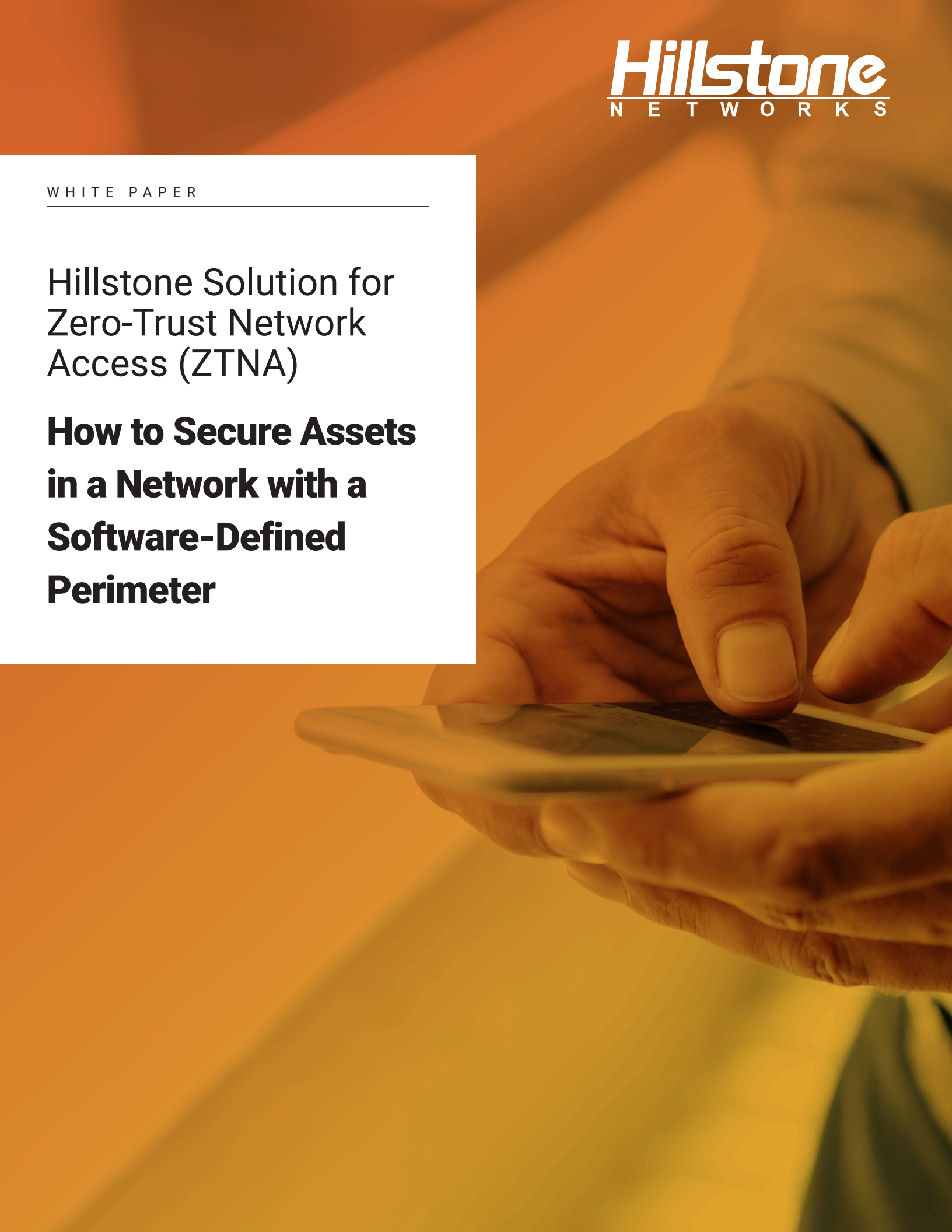
Hillstone NETWORKS

WHITE PAPER

Hillstone Solution for Zero-Trust Network Access (ZTNA)

How to Secure Assets in a Network with a Software-Defined Perimeter



Introduction

Even before the advent of the covid-19 pandemic the Work-from-home (WFH) and work-from-anywhere (WFA) industry movements were trending. Globally, CISOs were already looking to enable greater workforce agility and improve workplace flexibility. When the pandemic started, WFH/WFA quickly became the top priority for enterprises worldwide. Security and networking teams were then, and still are now, required to expeditiously onboard a plethora of remote workers—severely straining traditional VPN deployments designed to connect only a small fraction of employees. At the same time these teams had to, and must always, continue to protect against increasingly aggressive malware and ransomware threats. Employee home networks, being generally less safe, enable lucrative launching points for ransomware infections that lead to existential threats to companies.

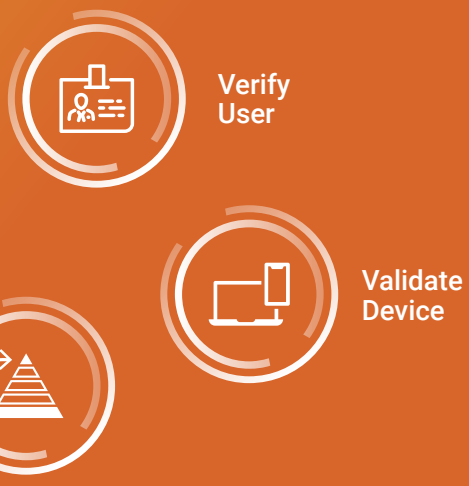
Even as the world slowly returns to normal, CISOs continue to be tasked with enabling secure multi-location access: on-campus networks, large physical locations, branch offices, employee homes, and across a mesh of worldwide public Wi-Fi and mobile networks.

Hillstone Networks has served CISOs well with a comprehensive portfolio of security solutions to ensure business protection—from the edge of the enterprise to core data centers. To meet the new access challenges posed by the enterprise's network edge becoming virtual and software-defined rather than a physical border around buildings, Hillstone is expanding its edge solutions suite to incorporate zero-trust network access (ZTNA).

