HAUMOUN
IT PIONEERS

Symantec
by Broadcom Software

WHITE PAPER

Symantec® Zero Trust Network Access

Four Use Cases to Solve Real-World Connectivity Problems and Drive Business

WHITE PAPER

Symantec Zero Trust Network Access

Four Use Cases to Solve Real-World Connectivity Problems and Drive Business

Symantec by Broadcom Software

TABLE OF CONTENTS

Instantly providing services to customers has become a differentiator for many businesses today. However, when it comes to providing employees or partners with instant access to the organization's internal resources, this urgent *need for speed* clashes with reality. Large organizations are being pressed to address connectivity challenges to both internally-hosted applications and those applications that might have been moved to the cloud. IT and security professionals are tasked to deliver *right-now access* without sacrificing the *must-have security requirement* that today's threat environment demands.

We will analyze the following four common application connectivity challenges that organizations face:

- Enabling secure remote work
- Accelerating productivity after a merger or acquisition
- Supporting an IT consulting partnership
- Ensuring consistent data security compliance

Is there anything close to a magic solution that allows organizations to deliver secure access to private applications, in the cloud or on-premises, at the scale and speed that modern businesses require? The answer is, *yes*. Zero Trust Network Access (ZTNA) is a critical component of a complete Secure Access Service Edge (SASE) solution that delivers swift, secure access to critical applications.

In this document, we will illustrate how ZTNA enables the instant access that users demand and the security that the organization must enforce.

TRUST NO ONE UNTIL VERIFIED AND LIMIT ACCESS TO ONLY ALLOWED APPLICATIONS AND RESOURCES

ZTNA Overview

Zero Trust is a security concept that relies on the *assume you have been breached* approach. The goal of Zero Trust is to trust no one until verified and limit access to only allowed applications and resources, thus reducing any possible impact and minimizing damage in the event a breach occurs. ZTNA is a security technology that emphasizes the importance of authentication, authorization, and auditing for every user, device, and action before granting access to the application. ZTNA supports the Zero Trust framework and enforces secure access to only what a user needs and has been provisioned to access. The following four points characterize an effective ZTNA solution:

- Cloak the applications from the outside network so that they are only visible to authorized users, not threat actors.
- Deliver Least Privilege Access so users are granted secure access only to what is necessary, not the entire network.
- Authenticate, authorize, and audit every request performed by the user.
- Provide full visibility and granular policy control to security professionals.

ZTNA provides secured, point-to-point connectivity between the corporate users (employees, contractors, partners, and others) and the corporate resources, isolating the corporate resources from the end user's network, as well as the Internet. Every instance of user access is authenticated and the device is inspected and validated for compliance before access is granted.

Modern ZTNA solutions (such as Symantec® ZTNA) allow real-time governance of the user's access and provide a full audit trail of all actions within corporate applications. Remote workers and contractors who have their own unmanaged devices are still given access only after authentication and establishing that their device is secure. Any suspicious or malicious actions are blocked.

Now let us examine where ZTNA can be applied in real use cases.

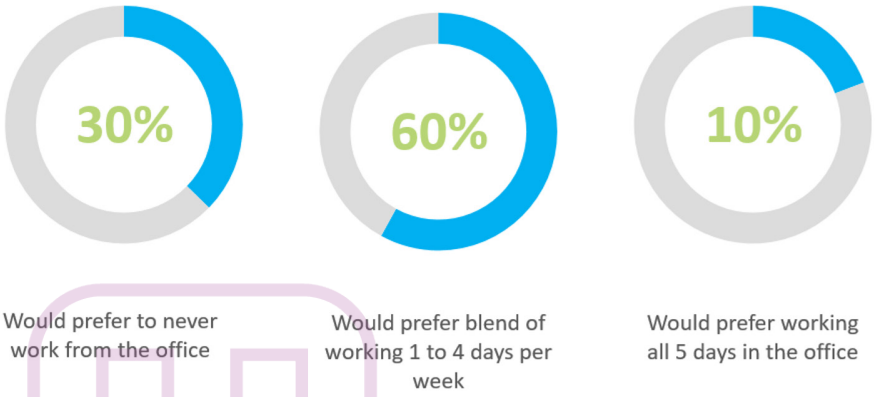
Use Case: Enabling Secure Remote Work

One of the key challenges that ZTNA can help solve is to support secure and productive remote work. Overnight, the workforce moved from offices to homes, airport lounges, public parks, or the corner cafè, creating a large number of security challenges. The COVID-19 pandemic increased the adoption of remote work and forced organizations to find ways to securely connect their employees to the corporate network from any location, almost instantly.

