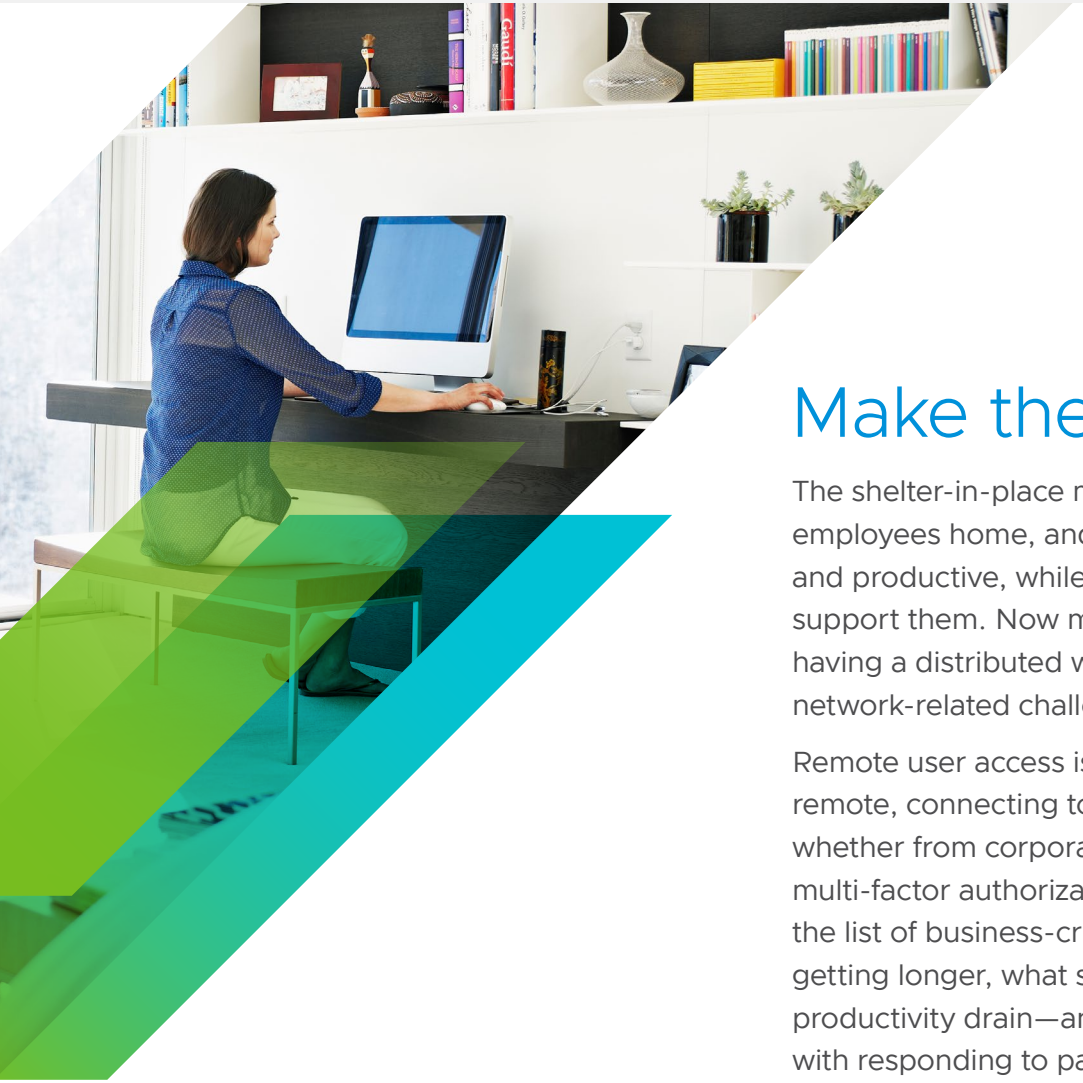
vmware®

GET STARTED

A Buyer's Guide to Optimizing Your Remote Employees' Extended Network



Make the Extended Network Work

The shelter-in-place mandates put in place earlier in 2020 sent most employees home, and for the next few months they strived to stay connected and productive, while IT teams scrambled to provide infrastructures to support them. Now many organizations have realized there are benefits to having a distributed workforce, and thus are focused on tackling some of the network-related challenges that have compromised employee experience.

Remote user access is one top-of-mind concern. When employees are remote, connecting to on-premises apps can be complex and convoluted—whether from corporate-owned or personal devices. Think multiple multi-factor authorization prompts and similar sources of frustration. With the list of business-critical apps and collaboration tools commonly used only getting longer, what started as an inconvenience is fast becoming a major productivity drain—and a huge time commitment for the IT teams tasked with responding to password reset help desk tickets.

