PRODUCT BRIEF

## AT A GLANCE

Symantec® Zero Trust Network Access (ZTNA) is a critical component of a complete SASE solution.

## ZERO TRUST ARCHITECTURE ELIMINATES APPLICATION EXPOSURE

- Least privilege access reduces the attack surface
- Application-level connectivity between authenticated users and applications
- No inbound connections to the network cloak applications from attackers

## ANY DEVICE, ANY LOCATION, ANY CLOUD

- Agentless access for all types of applications (web, SSH, RDP, TCP) from any device, in any location, in any cloud
- Single-agent application access option alongside the Symantec EPP, EDR, Cloud SWG, CASB, DLP, and ZTNA security stack
- Seamless, native, and best-in-class user experience without a VPN

# Symantec® Zero Trust Network Access

## Anytime, Anywhere, Any Device Access to Cloud-Hosted or On-Premises Applications

### The Need for Zero Trust Secure Access for Cloud and On-Premises Applications

Providing access to corporate applications and services for authorized users was straightforward when everything was located in large corporate data centers and users all resided in predictable locations, using corporate-issued devices. Inside the network perimeter, users had full visibility to see applications and services. Outside the perimeter firewall, they used tools such as VPNs to get access to the corporate network and then to the applications required to do their work.

The cloud generation has forever changed the way employees access information, and IT has had to keep pace. Moving applications to the cloud, without sacrificing user mobility and anywhere-access is paramount. This transformation has created significant complexities and has exposed security vulnerabilities that exist in traditional VPN access methods. These challenges include the following vulnerabilities:

- **Wide network surface attacks:** Vulnerability scans and other techniques expose the entire network and map available applications. Traditional solutions frequently lack just-in-time privileged access, granting full access to unneeded resources.
- **Lateral movement:** Creating direct connectivity with the mesh of services and clients significantly increases the chance for lateral movement.
- **Lack of visibility:** Activities performed by users connecting to applications make end-to-end tracing extremely difficult.
- **Complex maintenance and scalability challenges:** Deploying multiple gateways to support all possible traffic backhaul options require DMZ and firewall setup, which is expensive and complicated.
- **Poor user experience:** The inability to support third-party contractors with their own devices hinders productivity. Backhauling traffic leads to higher latency, inconvenience, and a poor user experience.

Today's dynamic business environment, sophisticated threats, and cyber attacks present unique challenges that require a new mindset, one that moves past a dated, perimeter-based approach that exposes corporate networks and applications and is not built for the cloud era.

## EFFORTLESS ADMINISTRATION

- Rapid onboarding with Zero Touch Provisioning
- Manage access to any hosted application in any cloud and on-premises data centers
- Full audit trail of user activities within an application

## DATA GOVERNANCE AND PROTECTION

- Fine-grained policies based on identity, location, device state, action, resource accessed, and data compliance level
- Symantec Advanced Threat Protection and Content Analysis for deep inspection
- Data compliance with Symantec Data Loss Prevention Cloud inspection
- Policy-based Remote Browser Isolation for traffic over the ZTNA connection

# Symantec Zero Trust Network Access

Symantec Zero Trust Network Access (ZTNA) is a cloud-delivered service providing highly secure, granular access management for enterprise applications deployed in IaaS clouds and on-premises data center environments. Symantec ZTNA eliminates inbound connections to your network, creates a software-defined perimeter between users and corporate applications, and establishes policy-based application-level access. This service ensures that all corporate applications and services are completely cloaked and invisible to attackers, addressing the whole set of challenges where traditional solutions struggle.