CREATE SECURE, SEGMENTED ACCESS FOR REMOTE EMPLOYEES, PROVIDING ONLY NECESSARY ACCESS AND PREVENTING LATERAL MOVEMENT THROUGHOUT THE NETWORK

Even with the decline of the pandemic, it is clear the work-life blend has been changed forever. Remote work is the new normal for many and here to stay. Research shows that 37% of desks will be empty and that 60% of employees prefer some form of blended office and remote work.

Figure 1: Employee Work-Life Preferences



When only a few traveling workers needed access to corporate applications, the burden fell on VPNs. They have traditionally been the go-to solution to create a secure connection and backhaul traffic to the remote application. However, modern network architecture exposes the limitations of VPNs for the following reasons:

- VPNs lack the granular control and visibility needed to effectively secure remote access.
- VPNs are not suitable for use cases where workers bring their own devices.
- Large organizations require a scalable solution that VPNs cannot support.
- VPNs expose the entire network surface to a potential attack as users are granted network-level access.
- IT professionals complain that VPNs are cumbersome to set up and not ideal to use for public cloud access.

Compare this model to ZTNA. It allows organizations to create secure, segmented access for remote employees, providing only necessary access and preventing lateral movement throughout the network. Employees can only access the resources they need through managed or unmanaged devices, and that access is constantly controlled through policy and audited in real-time. This control helps prevent unauthorized access or data leakage, yet still fosters productive work from remote users while maintaining adherence to proper business and security operations.

SUPPORT SUDDEN GROWTH IN REMOTE WORK AND MAINTAIN A POSITIVE USER EXPERIENCE, REGARDLESS OF THE USER OR APPLICATION LOCATION

But what about a global, distributed organization with users and resources spread across the globe? ZTNA is designed for just this type of organization. As a cloud-native service, ZTNA scales easily for any size organization, satisfying the need to support sudden growth in remote work and maintain a positive user experience, regardless of the user or application location.

Figure 2: Example of Global Distribution

Use Case: Accelerating Productivity After a Merger or Acquisition

Now that the merger is over, it is time to integrate IT systems. Executives want systems from each side of the merger to be accessible and drive productivity, and they want it now. IT teams that are tasked with granting swift access may be at odds with security professionals who are concerned with security and potential compromise to corporate applications or resources. Balancing the objectives of both organizations can be difficult and productivity is less than expected.

According to Accenture, 45% to 60% of the expected benefits from acquisitions depend directly on effective IT integration. The combined organization cannot function effectively and leverage business synergies until the IT infrastructure and applications of the acquired business unit are integrated with the acquirer's existing systems and processes. Not surprisingly, IT integration is the second most frequent reason for acquisition failure.

Merging IT operations is a complex and risky process, as it involves merging two or more different security architectures and potentially exposing sensitive data to new threats. Split tunnel management, establishing appropriate segmentation, unifying firewall policies, creating cross-cluster connectivity, and concentrator convergence are difficult and time-consuming challenges.

UNIFY THE NETWORK ACCESS DATA PATH AMONG ALL ORGANIZATION'S ISOLATED NETWORKS

Yet, the operational complexity the IT Administration team must tackle is not the biggest challenge. The biggest challenge is preserving a positive and productive end-user experience. Post-acquisition, users often suffer from poor or no connectivity to needed resources. They experience slow performance and multiple steps to reach a specific organization's resource (such as disabling and enabling agents just to reach an application).

ZTNA is designed to allow secure, seamless, and instant access to the internal resources following a merger and acquisition closing. Running connectors (lightweight Docker containers) in the desired data cluster or data center is all that is required to securely expose the applications to the new organization's users for immediate access and productivity.

As a cloud-native service, ZTNA replaces the set of VPN concentrators that frustrate users and administrators. It also reduces network access compatibility challenges, and multi-vendor and multi-architecture conflicts.

Security professionals should recognize the huge value that ZTNA provides by unifying the network access data path. However, those security professionals still have to answer the question, "How do I handle the multiple Identity Providers (IDPs) that we have following the acquisition?"

That question is the last part to cover in this use case. ZTNA's ability to unify the network access data path among all organization's isolated networks allows the organization to leverage multiple, existing IDPs already in use for authentication. IT and security professionals can quickly provide needed access to any application from either organization to facilitate immediate collaboration and productivity, without rushing into the replacement of all building blocks of the network topology.

With that phased approach through ZTNA, organizations ensure that the integration process is seamless and secure while preserving a positive and productive user experience.

Use Case: Supporting an IT Consulting Partnership

The IT consulting business continues to grow, even in a down economy. IT consulting vendors and their customers often have the following questions when initiating a business relationship:

- How does the customer provide the consultant with only the necessary network resources and applications without exposing unnecessary network segments and ports?
- How does the customer provide access to these internal resources when the consultant's laptop does not have your organization's VPN agent or is even a restricted platform prohibited by the customer's policy?
- How does the customer avoid network conflict when a consultant's machine has its own VPN agent to access the network of the IT consultant's company?

