Skyhigh
Security

WHITE PAPER

Going Above and Beyond Zero Trust Network Access

Table of Contents

Executive Summary

Virtual Private Networks (VPNs) are no longer an adequate solution for granting access to private assets such as internal applications, infrastructure, and data. VPNs are architecturally inefficient and lack robust security capabilities required by the work-from-home norms in a post-COVID world. Zero Trust Network Access, or ZTNA, is a promising replacement bringing a streamlined architecture, rich context awareness, and a granular, least privilege policy application.

The many ZTNA solutions available today can be categorized into two groups: stand-alone ZTNA vendors and platform players. Platform players follow a security service edge (SSE) architecture, incorporating synergistic technologies that yield superior security efficacy. A mature, holistic data security platform brings enterprise-grade data classification and unified incident handling in a single interface. Superior contextual awareness comes from a robust endpoint security stack, which provides a deep understanding of device posture and risk. User identity and behavioral analytics further support context awareness by identifying users exhibiting risky behavior, holding elevated permissions, or having access to sensitive data. User productivity is improved by enabling the use of unmanaged and mobile devices while still maintaining proper security posture. This can be accomplished using technologies native to the SSE platform, such as cloud access security broker (CASB) and remote browser Isolation (RBI).

Organizations should select a ZTNA solution that can bring not only the compelling architectural benefits inherent to ZTNA, but also the heightened security posture assessment level, which is available only when ZTNA is coupled with the larger framework of an SSE platform.

The Inadequacies of VPN

Today, corporate security organizations are pulled in many directions by multiple currents of change. The most widely felt is the evaporation of the traditional network perimeter, which is all but complete. This evaporation is the result of two other trends:

- The migration of infrastructure, applications, and data, to the public cloud
- The proliferation of remote users

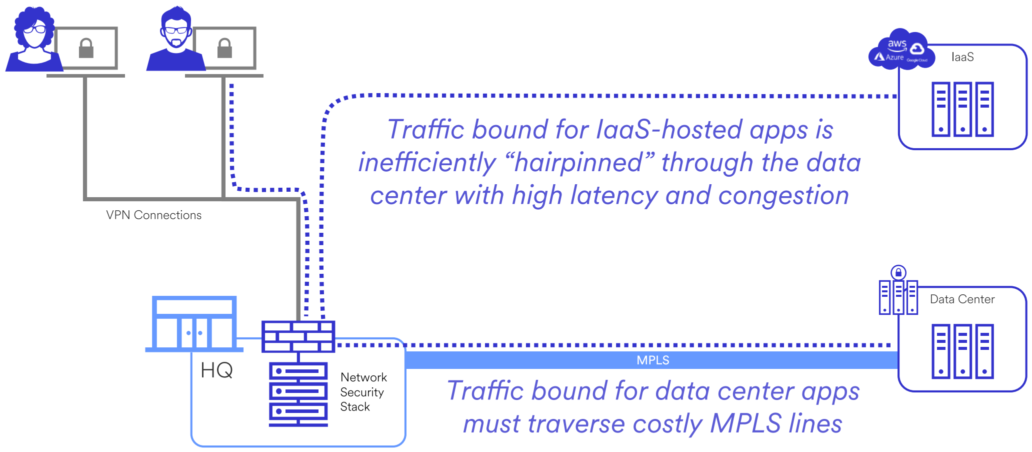
Today's norm involves users working from anywhere and accessing data in public cloud applications, such as Microsoft Office 365 or Amazon Web Services (AWS) housed outside of the corporate network. However, despite these ubiquitous trends, there remains a contingent of corporate assets that are, in fact, still defended by the traditional castle-and-moat approach of the corporate network perimeter. Often, these corporate assets have no foreseeable future where they are publicly available, but their users are increasingly remote. This presents security teams with the challenge of providing reliable, high-performance, and secure access to both these new cloud assets and retained onsite assets.