Contents

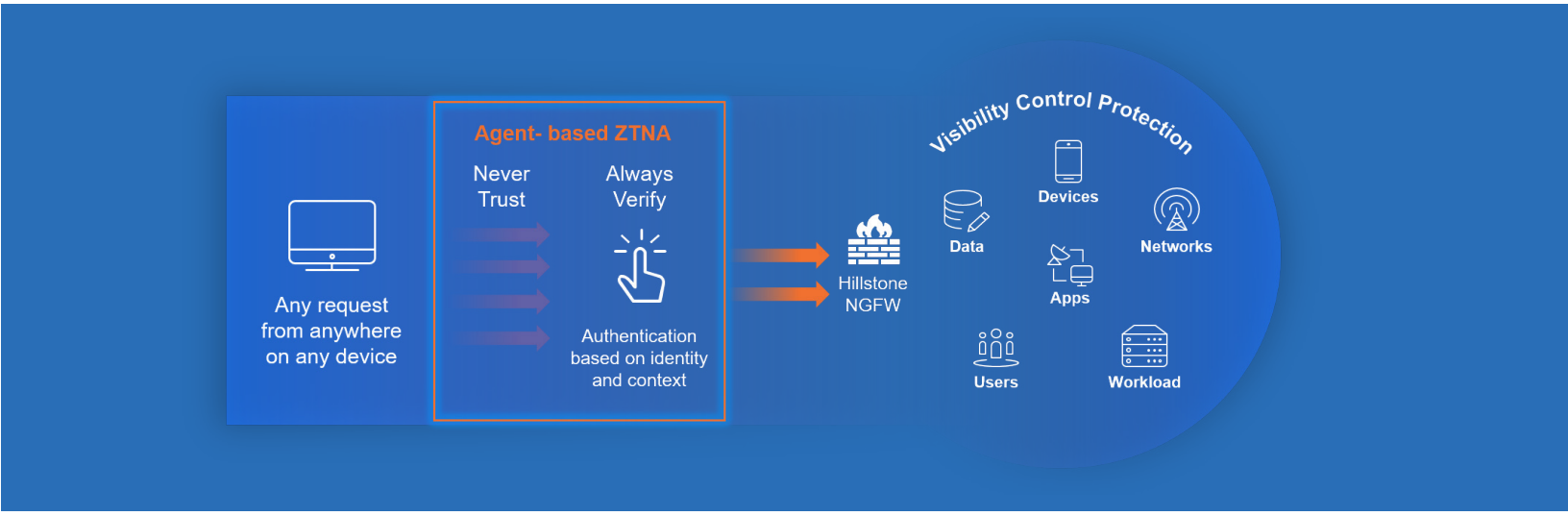
Learn about the Hillstone Networks Zero Trust Network Solutions

Visit us at **Hillstonenet.com**



What is ZTNA?

Zero-trust is a model of security founded on the concept of trusting nothing and granting only least-privilege access.



Many traditional security solutions tend to offer binary access models:

• Everything inside the perimeter is trusted to access (or at least to attempt to access) all resources, and all resources are visible to all internal users.

• Everything outside the perimeter is untrusted and has no access, and no resources are visible to outsiders.

VPN technology allows limited access from outside to inside, but has scalability challenges and exhibits many drawbacks that make its security posture suboptimal in today's network and threat environments. Websites face the outside and also has access to the inside to do business transactions; these border elements exhibit many security challenges and are prime attack targets.

Traditional security solutions often grant access privileges based on IP address and/or recognizing corporate-managed devices, while modern networks instead require:

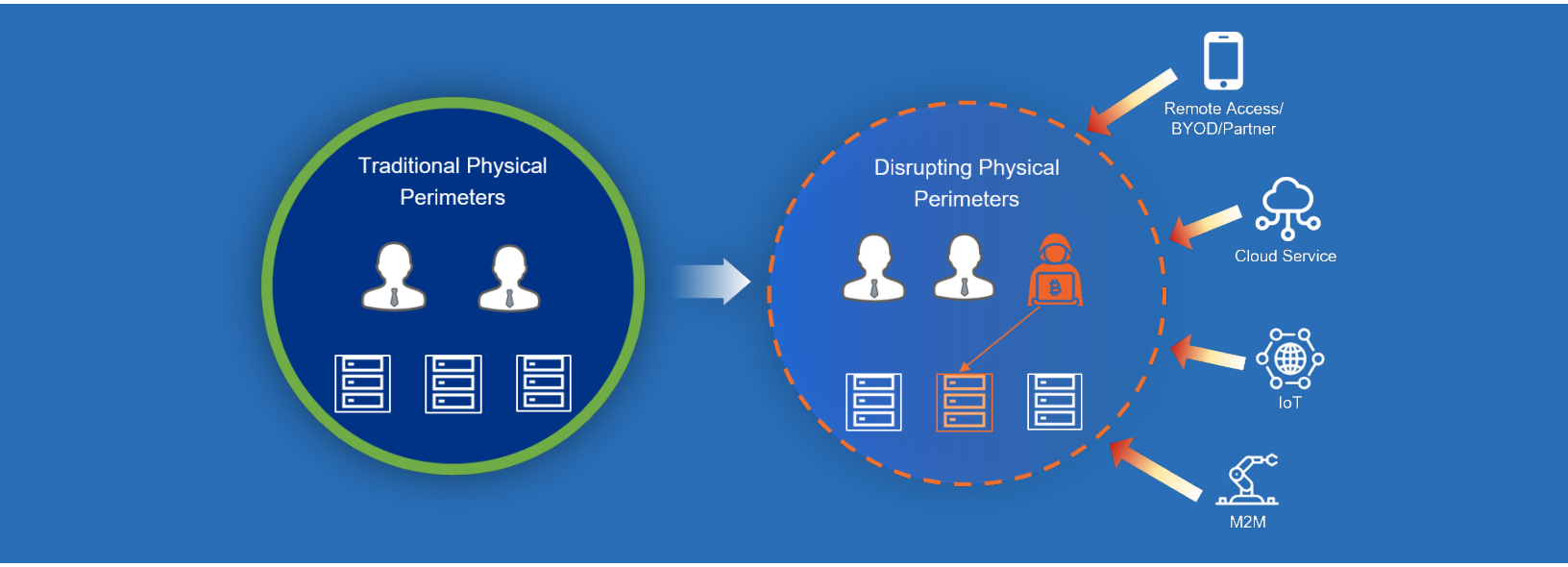
• The examination of a **user's credentials** independent of where they may be. An IP address is no longer significant or trusted for authentication or granting access privileges; it is significant only for the purposes of connectivity.