Section continues >

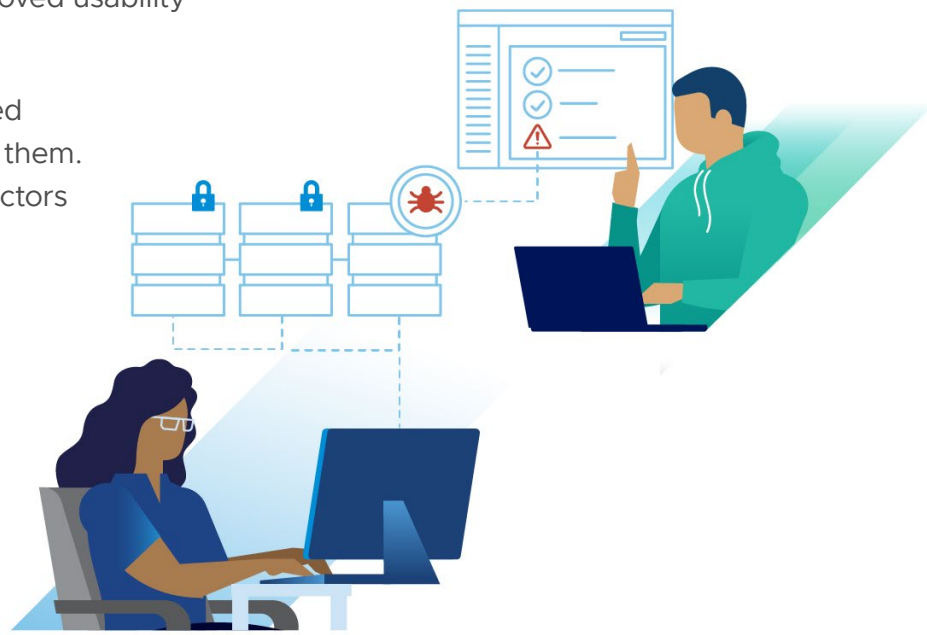
Slow or unreliable access to SaaS apps (such as collaboration tools) can be another problem. When employees are working from home, they often are competing for bandwidth with other people in their household or neighborhood, and this can compromise app performance.

Finally, with a distributed workforce, there is no network perimeter, which means that IT teams no longer have visibility into the devices that authentication requests are coming from. This lack of transparency increases security risk.

As a result, IT teams are searching for ways to optimize the remote employee's extended network, and many are considering implementing:

- Zero Trust security with conditional access
- SD-WAN solutions to improve connectivity and performance
- Modern management, endpoint security, and VDI technologies for improved usability and more-effective support

But it's important to remember that not all technology solutions are created equal, nor are the ways that different organizations can most benefit from them. This goal of this guide is to help organizations understand the three key factors to consider.



Factor #1: To Provide Seamless and Secure Remote Access, Is Zero Trust a Must?

Security is an ongoing challenge for organizations, and with today's dynamic workforce, the challenge is ever-increasing.

John Kindervag first coined the term *Zero Trust* while at Forrester in 2010 to describe a security model that does not automatically trust entities within the security perimeter. Since then, rapidly changing work styles and increased use of SaaS applications have resulted in the Zero Trust model becoming one of the most important forms of security.

Now that employees are remote and working from who-knows-what devices and networks, the need for Zero Trust has never been greater. When IT can't ensure that apps are being accessed from secure, trusted or known devices, security risk rises. When employees are working remotely and using personal devices, user experience degrades. A leading reason is that connecting to on-premises apps from remote locations often means navigating cumbersome (and annoying) access and security protocols, or trying to remember long-forgotten passwords.

With the list of business-critical apps and collaboration tools getting only longer, figuring out which password is for what app and then how to log in can feel like a full-time job. Simply said, usernames and passwords are not an effective way to secure access to information. As a result, federated authentication and enabling SSO via modern identity providers and identity standards are now table stakes.

How digital workspace platforms using Zero Trust strategies help

Digital workspace platforms that leverage Zero Trust concepts make it possible to enable the implementation of conditional access policies that factor in identity, location and device context. This is particularly important for remote workers. If an employee who typically logs in from one location suddenly logs in from a different location, then it makes sense to require additional authentication for security purposes. Doing so requires that the identity management, device management, and security systems in place are connected and can communicate with one another. Most organizations also want to use their existing resources to improve security and experience for remote users accessing apps. This means that conditional access capabilities need to be built on a foundation of Unified Endpoint Management (UEM) to provide the visibility into devices that is necessary to block access if they are missing important security patches, for example.