Traditionally, these challenges were met using virtual private networks (VPNs), which enabled remote users to be logically translocated onto the corporate network where they gained access to any corporate asset as if they were working in the building. This approach delivered strong outcomes for many years. The effectiveness of VPNs has been eroded. VPNs were designed in a time when remote access was the exception rather than the rule and when trust was more implicit and device-centric. Today, work happens anywhere, at any time, and from nearly any device. This is incompatible with the old paradigm, where a minority of users occasionally accessed internal applications exclusively from company-managed laptops.

Old Paradigm	Today
Most users were local and connected directly to the corporate network.	Offices are largely empty, with few people on the corporate network.
There was a very small proportion of remote and travelling workers.	The majority of users are working from home—many on a permanent basis.
Applications were hosted locally on the corporate network or in nearby data centers.	Users rely on a variety of corporate and personal devices to access corporate applications and data.
Users typically relied on their corporate PC to access applications and do their jobs.	Most users were local and connected directly to the corporate network.
Corporate networks were considered “safe zones,” where all applications and authorized users could be trusted implicitly to coexist.	Organizations are adopting Zero Trust, moving to “leastprivileged” access models to minimize security risk.

VPNs are a simple solution to the problem of remote access, but they take a suboptimal approach architecturally. Historically, this was acceptable because VPN was designed and sized for a small subset of users. Organizations typically deployed a small number of VPN endpoints regionally to supply remote access to internal assets. These VPN endpoints were sized for the small population that used them, and, consequently, they lacked a robust, global footprint to provide optimal reliability and performance. In addition, the private assets were often remote from the VPN endpoints, resulting in a hair-pin traffic flow.

For example, a user in Ohio may have connected to a VPN endpoint in California in order to reach a server hosted in a data center in New York. This, of course, introduced a significant amount of latency but also consumed expensive multiprotocol label switching (MPLS) lines. Today, it is likely that the asset may be privately hosted in a service such as AWS or Microsoft Azure. MPLS may be spared, but the traffic will then traverse the organization's internet pipe twice. This paradigm is untenable as the remote user population scales up.



Traffic bound for IaaS-hosted apps is inefficiently "hairpinned" through the data center with high latency and congestion

Traffic bound for data center apps must traverse costly MPLS lines

Figure 1. Inefficient remote access via VPN and MPLS.

VPN technology is a core component of the traditional castle-and-moat approach to security of the past. This all-or-nothing approach to security grants the keys to the kingdom to users based simply on the logical location of being "on the corporate network." Generally speaking, network connectivity to the organization's assets is granted based on a user's presence in a company office. VPNs extend this privilege to remote workers. If a user has a corporate laptop, a user account, and an internet connection, they can connect to any private asset and even discover assets they weren't intended to access. This approach is, at the same time, too permissive and too restrictive. It flies in the face of the modern idea of Zero Trust while also preventing the user from working from anywhere on any device. In contrast, when using a corporate issued laptop on VPN, all doors are open to the organization's most valuable assets. However, users are bound to a cumbersome laptop and a repetitive, time-consuming connection process while they are locked out from using more convenient devices, such as their mobile phones or tablets. This results in the worst of both extremes: it's too cumbersome and too insecure.