• On **any device** of the user's choice. Device credentials are considered separate from the user's credentials. Corporate-managed devices may still grant different access privileges from mobile or personal devices, but all devices can be processed for granting an appropriate level of access with ZTNA technology. IoT devices can be screened out, or given highly restricted privileges as these devices pose a glaring attack surface in modern networks.

In a ZTNA model, systems grant the minimum access needed for resources and users to perform their tasks. Access determination is independent of whether the user is inside or outside the traditional enterprise perimeter, thereby providing equal protection against attackers that are inside your network as well as for those outside your network.

Zero-trust models are sometimes viewed as perimeter-less security, though it is more accurately a security model for a dynamic software-defined perimeter (SDP) rather than no perimeter. Several factors have contributed to the disruption of the traditional perimeter in enterprise networks, including:

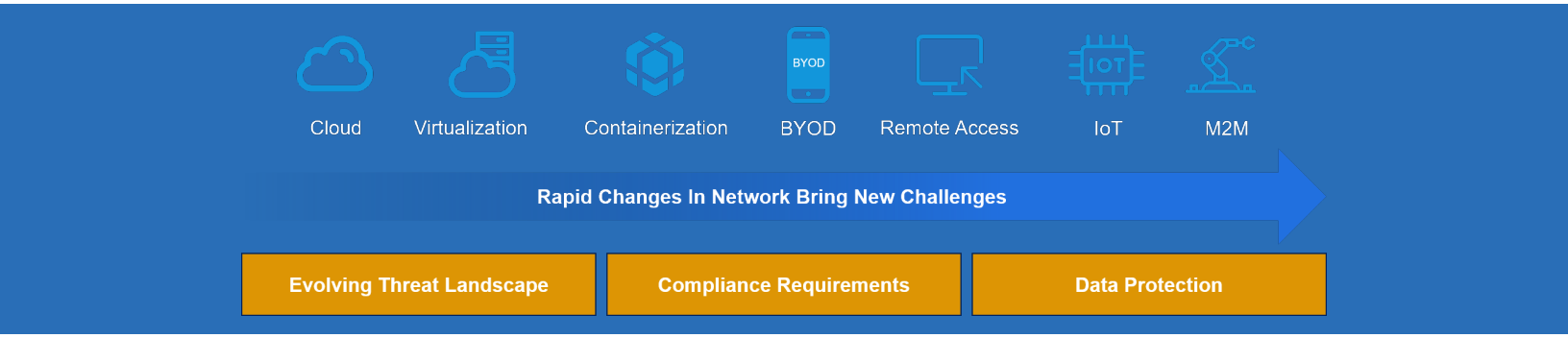
- Technology Challenges:
  - Cloud computing
  - Network virtualization
  - Known VPN vulnerabilities
- Business Challenges:
  - Increased number and types of devices, both personal and corporate
  - Extended types of users, many of which are off-premises and/or mobile
  - Hybrid architectures



ZTNA blocks all access by default; nothing is trusted. Resources not explicitly provisioned for access are invisible to users and rendered unreachable and undiscoverable. A ZTNA approach uses the identity credentials of users and devices, coupled with a large variety of additional attributes—considered along with the context of the requested interaction—to grant or deny access (or partial access such as view-only rather than modify, or download-only rather than down-and-upload) to crucial enterprise resources.

Why ZTNA?

By focusing on identity and context—user, device, location, application—ZTNA allows fine-grained access control to enterprise resources and allows secure access in a WFH/WFA world. ZTNA also covers an environment where businesses connect with, and collaborate with, non-employee users such as partners and contractors. It also protects in an environment of increasing IoT penetration inside enterprise networks.

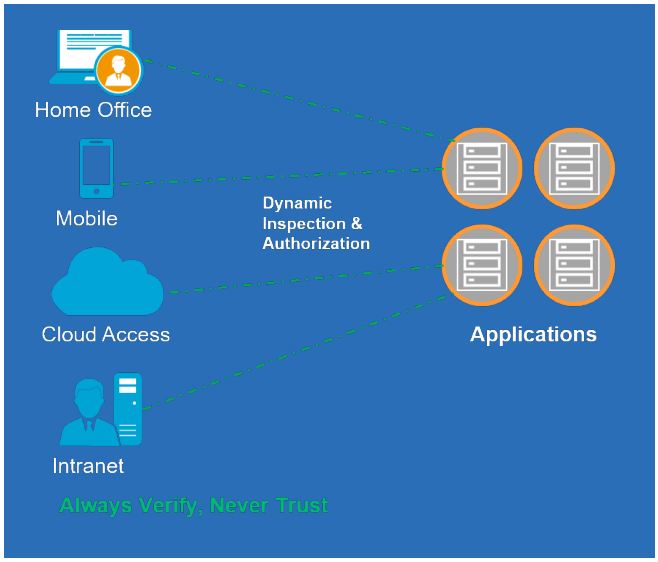


Challenges to Network Security due to the Digital Transformation

ZTNA uses a combination of factors to grant or deny grades of access to enterprise resources, including:

- the identity of the user
- the location of access
- the user's role in the enterprise
- the state of the device

ZTNA implementations can protect resources anywhere—in branches, in enterprise data centers, in home networks, and in public or private clouds. It has the flexibility to provide different levels of access privileges based on the combination of a large number of attributes, as well as integrating with your existing identity servers. For example, companies can limit employees to read-only versus write access if the user is connecting from an untrusted public Wi-Fi network at an airport, or from a personal device deemed to have a marginal security posture. A ZTNA approach ensures that enterprises can minimize their attack surface without impeding employee and business productivity.