Symantec ZTNA provides a very effective out-of-the-box solution to answer all of the previous questions.

INTERNAL RESOURCES CAN BE SECURELY ACCESSED FROM ANY DEVICE FROM ANY PLACE

Utilizing authorization policies that support least-privilege access, Symantec ZTNA allows security professionals to provide enough access to specific applications for consultant users. It also controls data governance by allowing or limiting particular actions (such as, GET, POST, file download commands to specific URIs) and enforcing granular control of the user's activity. While this amazing capability is achievable with a proper ZTNA vendor, it is not available in VPNs as they rely only on network-level connectivity.

But what about the third question on avoiding network conflict when the IT consultant is using their own VPN? Addressing this issue is a capability that Symantec ZTNA easily solves. It allows agentless access to any resource (web, SSH, RDP, or any custom application on top of UDP) with the same capabilities previously listed. Leveraging global DNS, the internal resources can be securely accessed from any device from any place, according to the customer's authorization policies.

Use Case: Ensuring Consistent Data Security Compliance

Moving to the cloud has long been an objective of many organizations, yet some are just embarking on their digital transformation journey. With the hopes to consolidate multiple data centers, provide a better user experience and cut operational and management expenses, executives have finally given approval to move applications to the cloud and implement a SASE architecture to support strong security.

However, a cornerstone of an effective SASE framework is data protection that follows established governance policies that have been developed over years. How does a company enforce the compliance rules for all of these applications that are now sitting in different cloud data centers?

Trying to solve this challenge with a VPN will lead to a *hairpin* architecture, steering the traffic from all data centers toward a single place where the data loss prevention (DLP) rules were enforced. This approach is challenging for both the IT team, which assumes responsibility for building such a complex setup, as well as for the users who are going to experience increased latency and frustration when uploading and downloading data.

Here ZTNA comes to the rescue again. As organizations shift applications to the cloud, securing data with a SASE vendor with Cloud DLP expertise (such as Broadcom), security teams 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.

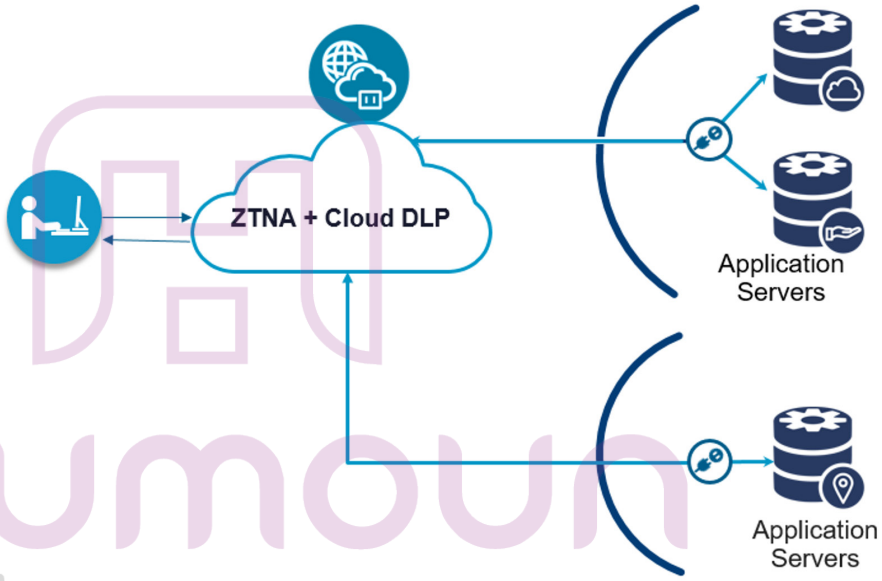
REDUCE THE RISK OF EXTERNAL THREATS, PROTECT SENSITIVE DATA, AND PRESERVE POSITIVE USER ACCESS TO NEEDED APPLICATIONS

Conclusion

ZTNA can be a powerful tool for organizations looking to secure their remote work, drive productivity after merger and acquisition events, enable secure and productive consulting partnerships, and maintain strict data security compliance as they progress through digital transformation.

With granular authentication, authorization, and auditing capabilities, coupled with strong data governance and DLP, Symantec ZTNA provides a cloud-native security service to help organizations reduce the risk of external threats, protect sensitive data, and preserve positive user access to needed applications.

Figure 3: Application of ZTNA and DLP



BROADCOM SOFTWARE

About Broadcom® Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software has an extensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

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

UC-ZTNA-WP100 February 24, 2023