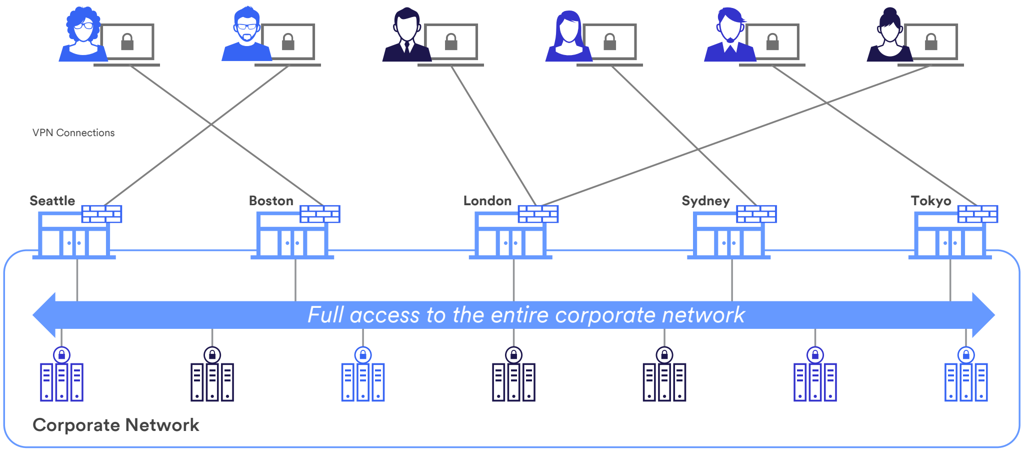


Figure 2. VPN access limitations.

ZERO TRUST ≠ ZTNA

Because of the common naming, many people are quick to conflate the terms Zero Trust and Zero Trust Network Access (ZTNA). However, these two terms while related are not the same.

A Zero Trust mentality allows organizations to restrict and compartmentalize access and data manipulation while still maintaining optimal user experience and productivity levels. Guidelines such as those from the National Institute of Standards & Technology (NIST) can provide a practical framework to explore and implement Zero Trust.

What is ZTNA?

The modern trend towards a Zero Trust security model and the dissolution of the traditional network perimeter laid bare the challenges and inadequacies of VPN technology. A new approach was needed, and the security market answered with a promising new technology, Zero Trust Network Access (ZTNA). ZTNA brings a Zero Trust approach to granting access to private applications, data, and infrastructure while also optimizing traffic flows and reducing infrastructure costs. The Zero Trust approach elevates security posture by enabling granular, context-aware access control to these assets. ZTNA solutions grant least privilege access while continuously validating indicators such as user identity and device posture. ZTNA also eliminates VPN infrastructure and allows remote users to directly connect to on-site assets without the need for hair-pinning traffic from one corporate location to another. Many ZTNA solutions today leverage a robust, global, multi-tenant cloud infrastructure offering levels of reliability and performance that few organizations could achieve internally. This simplifies network design, improves performance, and boosts availability, while reducing costs significantly. User productivity and the user experience are dramatically improved by providing an "always-on" connection to private assets without a cumbersome connection process. This can be extended to any device while maintaining appropriate device posture-based security controls.

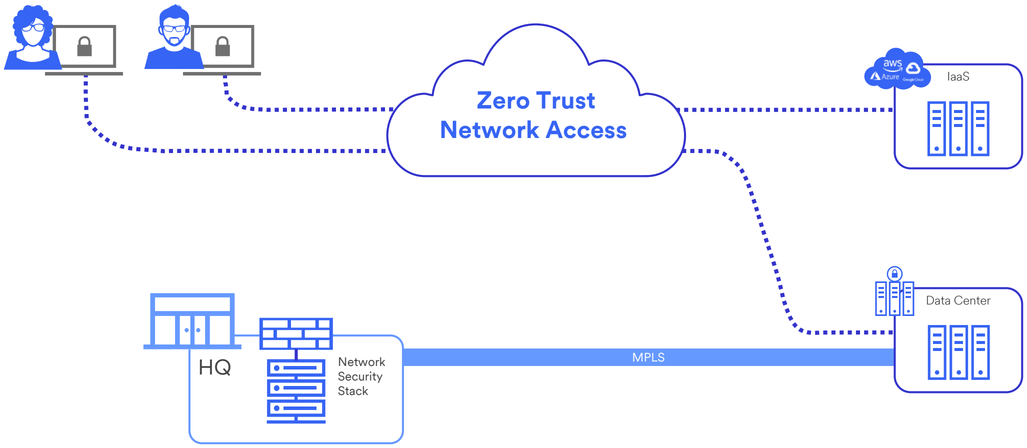


Figure 3. Direct-to-app connectivity with Zero Trust Network Access.