Implementing ZTNA

ZTNA solutions can be implemented in an endpoint-initiated or a service-initiated architecture.

• The **endpoint-initiated** approach uses an agent, or client, installed on the endpoint which initiates the connection to the application. A ZTNA controller authenticates and verifies the request. Once granted, the endpoint connects directly to the application.

• The **service-initiated** approach—also known as clientless—uses a software element between the endpoint and the application that brokers the connection. Once the request is authenticated, the broker proxies the connection, ensuring no direct access from the endpoint. The advantage of this approach is that is requires no special software to be installed on the endpoint.

Three components that are typically present in an endpoint-initiated ZTNA solution include an endpoint, a gateway and a controller/manager.

• **Endpoint:** An endpoint agent resides on the user device and gathers information such as whether:

  - the device is a registered and valid corporate device (via MAC address, installed software certificate, or hardware-trusted platform modules)
  - the device has antivirus or anti-malware software installed
  - the device contains the necessary patches and software updates

• **Gateway:** The gateway element is responsible for executing advanced ZTNA policies associated with application access control. A ZTNA gateway can be deployed at the edge of either your data center or the cloud, protecting not only on-premise assets but also applications or data hosted in any public or private cloud.

• **Controller/Manager:** The controller or manager has global visibility across all ZTNA elements and is able to perform sophisticated analytics on access requests involving user and device posture and behavior. It works in concert with other ZTNA elements and corporate identity directories to determine the appropriate ZTNA policies. There are several industry approaches to ZTNA controller implementation, including on an existing security device such an NGFW, as a centralized appliance in the data center or as a service in the cloud.

Complementing Existing Security with ZTNA

ZTNA is not a standalone solution but works in concert with existing network security solutions such as NGFW. It increases the value and longevity of CISO investment in perimeter solutions, both in hardware appliances and virtualized software packages for private and public clouds.

By enabling a more informed access decision and unlocking fine-grained controls, CISOs are able to broaden the controls already built into existing perimeter-based solutions. At the same time, the fine-grained ZTNA controls dramatically reduce the attack surface of the enterprise, even with WFH/WFA users accessing resources from outside corporate environments. A ZTNA approach significantly tightens your security posture compared to traditional VPN solutions.

Achieving the desired combined outcome of increased security at the same time as increased productivity is a massive win for CISOs, especially in today's post-breach world with rampant threats from ever-more sophisticated attackers.

Hillstone ZTNA Solution Highlights and Benefits

Hillstone combines and leverages the capabilities of the Hillstone Security Management (HSM) Platform with its NGFW product line to offer a ZTNA solution. Hillstone ZTNA supports a wide range of authentication schemes for popular enterprise devices and operating systems. Additionally, HSM enables deployment and management at scale.

Highlights

- Identity-Based, Least-Privileged Secure Access
- Context-Aware, Adaptive Access Control
- Centralized and Efficient Management
- Award-Winning Enterprise-Grade Security Foundation

Hillstone Solution Architecture

The Hillstone ZTNA solution architecture consists of the following components:

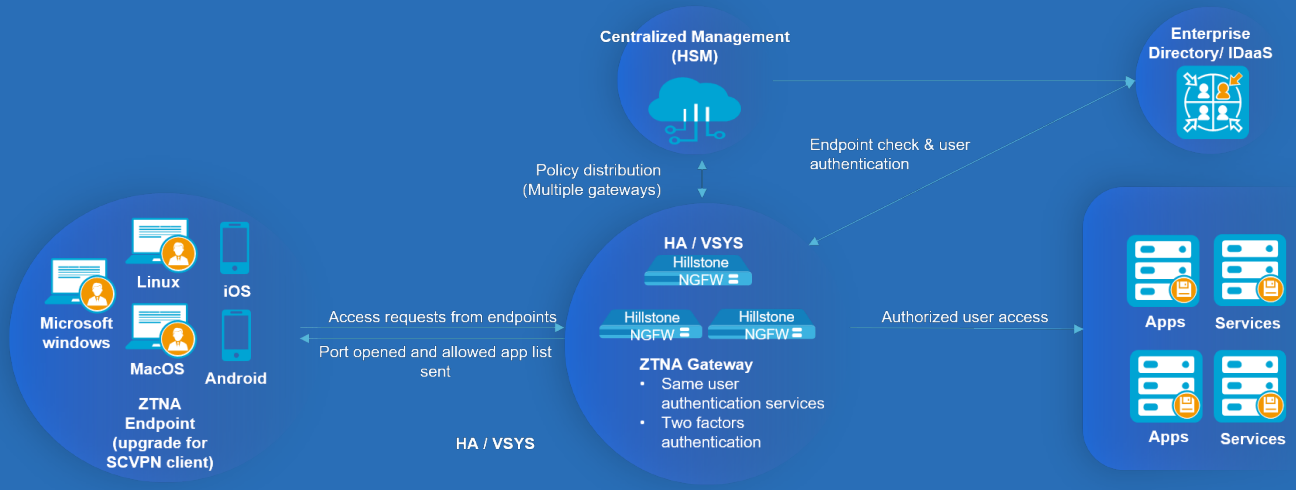
• **ZTNA Gateway:** Existing NGFW platforms take on the role of gateways in brokering ZTNA authentication transactions. Access can be switched seamlessly between mutually backed-up gateways.

• **ZTNA Endpoint:** An endpoint agent aids in user and device authentication, for example, tracking its security posture such as OS levels, patches and updates.

• **Enterprise Identity Server:** Existing enterprise directories containing user, group and role identity information integrate into the ZTNA solution to contribute to the process of authentication and granting access privileges.

