Datasheet

Updated 10/19/2021

VMware Secure Access

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

vmware

Secure Access™

At a glance

- Managed remote access-as-a-service
- Multi-region, cloud-hosted remote access solution
- Remote access with Zero Trust Network Access framework
- Protecting remote access users from web threats

Introduction

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. As employers adapt to a world in which a large majority of their employees are working remotely accessing all applications (on-premises, virtual, cloud, or SaaS), the traditional security models of protecting the network perimeter will become 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 providing users with consistent, optimal and secure application access.

VMware Secure Access Solution

The VMware Secure Access solution provides remote and mobile users a 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:

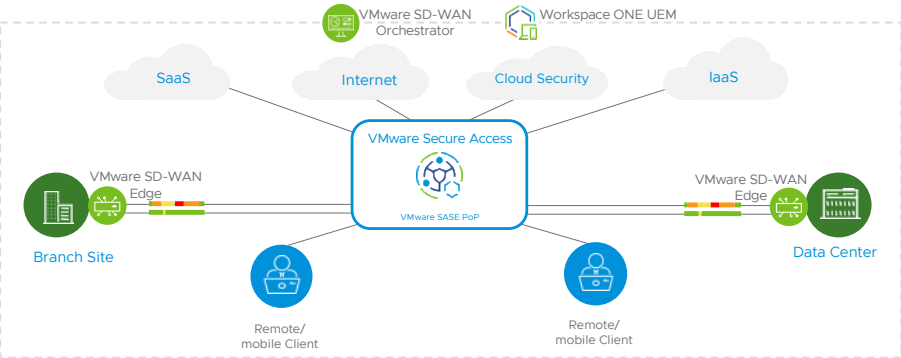

FIGURE 1: VMware Secure Access brings secure, optimized, high performance to remote and mobile users

- 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.

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

- 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 reducing the surface of attack.
- The solution leverages VMware's global SASE Points of Presence (PoPs) footprint and optimizes traffic handling capabilities for lower latency and better application performance, enabling customers to have a branch like experience for remote workers.
- VMware Secure Access is offered as-a-service, with the built-in ability to scale up or down based on the enterprise's needs to support user demand and consumption without having to worry about deploying and maintaining worldwide remote access infrastructure.

Together with VMware SD-WAN™ solution for branch office and home office workers, Secure Access offers employees a consistent experience whether that employee is in the office, working from home, or remotely.

Secure Access key features and capabilities

Capability	Description
Cloud-hosted remote access service	Fully managed with built-in redundancy, scalable, and low latency remote access solution designed for the cloud.
Access to worldwide PoPs	Access to a network of worldwide PoPs that are close to both users and applications to ensure great user application experience.
Tunnel Client	Client software for building a Secure Access tunnel between the client and Secure Access service hosted in VMware PoPs, providing per app access to resources. Available on Windows, macOS, iOS and Android for Workspace ONE managed devices. For unmanaged devices, the tunnel client is available on Windows today, with macOS, iOS and Android support coming soon.
Secure Mobile Web App	A mobile web browser for connecting to internal applications without VPN, with pre-configured corporate bookmarks and home pages. Available on both iOS and Android.
Authentication support	Active Directory and UEM local user database can be used to authenticate users and generate per-user Secure Access connection profile.
Zero Touch Tunnel Client Configuration	The per-user tunnel client profile is automatically applied when the user initially enrolls the device for an easy, zero touch tunnel setup.

Per-App Tunnel	Per-App Tunnel restricts tunnel traffic only to authorized applications on the endpoint and destinations (domain) specified by the administrator when configuring the Device Traffic Rules.
Full Device Tunnel	On Full Device Tunnel configuration, traffic is restricted based on the authorized destinations (domains or IPs), regardless of the application. Full Device mode is available only on Windows 10 today.
Connection to Data Center and Clouds	Secure Access comes with licenses for connecting up to 5 different non-SD-WAN destinations including data centers and IaaS clouds. Additional connection licenses can be purchased.
Log streaming	Ability to send access logs to third-party syslog destinations.
Tunnel Certificate Lifecycle Management	Support for rotating public SSL certificates and the profile grace period with zero downtime for end users.
Monitoring	Monitoring the status of user enrollment, device connection status, device information, and much more, via Unified Endpoint Management console.

Workspace ONE for managed devices

The Secure Access solution capabilities are greatly enhanced when the endpoints are managed directly through VMware Workspace ONE. Workspace ONE manages any app on any device by integrating access control, application management, and multiplatform endpoint management. Together with Secure Access, they offer deeper contextual policies based on additional information from Workspace ONE.

Product	Description
Advanced Identity and Access control	Identity-based access control based on user group, user network range, authentication strength, authentication provider and other factors.
Risk-based Conditional Access	Access policy based on risk scores calculated from the user, their devices and user behavior. Organization may choose to allow access for low risk, step-up authentication for medium risk and deny access to users with high-risk scores.

Mobile & desktop endpoint management	Solution to manage, secure, and deploy corporate resources and applications on desktops, mobile, rugged, wearables, and IoT.
Device compliance	Ensures that devices comply with IT policies and policies enforced through the policy engine.
Integrated insights for entire digital workspace	Correlation of device, application, and user data together in one place gives a complete view of the entire digital workspace environment. Preset dashboards that can be customized show the evolution of the environment's security risks, app deployments, device management, app engagement, and patch rollouts.

Other add-ons

Beyond providing remote and mobile users with a secure and optimal way to access corporate applications, VMware also protects those users from known and unknown attacks with Cloud Web Security and Carbon Black for a complete Anywhere Workspace solution.

Product	Description
User protection with **VMware Cloud Web Security**	Cloud Web Security is a cloud-hosted security service that protects both Secure Access and SD-WAN users accessing SaaS and Internet apps, offering security, visibility, control, and compliance.
Endpoint security with **VMware Carbon Black**	Prevent malicious attacks on your organization's resources with a single NGAV and EDR solution offering comprehensive prevention and endpoint activity analysis capabilities.

For more information on Secure Access, please visit *sase.vmware.com/secureaccess.*