How Is ZTNA Used?

Fundamentally, organizations look to ZTNA for two reasons: improving on VPN's architectural deficiencies and up-leveling security.

Organizations are drawn by the fact that ZTNA typically brings a global, robust cloud infrastructure with superior performance, less deployment of on-premises hardware, and elimination of expensive MPLS links and hair-pinned network paths.

While the adoption of ZTNA had already begun, the rapid acceleration of work-from-home, triggered by the COVID-19 pandemic, caused an immediate, urgent need to take action. Nearly overnight, users overwhelmed VPN solutions that were sized for a fraction of the employee population. Not only were VPN endpoints overwhelmed, but the hair-pinning of traffic saturated internet pipes further impacting reliability and performance.

Many organizations quickly scaled up their VPN solutions to handle the load, but this was just a stop-gap measure deferring a true solution. These organizations will continue to see private assets move to public cloud IaaS services exacerbating the hair-pinning problem and further saturating their internet pipes. Seeing this inevitability has led many organizations to opt instead for a positive paradigm shift by deploying ZTNA.

Now that most organizations have been forced to address the scale of their remote worker connectivity solution, the primary draw for ZTNA today is the ability to apply a Zero Trust model to providing access to private assets.

Where VPNs grant access in an all-or-nothing manner, ZTNA is able to allow granular access with a least privilege methodology. This approach is applied by considering a much richer security context in their access policies, including elements such as user identity, user risk, and device security posture. Users are only granted access to the applications they need, using appropriate protocols and access methods, and access is contingent on a maintaining a trustworthy security posture that is continuously evaluated. This not only improves the overall security posture of the organization but it also enables properly limited access to unmanaged devices and third parties.

For instance, the security posture of a fully managed laptop with an up-to-date endpoint security stack may give the user access to certain assets that would be blocked from a privately-owned tablet. User productivity and satisfaction are also improved as an "alwayson" connection is available without a cumbersome connection process. Users are able to use any device from anywhere, and organizations are able to maintain a desirable security posture while enabling this level of access.

ZTNA Vendors

Today, there is a plethora of ZTNA solutions available from many vendors. Regardless of their differences in features and functionality, they all fall into two major categories: stand-alone ZTNA vendors and platform players. When ZTNA was in its infancy, many vendors entered the market with their own innovations as startup companies. The majority of the players in the market today are still stand-alone ZTNA solutions with their own strengths and weaknesses—some more capable than others. However, the market has matured over time, bringing more consistency, integration, and consolidation. Primarily, analyst firm Gartner has defined SSE as an emerging, consolidated market encompassing a multitude of mature technologies, including ZTNA. ZTNA is now a hallmark component of a new security paradigm with a much farther-reaching scope.

There are several critical factors to consider when making a decision to deploy a ZTNA solution. Many vendors offer dedicated ZTNA solutions that may offer unique features and capabilities. However, these solutions often come from a narrow view of ZTNA's role as simply a replacement for VPN, focusing solely on the architectural change. Other vendors offer ZTNA as a component of a larger SASE platform incorporating related technologies such as cloud access security broker (CASB), secure web gateway (SWG), data security, RBI, Firewall as a Service (FWaaS), and more. By the very nature of a converged, cloud-based SASE platform, these solutions achieve the desired architectural change. In addition, the breadth of the platform brings more valuable capabilities that enable the next level of secure access to private assets.

Data Security

The most likely reason for on-site assets remaining private is the presence of sensitive data. Many organizations are simply not willing to entrust their intellectual property or regulatory compliance to a publicly accessible, third-party solution whose infrastructure they do not directly control. Therefore, the primary consideration for applying a Zero Trust access policy to these assets is the protection of data. To this end, many ZTNA solutions do offer an often limited, built-in data security capability to prevent, for example, the download of sensitive data from an on-site Microsoft SharePoint server to an unmanaged device. However, this is often an entirely siloed data security solution offering no integration with a holistic data security platform.