Compared to the legacy perimeter-based solutions, Symantec ZTNA provides the following functionality:

- Delivers the must-have component of SASE for security access to applications, as outlined by industry analysts.
- Eliminates network surface attacks by cloaking the applications from unauthorized users and preventing lateral movement of authorized users beyond their approved application.
- Integrates with any existing identity provider, ZTNA continuously reauthorizes the user's access and activity in real-time within a context-based least privilege approach, validating each and every request across a wide set of security parameters.
- Uses Symantec DLP to provide full data governance and monitoring control to enforce allowed activity policies and in-line data inspection for compliance and malware threat protection.
- Inspects all traffic against Symantec Threat Intelligence Service and also utilizes Remote Browser Isolation when needed, delivering enhanced threat protection for ZTNA traffic.
- Shifts the security paradigm to fully address modern security challenges.

Symantec ZTNA provides a best-in-class user experience by taking the application traffic from an end user directly to the application as quickly as possible, no matter their location. Symantec ZTNA provides the following benefits:

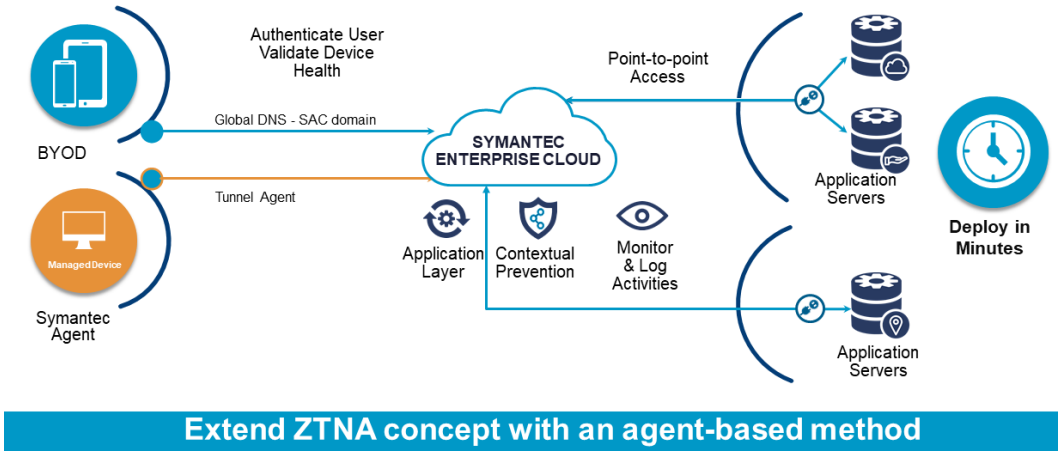
- Being a born as a cloud service, it optimizes the application access route, avoiding unessential delays caused by network traffic backhaul architectures.
- Symantec ZTNA leverages the Google Cloud infrastructure, bypassing congested public Internet routes for an improved user experience when accessing the organization's applications.
- Agentless application access grants users the flexibility to access applications from any device.
- Seamless access, without a gateway, to any application (IaaS, PaaS, web, or internal).

In contrast to the traditional perimeter-based solutions, maintenance and scalability challenges disappear for Symantec ZTNA. The need for the complex deployment and maintenance of dedicated security gateways is eliminated.

## Rapid Onboarding

Symantec ZTNA reduces complexity through a simple, 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. The connection allows them to securely access any hosted application on distributed data centers, either in a private or public cloud, or on-premises data centers.

Figure 1: Access with ZTNA




### How It Works

When an authenticated user requests remote access to a corporate resource, Symantec ZTNA creates and continuously monitors a temporary secure connection between the user and the requested resource. A bidirectional HTTPS connection is established at the application layer and eliminates the need to allow users onto the entire corporate network. The connection is transient and automatically terminates once the user completes their task. With Symantec ZTNA, users gain access only to the specific applications and resources for which they are authorized. The solution takes the zero-trust access approach further by providing full visibility, governance, and contextual enforcement for user actions, monitoring and logging every operation for simplified auditing and reporting.

## Use Cases

### Securing Access to Corporate Applications Migrating to the Cloud

As enterprises migrate applications to the cloud, IT teams must provide users with secure and frictionless access to the resources they need to remain productive. The solution must eliminate the complex setup and maintenance of tools that were not designed to address the security and compliance challenges of a perimeterless world.

