VMware Secure Access

Secure, optimized, and high-performance access for remote and mobile users

vmware®

Secure Access™

KEY TAKEAWAYS

- Provides secure, optimized, and high-performance access for remote and mobile users
- User-centric policies with deeper contexts, based on Zero Trust Network Access framework
- Cloud-hosted service simplifies operations while ensuring consistent policy enforcement

As enterprises move their business-critical applications to the cloud and their users become increasingly mobile, the traditional remote access model of deploying VPN concentrators at enterprise data centers is no longer efficient. Employers are adapting to a world in which a large majority of their employees are working remotely—and accessing all applications remotely (on-premises, virtual, cloud, or SaaS)—making the traditional security models of protecting the network perimeter obsolete. Providing exceptional, secure user experiences and maintaining the supporting infrastructure for solving these problems requires resources, expertise, ongoing maintenance, and is often costly.

VMware Secure Access™ is a remote access solution that addresses these challenges. Based on a Zero Trust Network Access (ZTNA) framework, the cloud-hosted solution offers multiple benefits over traditional VPN solutions. It provides users with consistent, optimal, and secure application access.

Challenges facing today’s remote access solutions

Hairpinning to the data center

For VPN deployments, a VPN concentrator is usually deployed inside an enterprise data center. The VPN concentrator terminates a mobile or remote user connection and directs all session traffic to the data center, regardless of the destination. With most of the applications moving out of the data center and into the cloud, VPN traffic is sent back out to the Internet and to SaaS/IaaS, causing traffic hairpinning. This approach makes communication between the VPN endpoint and application server take a much longer path through the data center. The VPN traffic takes on additional latency and must compete with other applications for data center internet bandwidth. This introduces additional packet drop, latency, and jitter, resulting in a poor user experience and loss of productivity.

No custom access to applications

Remote and mobile users today have a different experience accessing corporate applications compared to users inside a branch office. Traditional security models, including VPN, have employed the inside/outside trust model. Users in the branch or campus are considered “trusted”, and users outside of the branch or campus are considered “untrusted” until they VPN into the data center. There is no visibility into end device postures. Network policies are static and based on IP address ranges. As a result, application access cannot be tailored for each user and applications are open widely to attacks once access is compromised.

Exposed threats from BYOD and web attacks

The growth of the bring-your-own-device (BYOD) trend proves that it is no longer optional to support these devices—it has become a requirement. Employees today can access any application hosted in any cloud, using any device. This introduces a set of challenges for IT to secure the end devices that they do not own and protect the users from the web threats from actions that users take on their devices when they are not using them for work.

Scaling the remote access infrastructure

As more workers are increasingly mobile and dispersed, IT is facing challenges in supporting them. IT must ensure that these remote and mobile workers can access the enterprise applications they need, and that the applications perform well. Deploying and maintaining VPN concentrators in multiple data centers around the world can be costly because of the expertise required and cost of deploying and maintaining infrastructure.

VMware Secure Access

The VMware Secure Access solution provides remote and mobile users with consistent, optimal and secure cloud application access through a network of worldwide managed service nodes. The solution is based on a ZTNA architecture that offers multiple benefits over the traditional VPN solution:

- **VMware Secure Access is cloud-hosted,** enabling enterprises to offload the costly deployment, maintenance, and scale of the remote access solution for improved IT efficiency.
- **VMware Secure Access offers user- and application-centric access** versus network-based access with VPN. Access is granted based on the user identity and end-device posture, with access to only the applications the user needs, significantly reduces the surface of attack.
- **Location independence means a consistent access policy** regardless of where the user is.

The solution leverages VMware's global Points of Presence (PoPs) and optimizes traffic handling capabilities for lower latency and better application performance, enabling a branch-like experience for remote workers.

Support multi-region connectivity with network of VMware PoPs

Remote workers who are not from the same region as the enterprise headquarters know very well that finding a VPN concentrator closest to their location is challenging. Enterprises often do not have the resources to deploy VPN concentrators across the world for employees' remote and mobile access. As a result, both remote and mobile workers find it challenging to connect to a concentrator across the country, and often, across continents, to access the applications needed. User experience is adversely impacted, and productivity suffers. Without a VPN concentrator close by, users endure added latency, extra hops and additional packet drops. VMware Secure Access supports multiple regions through its distributed Service Nodes, ensuring users can always find a VMware Secure Access PoP closest to them.

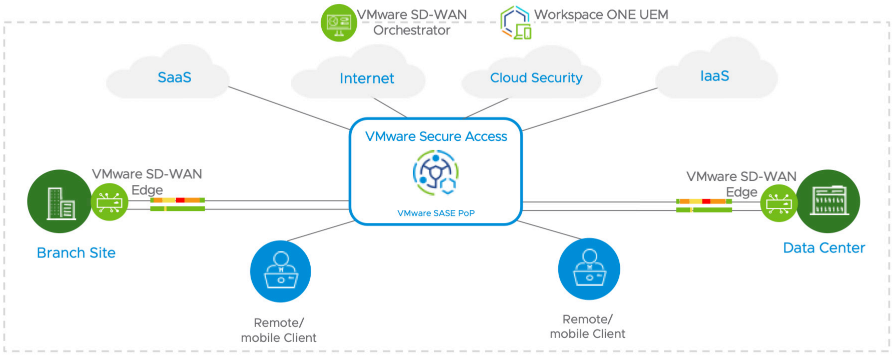

FIGURE 1: VMware Secure Access brings secure, optimized and high-performance to remote access and mobile users