The challenge of securing an organization's sensitive data cannot be overstated, and taking a piece-meal approach can spell disaster in many cases. Just the cost of simply defining what constitutes sensitive data can be tremendous both in financial terms and man-hours. Repeating this daunting task by redefining sensitive data multiple times using different engines that do not behave in the same way can multiply the cost and effort required and create coverage gaps. In addition, multiple incident management solutions must be used in order to achieve a "big picture" view of where data resides and how it's used. When considering a ZTNA solution, organizations must first rule out any solution that does not include a data loss prevention (DLP) capability, as they simply cannot deliver the level of data protection required. When evaluating the remaining solutions, pay careful attention to the maturity and robustness of the DLP engines to ensure they can accurately identify sensitive data without flooding security teams with false positives. DLP facilities that rely on simple dictionary-based scanning or regular expressions are not likely to yield accurate results.

However, a robust engine that includes data validation, exact data match (EDM), and indexed document matching (IDM) will be more successful in accurately protecting data without a flood of false positives. Organizations should also heavily favor offerings that exist as part of a larger platform that offers a comprehensive data security solution. This will allow the quick extension of existing data security classifications and policies to users and devices accessing the highly valuable and sensitive data residing in the private assets protected by ZTNA. Visibility into any data access or violations will be seamlessly ingested into existing tools, workflows, and processes. This ensures consistent DLP policy enforcement across vectors, as well as streamlined incident management, where all incidents can be viewed in a converged incident manager. These benefits are only offered by ZTNA solutions that are part of a larger, end-to-end data security platform.

Security Context Awareness

As discussed previously, taking a Zero Trust approach to granting access to private assets is now the key driver for most organizations abandoning VPN in favor of ZTNA. However, a Zero Trust policy is only as powerful as the security context on which it is based. Applying a Zero Trust approach without a deep understanding of user identity, user risk, data sensitivity, device posture, user location, and up-to-the-second threat intelligence doesn't sufficiently up-level the security posture of an organization. These critical policy elements are far from trivial to discover and require many additional information sources. This is one of the most critical reasons why ZTNA solutions should be part of an SSE platform, rather than a stand-alone solution requiring considerable third-party integration work that will drive up deployment costs and may not deliver optimal results.

Consider all the device posture elements that may be relevant to a policy granting access to an organization's critical, private assets:

- What type of device is it?
- What type of antimalware solution is installed? Is it enabled?
- When was the last full scan of the device, and have there been any malware detections recently?
- Is the organization's endpoint DLP solution installed and enabled?
- Is the storage encrypted?
- What process is attempting to connect to private assets?

Some of these questions can be easily answered by most ZTNA vendors, but others can only be adequately answered by an endpoint security vendor. Therefore, at least a deep integration, if not a full convergence with the relevant endpoint security elements, is required to achieve a proper level of endpoint contextual awareness.

User identity and risk awareness has now become another keystone in security context awareness and access policy. At an elementary level, this involves the user identity, which includes an authenticated username, preferably using multi-factor authentication (MFA), and user group memberships.

However, this is just the bare minimum. A proper Zero Trust policy will take into account additional user context, behavioral analytics, and business awareness. Questions to consider include:

- Does this user normally access this application or asset?
- Are they connecting from an unusual location? Is this a normal working hour for the user?
- Have we seen any strange behavior from this user recently?
- What sensitive data does this user have access to?

These answers are necessary to achieve a full understanding of the true risk posed by a user accessing a private asset. For instance, if a user in Europe is connected to an internal GitHub server, and then the same user account authenticates to Office 365 from China, then access to private assets may be immediately revoked due to potentially compromised credentials. A user's risk level should at least partially relate to the sensitive or classified data to which they have access—which again brings into question the data awareness discussed earlier.

