple data centres? How are you planning to enforce existing DLP rules? Can you ensure only the right people are accessing the right data?

Symantec ZTNA delivers full data governance and data control ensuring consistent protection and compliance posture. It keeps your DLP rules and compliance policies in place, regardless of the resource location. All of your Symantec DLP rules can apply to any traffic crossing over a secure ZTNA connection.

Complete Visibility and Control

Symantec ZTNA delivers full visibility of users' actions when they access corporate resources, as well as real-time governance of these resources. The Symantec ZTNA clear management approach makes enforcing policies and monitoring easier, ensuring that any suspicious or malicious actions are blocked.

Maintain compliance

To ensure you meet those compliance regulations, you can enforce the DLP rules in the cloud as part of the ZTNA inline data path. This policy will maintain compliance, while requiring zero effort from the IT administration team, delivering users a great experience with low latency, regardless of the user or application's location.

Comprehensive Malware Inspection

ZTNA is more than just an access method, it is also a security tool. Symantec ZTNA inspects all traffic and leverages the same multi-layered threat inspection supported by Symantec's industry-leading threat intelligence.

Simplifies and improves end users experience

- Symantec ZTNA reduces complexity through a simple, agent or agentless deployment, without needing changes to existing security configurations.
- It easily integrates with existing identity and access management solutions. Authorized users can connect from anywhere in the world, using any device. This allows them to securely access any hosted application on distributed data centers, either in a private or public cloud; or on-premises data centers.
- Symantec ZTNA simplifies administration with the use of Role Based Access Controls (RBAC). RBAC allows you to delegate administration privileges to individual teams, reducing complexity, cuts down administrative overhead, improves operational effectiveness and security resilience.
- Symantec ZTNA streamlines policy creation providing fast, agentless, and secure access to corporate applications and resources, regardless of location.

Scalability

- Symantec ZTNA is run on Google Cloud, along with the rest of our security stack, improving performance issues, overcoming the problems of scaling to a larger user base, and preventing outages.
- It optimizes the application access route across Google's global Internet infrastructure, avoiding delays that other ZTNA offerings experience when traffic is forced to travel across public Internet routes.
- As organizations scale, RBAC simplifies the process of granting and revoking access to temporary users as administrative roles can be adjusted across groups rather than individual users. Through RBAC you can control what end users or contractors can do at the broad or granular level and establish time constraints for content access.

Symantec ZTNA
A key component of Symantec Security Service Edge

As organisations continue to adapt to the this new digital landscape, the choice between Symantec ZTNA and traditional VPNs becomes increasingly clear. Symantec ZTNA addresses the limitations of VPNs, providing enhanced visibility, control, and security resilience.

In addition, Industry analysts have identified ZTNA as a critical component of a complete SSE solution. ZTNA as part of an overall SSE solution provides the following benefits to an organisation:



More Secure: By minimizing attack surfaces, it makes it easier to detect and respond to real threats. Furthermore, Symantec ZTNA inspects all traffic using Symantec's integrated Threat Intelligence Service to prevent the upload of malware files to applications.



Faster and more reliable: Symantec ZTNA is run on Google Cloud along with the rest of our SSE security stack. This has resulted in smooth performance, seamless scalability to a larger user base, and reliable uptime.



Improves Compliance: The unified approach helps maintain consistence compliance with industry regulations by providing detailed audit trails and governs internal resources through existing DLP compliance rules.



Granular Control: Enable access control and network visibility down to the level of specific applications and identities and ensure "least-privilege" access.

Symantec by Broadcom | Carbon Black. by Broadcom | ARROW

Learn more about
Symantec Network Protection