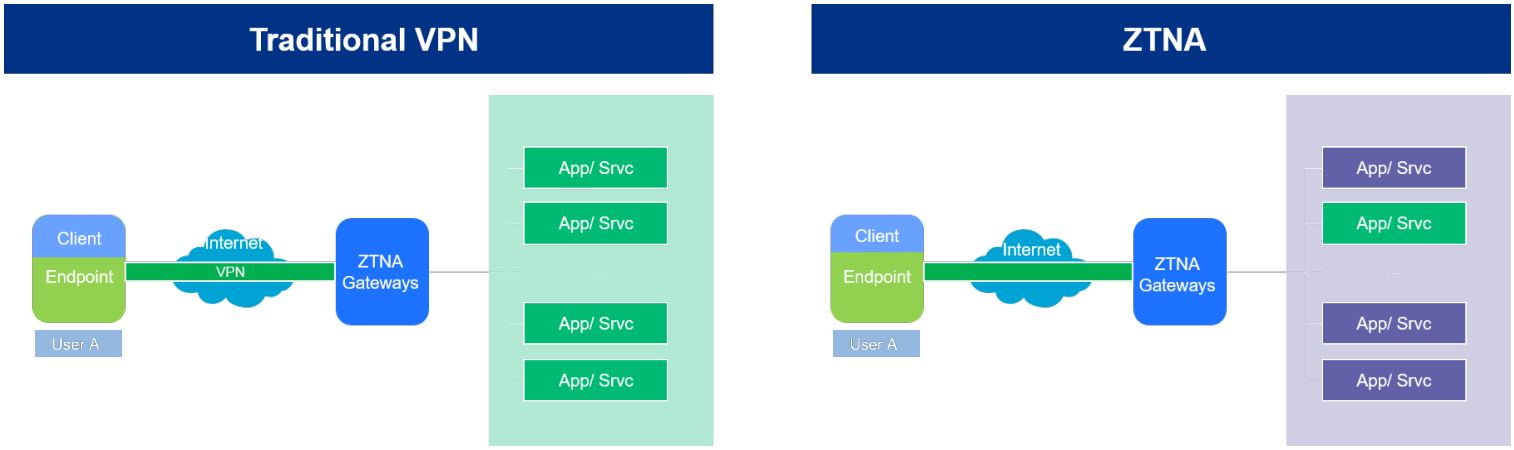
• **Applications:** Application configuration and knowledge are consulted during the process of authentication and granting access privileges to each particular application.

• **ZTNA Manager:** A central management point coordinating all the aspects and elements of the ZTNA solution.



Identity-Aware, Least-Privilege Secure Access

The foundation of ZNTA is that nothing is trusted, and only minimal access is granted to allow any particular transaction to proceed. Unlike earlier technologies, ZNTA is not a binary allow-or-deny decision approach; instead, various gradations of access may be granted (or restricted) based on the evaluation of the user/group credentials, device posture, application configuration, location, reputation and various additional context-aware attributes of the access request.



Traditional VPN solutions perform access authentication a single time when the user first contacts the VPN controller. Once authenticated, the user and endpoint are trusted by default, are essentially inside the network, and have visibility to all (or most) applications and services in the network similar to a situation where the user-and-device were physically inside the traditional network perimeter. This means that if a user's VPN login credentials or VPN-enabled device is breached, the attacker has broad access to discovery and lateral movement throughout the entire enterprise network.

A ZTNA architecture enforces an identity-aware, least privilege model where the user can only access pre-authorized applications and services. It renders invisible the rest of the network and its resources and restricts lateral movement if a single breach has occurred.

Upon authentication of a ZTNA endpoint client, both the user identity and device information, along with other attributes (time-of-day, location of access, source IP reputation, recent behavior and activity, resource being accessed) are processed by the policy engine, which renders an outcome not only of access granted or denied, but may include limitations on grades of access. Detailed role and group information from corporate identity directories is used as part of the decision-making.

Diverse User Authentication Schemes

Hillstone ZTNA supports multiple authentication schemes and identity stores. Integration with authentication, authorization, and auditing (AAA) systems via RADIUS, TACACS+, and support for multi-factor authentication (MFA) allows rapid deployment into enterprise networks.

User identity and role information stored within enterprise directories (Active Directory, LDAP) can be extracted and used as part of intelligent access policies. For instance, user group information can help determine which subsets of employees should have no network reachability at all into sensitive corporate systems, such as engineering, finance and accounting servers.

Extensive Client Authentication

As the world gradually reopens and travel resumes, an increasing number of employees are working in diverse locations and across different time zones. In this evolving landscape, it is essential for CISOs to ensure that access controls and sensitive data protection are in place for mobile workers. ZTNA provides robust security measures that safeguard mobile workers from data breaches and other security risks by restricting access to sensitive data while still allowing employees to access essential information.

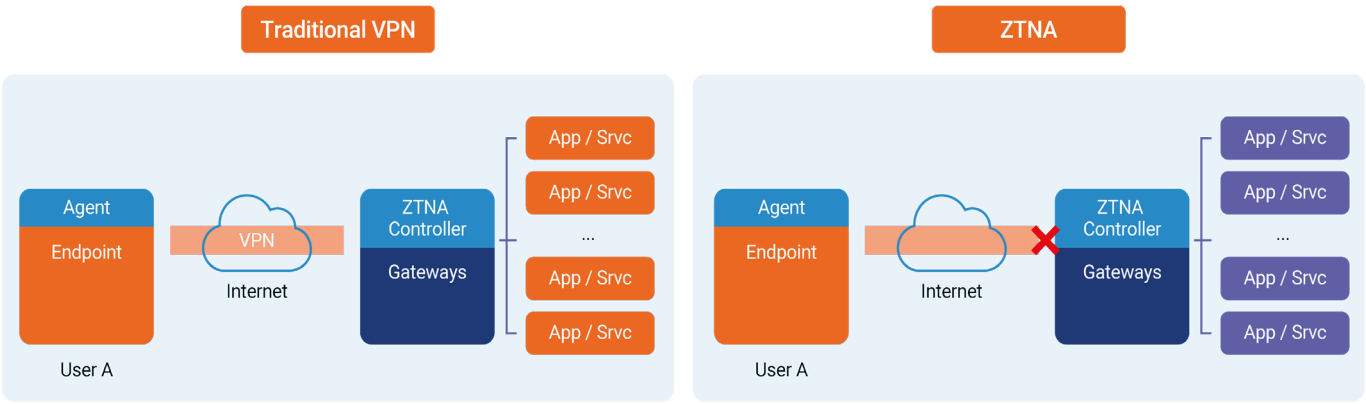
For finance employees who frequently travel, ZTNA offers the added advantage of least-privilege security measures, which enable them to access only the information they require and limit their exposure to risks when working in public places. This context-aware security measure has proven to be highly effective in risk management and enables more flexibility and productivity without compromising data security.