Symantec ZTNA provides fast, agentless, secure access to corporate applications and resources, whether located in the cloud or on-premises data centers. Granular policies define access controls based on user identity, device posture, the sensitivity of the application, and the operations the user performs. Users are never granted broad network-level access, and they are provided instead with narrow connections to specific applications based on the trust profile of the user.

### Securing Access for Personal Devices and Third Parties

User mobility and BYOD have become the new norm. Employees need to be able to access corporate applications easily and quickly, regardless of their location or the device used. The current dynamic business ecosystem often requires providing third parties, such as partners or suppliers, with access to corporate resources or systems, without exposing the organization to attack. Symantec ZTNA provides authenticated, zero-trust access to corporate resources without giving any network access. Remote users and partner employees can access specific applications based on their identity and device posture, and security professionals can take real-time actions to block undesired and suspicious activity.

### Driving Productivity After a Merger or Acquisition

Merging IT operations after an event such as a merger or acquisition is a complex and risky process, as it involves merging two or more different security architectures and potentially exposing sensitive data to new threats.

Users often suffer from poor or no connectivity to needed resources, slow performance, and cumbersome steps just to reach an application. Symantec ZTNA is designed to allow secure, seamless, and instant access to internal resources following a merger and acquisition closing. A simple setup is all that is required to securely expose the applications to the new organization's users for immediate access and productivity, without the need of deploying and managing a VPN.

### Securing Access for DevOps Environments

DevOps teams require access to both production and development environments. Securing these environments from unwanted parties and unauthorized users is crucial to keeping your organization running safely. Symantec ZTNA automatically provisions or removes access to your VMs, PaaS workloads, and applications in seconds, using a cloud-native, API-driven agentless solution. It ensures access to DevOps environments is authenticated, provided just in time, based on the principle of least privilege, and fully audited and recorded.

### Organization Compliance

A cornerstone of an effective SASE framework is data protection that follows established governance policies that have been developed over years. Enforcing the compliance rules for many applications sitting in different cloud data centers can be complex. As organizations shift applications to the cloud, securing data with a SASE vendor with Cloud Data Loss Prevention (DLP) expertise (such as Broadcom), security teams can enforce the DLP rules in the cloud as part of the ZTNA inline data path.

## Benefits of Symantec ZTNA

The following table summarizes the benefits that differentiate Symantec ZTNA from traditional solutions.

| Differentiator | Benefit |
|---|---|
| Easy Licensing | *Symantec ZTNA is available through simple per-user licensing and is a critical component of a complete Symantec SSE solution.* |
| DLP Integration | *Symantec ZTNA integrates with Symantec Data Loss Prevention, enabling organizations to enforce data governance policies.* |
| Agentless Access for BYOD | *Support personal devices from roaming users, third-party partners, or consultants to ensure secure access to corporate resources and applications.* |
| Support for DevOps | *Access to DevOps environments, such as VMs, PaaS workloads, and applications, is provided or terminated in seconds based on least privilege.* |
| Symantec Threat Intelligence Service | *Symantec delivers the largest civilian threat intelligence network and allows advanced threat inspection of all traffic over the secure ZTNA solution.* |
| Symantec Remote Browser Isolation Integration | *Enable policies to deliver traffic through Symantec Remote Browser Isolation for an added level of protection, without disrupting the user experience..* |
| Single Agent for Managed Devices | *Symantec customers can use the Symantec Endpoint or Cloud Secure Web Gateway client for rapid ZTNA onboarding to allow users secure access to corporate resources, with minimal operational effort.* |
| Cloud-Native Solution | *Built natively in the cloud, Symantec ZTNA leverages the power of Google Cloud for ultimate performance and scalability, regardless of the organization's size.* |

BROADCOM®
connecting everything®

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



SYM-ZTNA-PB102 April 4, 2025