Unmanaged Device Access

One of the great opportunities promised by the switch to ZTNA is the ability to provide access to private assets from either unmanaged BYOD devices or to third parties. VPN connectivity, in general, is only granted to devices that are managed by the organization, relegating employees to using their one corporate-issued device after a tedious connection process. Due to the all-or nothing nature of the access conferred, VPN connectivity represents the "keys to the kingdom" and cannot be risked for anything outside of a trusted, managed device. However, because ZTNA has more contextual awareness and grants least privilege, preferably with robust data awareness, it is possible to confer appropriately limited access to less trustworthy devices in these situations. While enabling secure access is the goal, the untrusted nature of personal, unmanaged devices calls for a more restricted level of access than a managed device.

As previously discussed, this hinges on a rich security context awareness and an ability to accurately classify sensitive data. However, understanding the risk is only half the battle, as there must be a technological way to properly control access in these less trustworthy scenarios and a method to apply this control to an unmanaged device without an agent. Not all ZTNA solutions on the market are able to provide access without installing software on the client device. Fewer solutions can fully assess the risks involved, and even fewer provide access in an isolated fashion that fully insulates private assets from the risk posed by untrusted client devices. Some less mature offerings may only have the ability to allow all access or block access entirely. Two key Security Service Edge (SSE) technologies today that can address these challenges are RBI and CASB.

RBI renders web-based content in a remote data center and only allows the client to view and interact with the remote browser. Absolutely none of the actual web content from the server reaches the client. This can enable a risky client to see and interact with a web application without being able to upload or download any content. Coupled with the reverse proxy capability inherent in most robust CASB solutions, this RBI approach can be used in a fully agentless way for unmanaged and third-party devices.

Reverse proxy enables a CASB solution to "plugin" to the single sign-on process performed using the SAML protocol and to achieve inline protection for unmanaged devices without any software installation. This powerful combination puts SSE platforms in a unique position to fully understand the risk and permit appropriately controlled access—and do so in a seamless, agentless fashion.

Introducing Skyhigh Security Private Access

Skyhigh Security Private Access is the industry's leading ZTNA solution that goes above and beyond the core Zero Trust benefits. Skyhigh Security Private Access provides data awareness to secure the highly distributed and hybrid workforce with integrated DLP and RBI capabilities.

Skyhigh Security Private Access utilizes a hyperscale service edge, operating at 99.999% uptime, to enable blazing fast, least privileged access to private assets from any location and device at any time. Deep data inspection and classification using Skyhigh Security's mature and comprehensive inline DLP engine keeps a check on inappropriate data handling by remote users. The innovative Skyhigh Security RBI offering, paired with reverse-proxy capabilities, shields private assets from untrusted and unmanaged devices by rendering the access over isolated web sessions.

Skyhigh Security Private Access seamlessly converges with our Security Service Edge (SSE) portfolio, which includes SWG, CASB, and DLP to address the core security requirements for Gartner's SSE framework. This uniquely positions our ZTNA solution as the best-in-class, integrated and cloud-delivered security solution, offering unified visibility and control across cloud, web, private apps, and endpoints.

Conclusion

In early 2020, the journey from legacy VPN deployments to modern ZTNA architectures was a train that had already left the station and was accelerating quickly.

However, the COVID-19 pandemic catapulted the technology into the mainstream nearly overnight. Today, organizations are presented with a multitude of compelling options to provide reliable, performant, and more secure access to private assets. However, the most game-changing ZTNA solutions will always exist as part of a larger whole, a SASE architecture. With a mature, end-to-end data security facility, deep device posture assessment, and a context-rich understanding of user identity and risk, SSE platforms are the most insightful solutions available. Coupled with native RBI and CASB technologies, granular access controls can provide appropriately restricted levels of access even in scenarios with elevated risk. These elements make up the private access capabilities that will empower business for the foreseeable future.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh
Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com