Content-Aware, Adaptive Access Control

User and device authentication are fundamental elements of secure access. ZTNA introduces yet another level of security by also taking into consideration the context of the requested access, and the security posture of the client, and adapting the policy appropriately.

A specific user may have view-and-modify access to a particular set of data if they request access while using a device with a safe security posture and is in a safe network location. But the same user may only be granted view access if the device they use has a less safe security posture, and may be granted no access if they are on an unsafe device and an unsafe network location.

A comprehensive ZTNA solution requires client agents to reliably report on device posture at initial login and as part of ongoing validation. Hillstone agents perform continuous checking to ensure that a device remains in compliance with corporate policies during the entire life of the session. This is of enormous importance in WFH/WFA scenarios where laptops might be connected for extended periods of time and where they can get infected while connected and not being used.



Traditional VPN solutions have no context awareness. An attacker or malware can easily perform port/IP scanning and attack discovered hosts and applications if the user's credentials or VPN endpoint is compromised by spam, phishing, or malware.

ZTNA solutions do continuous trust evaluation for each access request. The ZTNA agent on the endpoint monitors and evaluates the endpoint's status to determine if it is secure to connect. If the endpoint is compromised, access attempts are blocked by the ZTNA gateway.

Comprehensive Endpoint Visibility

Hillstone ZTNA continuously monitors and evaluates endpoint status and security posture, including:

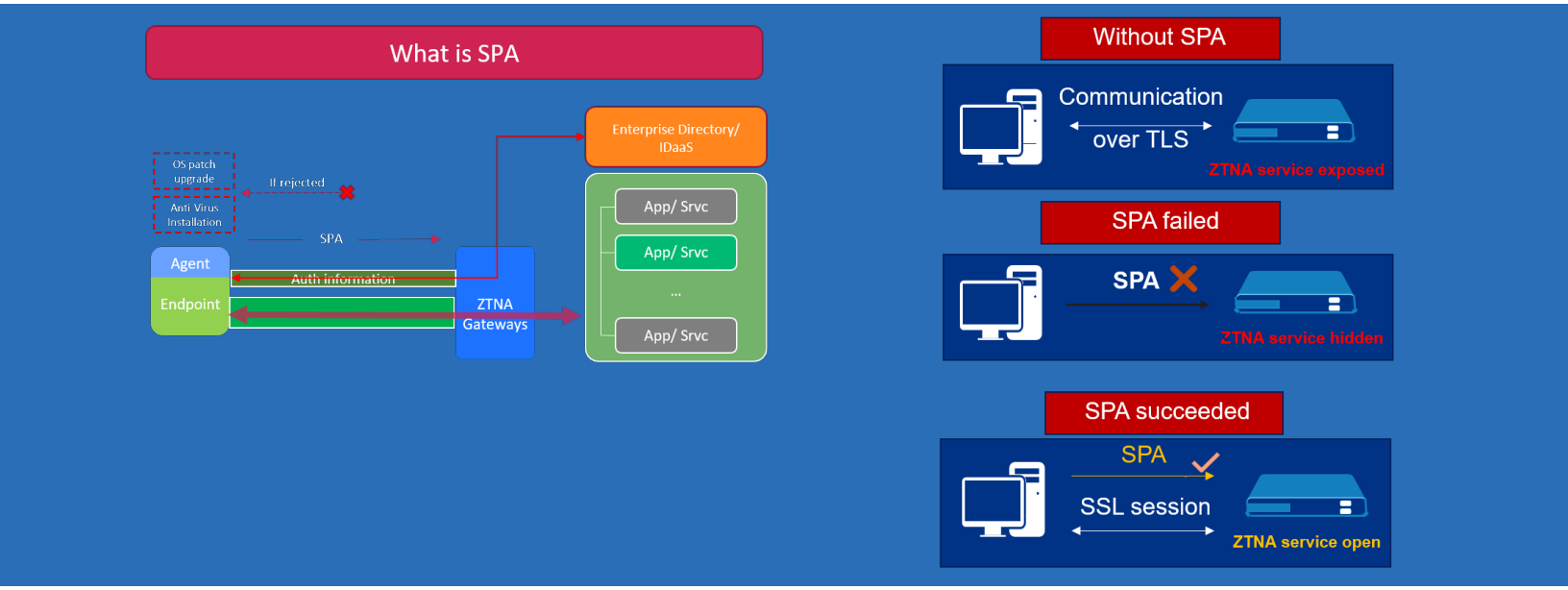
- Operating Systems (OS)
- OS patch levels
- MAC address binding
- Antivirus protection
- Data Leak Protection (DLP)
- Device identity (hardware certificate, software certificate)
- Browser security and patch levels
- Time
- Location

Upon initial authentication, all device posture elements are checked against ZTNA configurations and policies to provide an intelligent decision regarding access rights based on user, client and other contextual information.

Single Packet Authentication (SPA)

Single Packet Authorization (SPA) is a technique for securely including authentication, authorization and client identity information in a single initial packet (typically using TCP, UDP or ICMP) that the target host or server can evaluate before responding. This makes the target machines effectively invisible to unauthorized connection attempts.

Only source devices that know the required cryptographic secret can form a valid SPA packet in the first communication they generate towards a target. Invalid SPA packets in connection requests—for instance, when an attacker scans for open ports—are met with silence from the target machine. Once an SPA packet is properly authenticated, following a set of configured rules, the server can open a particular firewall port for a few seconds. This short window of time allows the authenticated client to establish a connection to the host or server.