Bringing off-premises users into SD-WAN fabric for optimal routing

VMware SD-WAN users today have access to a network of thousands of VMware SD-WAN Gateways deployed in more than 150 POPs worldwide. User traffic from branch offices is handed to the closest Gateway, to be routed to the application server hosted in either the enterprise data center, IaaS, or SaaS cloud. Because the Gateways are deployed inside the same data center that hosts IaaS/SaaS, the destinations are milliseconds away from the Gateways, enabling a smooth application experience. If the traffic is destined for the data center, users' traffic is optimized by VMware SD-WAN Dynamic Multipath Optimization™ (DMPO), which can mitigate network issues such as latency, jitter, and packet drops.

By hosting the remote access service in the same VMware POPs, remote and mobile users also have access to the same infrastructure as users in branch offices. Remote users are connected to the closest PoP. The Gateway will send SaaS/IaaS/Internet traffic directly to their destination without the need for backhauling to the data center, while only data center traffic will be optimized by DMPO and sent there.

Because of this efficient architecture, application performance is greatly improved. With no additional latency, enterprises can save on the cost of additional bandwidth purchase in the data center because there is no need for backhauling. Lastly, traffic destined for the Internet never enters the enterprise's network, protecting the network from attacks and protecting user privacy within the enterprise.

Zero Trust Network Access

VMware Secure Access is based on a ZTNA framework. By default, ZTNA doesn't trust any user or device regardless of whether the user is accessing from inside the campus/branch office or remotely, allowing a common policy for users both inside and outside the office.

Access is restricted until user authentication is successful and the device posture is verified. For example, if a user is coming through a device that is fully patched and has the latest antivirus definition, then the user can access the corporate resource. If the end device is not fully patched, then the user only has access to items such as the cafeteria menu.

With VMware Secure Access, access policies are based on user identity, user behavior and end device posture, instead of IP subnets. This allows IT to create per-user application access based on context of the user and end device. This user-centric policy can further grant access to only the applications that the user needs and hide the rest of the applications from that user, significantly reducing the surface of attack.

Protecting users from web threats with VMware Cloud Web Security

As SaaS applications are becoming widely available, enterprises are adopting them at a rapid rate, often without IT oversight. Users consume these business and personal applications on personal devices that are not fully protected, increasing the risks of advanced threats, malware, and loss of corporate data.

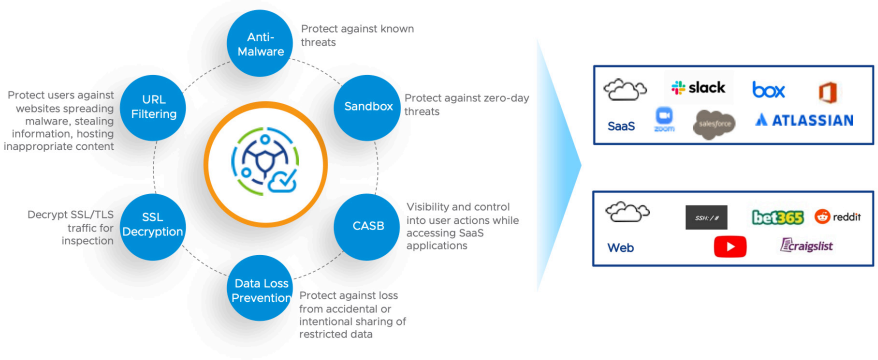
Anti-Malware
Protect against known threats
URL Filtering
Protect users against websites spreading malware, stealing information, hosting inappropriate content
Sandbox
Protect against zero-day threats
SSL Decryption
Decrypt SSL/TLS traffic for inspection
CASB
Visibility and control into user actions while accessing SaaS applications
Data Loss Prevention
Protect against loss from accidental or intentional sharing of restricted data
SaaS
slack
box
zoom
salesforce
ATLASSIAN
Web
SSH:/#
bet365
reddit
craigslist

FIGURE 2: VMware Cloud Web Security protecting users from threats

Once VMware Secure Access user traffic arrives at the VMware SASE PoPs, VMware Cloud Web Security can be applied to this traffic to protect users from known and unknown threats. VMware Cloud Web Security is a cloud-hosted service that protects users and infrastructure accessing SaaS and Internet applications from a changing landscape of internal and external threats. It offers visibility and control, prevents data loss, and ensures compliance. Cloud Web Security simplifies management of security services and helps IT tighten the security posture while balancing user productivity.

Managing and securing endpoints with Workspace ONE and Carbon Black

In addition to providing remote and mobile users with secure and optimized access to resources, enterprises must also secure endpoints to ensure these users are protected from hackers targeting these endpoints. VMware Workspace ONE is an industry leader in unified endpoint management. It offers the ability to easily manage any device, authenticate users with risk-based conditional access that is tied into single sign-on and multifactor authentication capabilities. Workspace ONE integrates with leading endpoint protection platforms such as VMware Carbon Black and other mobile threat detection products including Lookout, Checkpoint, and Zimperium to ensure users and devices are protected and authenticated in a work from anywhere environment.

For more information about VMware Secure Access, visit *sase.vmware.com/secureaccess*.