The benefits of including a SPA capability in your ZTNA architecture are:

• Reduces your attack surface by making internet-facing (as well as internal, or cloud) resources invisible to all except sanctioned clients.

• Mitigate DoS attacks over TLS.

• Protect assets. SPA obfuscates your network resources to limit breaches as well as lateral movement once a breach has occurred.

Award-Winning Enterprise-Grade Security Foundation

Hillstone ZTNA contains a substantial suite of features, but the true differentiation of the solution is that Hillstone is already a leading security platform with a broad customer base. Built from the ground up to be one of the most comprehensive security platforms in the industry, Hillstone's expertise in security shines in its ZTNA solution. With an integrated next-generation firewall, and unique breach and malware detection capabilities, Hillstone's security components are already used by over 20,000 enterprises worldwide and recognized by leading analysts such as Gartner across multiple solution classes.

Hillstone's extensive set of capabilities, including ML/AI-based detection and prevention, sandboxing, anti-spam, botnet command and control (C&C) prevention, IP reputation, application identification, intrusion prevention, URL and content-filtering, and antivirus protection have been battle-tested in many vertical industries worldwide. Advanced application layer security features could be included natively when defining the ZTNA policy.

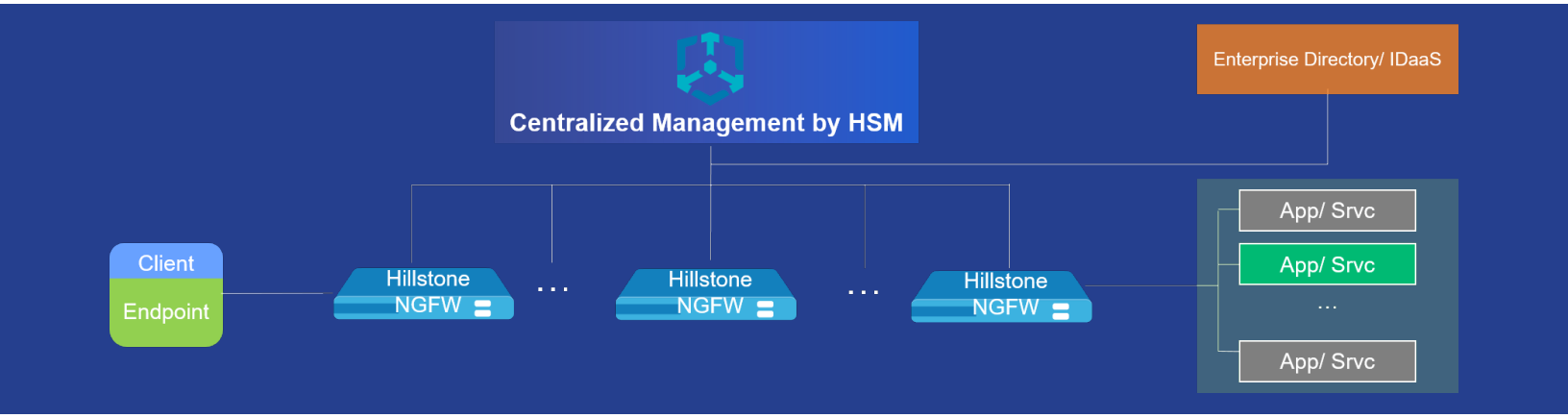
Hillstone ZTNA solution is built on this trusted and proven secure foundation, allowing you to adopt and deploy an integrated ZTNA strategy simply by upgrading software components. The A-series NGFW, X-series Data Center Firewall, and CloudEdge virtual NGFW appliance can be upgraded to act as a gateway in the ZTNA solution. Similarly, the Hillstone VPN client, SCVPN, can be upgraded to take on a client (agent) role in the ZTNA solution.

Centralized and Efficient Management

A hard-to-deploy and maintain solution negatively impacts CISOs and overburdens SecOps teams. Hillstone offers centralized policy management and global visibility of ZTNA settings with simple set-up and deployment from a central console. This centralized control is coupled with an effortless zero-touch deployment model that allows units to be onboarded in remote locations where experienced IT staff is often unavailable.

Hillstone Security Management (HSM) offers centralized capabilities including:

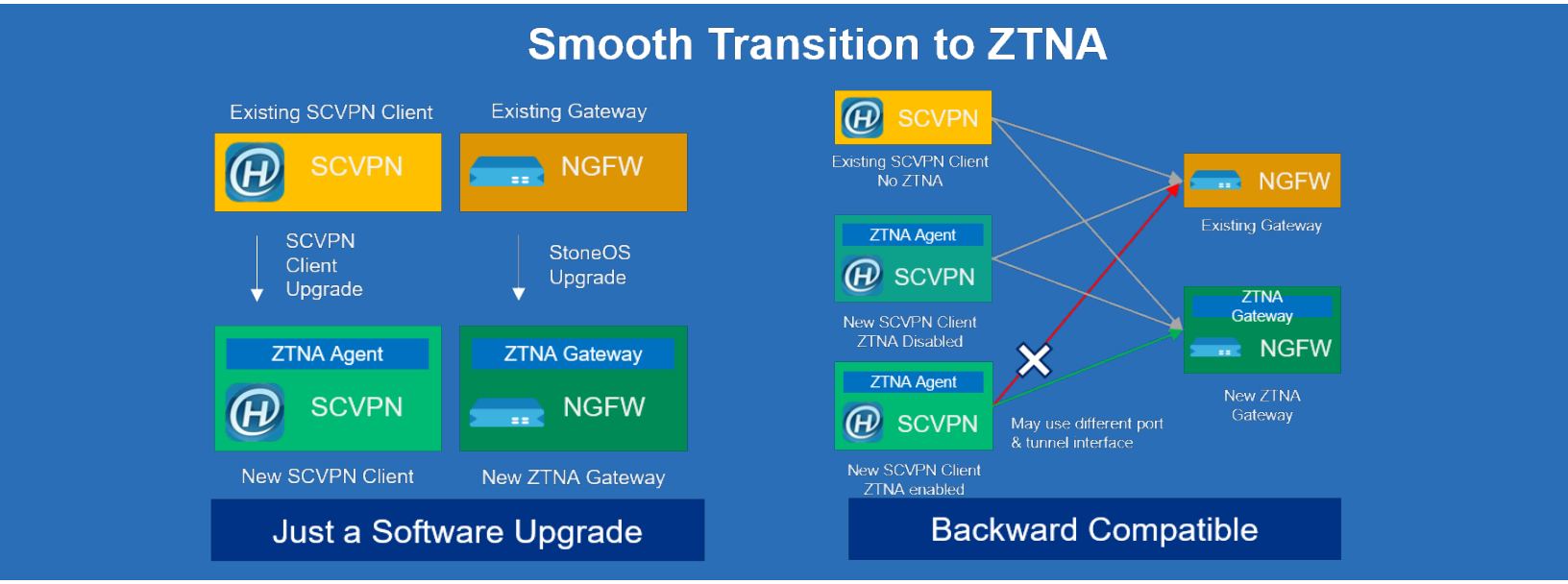
- Integrated device management
- Centralized ZTNA policy Management
- Comprehensive security monitoring



Smooth Transition To ZTNA

A major advantage of the Hillstone ZTNA solution is support for a smooth transition leveraging your existing Hillstone platforms to incorporate ZTNA roles and capabilities. NGFW platforms can be upgraded into the role of ZTNA gateways, and the Hillstone SCVPN client can be upgraded into a ZTNA agent. Additional advantages of this smooth migration path include:

- Similar user experience
- Support the same user authentication services (local, LDAP, TACACS+, Radius)
- Support two-factor authentication (2FA)
- Protects your investment
- Minimum effort and disruption during the transition
- Lower TCO



Typical ZTNA Use Cases

With Hillstone's superior security foundation, its ZTNA solution can be deployed effectively in many different scenarios, use cases and industries. Capabilities are not limited to the use cases discussed here, but the unique benefits highlighted in these typical scenarios can trigger ideas on how Hillstone's portfolio can help you regardless of which industry you may be in.

For Remote Employees

The WFH/WFA reality is here to stay. Companies worldwide have learned that employees can be as productive at home as in the office. Many companies expect to retain a blended workplace strategy with a mix of WFH/WFA and in-office work. This means that ongoing extended access from home or other remote locations must continue, and VPN solutions do not scale to allow this.

Hillstone ZTNA provides the flexibility to accommodate this WFH/WFA world while keeping the attack surface contained. The ZTNA solution ensures that only corporate-sanctioned devices are used to access the enterprise network, that up-to-date antivirus software is running, and that the operating system version is current. This helps you to avoid situations where attackers take advantage of a known vulnerability on a system and leverage it as a launch-point into corporate systems. Consider a situation where the operating system is not patched and updated. In this scenario, the employee is either blocked from accessing the corporate network and asked to remediate separately or put into a quarantine zone—with no access to sensitive corporate resources—where they can connect to the internet and other resources to help them remediate the system.

Similarly, a ZTNA solution prevents employees from using compromised or unsafe home computers with weak security and no anti-malware agents from connecting to the corporate network, exposing corporate resources to potential infection and attacks.

For Mobile Employees

As the world gradually returns to normal after pandemic lockdowns, travel is returning, and employees again embrace the flexibility of working from airports, coffee shops, and other unsafe locations. Just as ZTNA protects WFH/WFA employees, it also defends mobile employees. With Hillstone's extensive support for mobile devices, CISOs can achieve tighter security when employees are on the road or in hotels.

ZTNA ensures that employees get the necessary access to critical information to do their jobs while limiting access to sensitive data. For example, a traveling corporate finance employee could access their email but may not be allowed to connect to the finance or accounting systems while in public locations. Once they arrive at a location considered secure, they regain access to sensitive finance systems. This intelligent, context-based, least-privilege approach is excellent for managing risk and balancing security against productivity. ZTNA provides CISOs with the tools to surgically implement security policies, as opposed to the blunt hammer of all-access or no-access.

For Government Agencies or Regulated Industries

ZTNA provides the necessary additional layer of protection for government entities and enterprises with strict compliance requirements. Both are categories of organizations with a higher risk of compromise by malware and ransomware. ZTNA aligns with the philosophy of many of these agencies and industries, who themselves advocate a policy of least-privilege access and a need-to-know, need-to-access mindset.

For example, ZTNA policies can mandate that traveling government employees use multi-factor authentication and trusted devices for remote access. Hillstone ZTNA can be configured to block access if employees do not comply, or to allow restricted access only to systems such as email.

Hillstone's secure platform coupled with ZTNA can be advantageous for these organizations, making remote employee locations like home, or mobile locations like airports and hotels more resilient to attacks, protecting access to critical data even in the event of potential device compromise.

For Services Providers

Service providers looking to help their customers secure their IT resources for WFH/WFA scenarios find added value in Hillstone ZTNA solution. Many small and medium enterprises (SMEs) are under threat from ransomware but have little to no in-house IT expertise. In addition to requiring reliable connectivity for their digital assets, they need help with securing their employees and assets. By layering ZTNA on top of Hillstone NGFW solutions, service providers can offer these SMEs a value-add managed solution that significantly improves their security posture.

Hillstone ZTNA can easily be provided as a service to SMEs, allowing them to benefit from advanced policies while trusting the service provider to manage their security policies.

About Hillstone Networks

Hillstone Networks' Integrative Cyber Security approach delivers coverage, control, and consolidation to secure digital transformation for more than 26,000 enterprises worldwide. Hillstone Networks is a trusted leader in cyber security, protecting enterprise critical assets and infrastructure, from edge to cloud, regardless of where the workload resides. Recognized as a Visionary in Gartner's Magic Quadrant for Network firewalls, Hillstone Networks' entire suite of cyber security solutions is relied upon in many of the world's most challenging technology environments.

Hillstone NETWORKS

Visit **www.hillstonenet.com** to learn more

or contact Hillstone at **inquiry@hillstonenet.com**