Simplifying and streamlining access for remote workers requires federating all apps and implementing modern authentication mechanisms with user-friendly, multi-factor authentication experiences. Zero Trust and conditional access platforms need to be able to work with an existing identity provider to leverage any investments already made in federating SaaS apps.

KEY CONSIDERATIONS

Finding the right digital workspace platform means knowing how it will be used, and which features are most important based on intended uses. IT teams can get started by asking these questions:

Use case considerations

1. How many SaaS and mobile apps do employees use today, and will more be introduced in the future?
2. Do IT teams spend too much time on password reset requests?
3. Is visibility required into which employees and devices access corporate data?

Solution considerations

1. Does it integrate with the UEM or client management platform?
2. Does it deliver an improved user experience for better IT-business partnership?
3. Does it support conditional access for all types of apps?
4. Can it connect to other cloud services for maximum efficiency?
5. Will it integrate with any identity management platforms and SSO mechanisms that have already been implemented?
6. Can it be hosted as a service for greater agility?

VMware Workspace ONE and Workspace ONE Access Technology

With the VMware Workspace ONE® digital workspace platform featuring Workspace ONE Access technology, organizations can leverage existing identity management investments and provide multi-factor authentication and conditional access to any application, from any device.

Workspace ONE provides visibility into devices through unified endpoint management and security integrations. By using Workspace ONE Access technology on top of the UEM and security features, it's possible to implement a Zero Trust security model that protects sensitive information without compromising user experience. Together, the two technologies solve the key extended-network challenges that plague both end users and IT teams.

The Workspace ONE Conditional Access Control Model

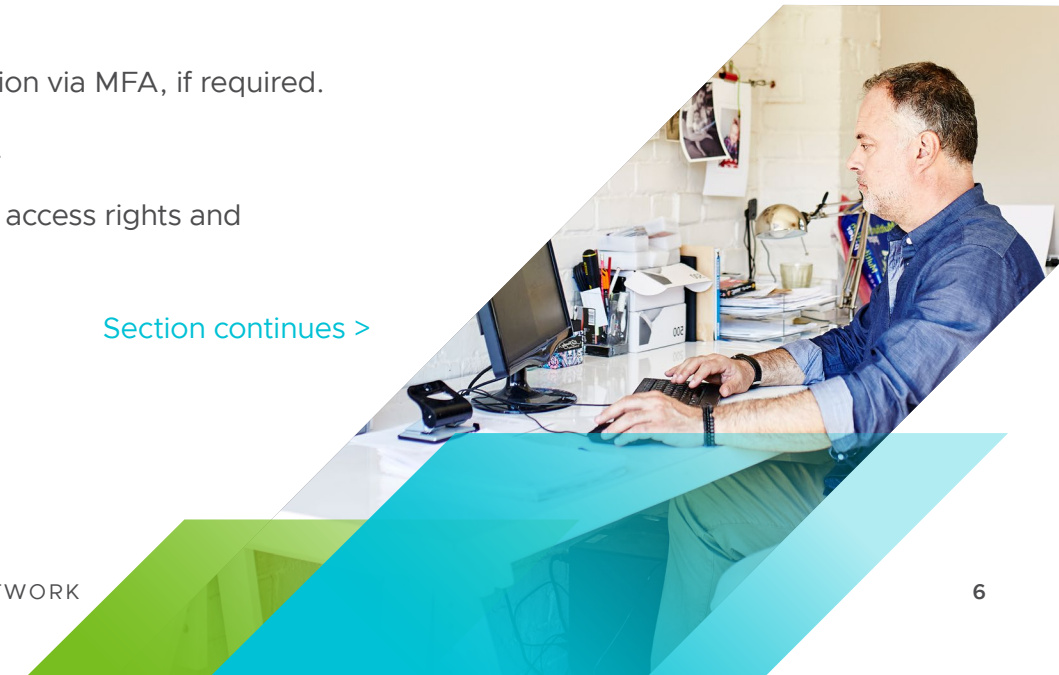
The Workspace ONE Zero Trust platform and conditional access control model policies incorporate the following key elements:

- Device information, such as health, whether it's managed, has a password, and has been patched or jailbroken.
- Identity data, such as recent authentication or strong authentication via MFA, if required.
- Transport, to validate the method and security of the connection.
- Apps and data to determine whether the user has apps and data access rights and if the app has appropriate digital rights management.

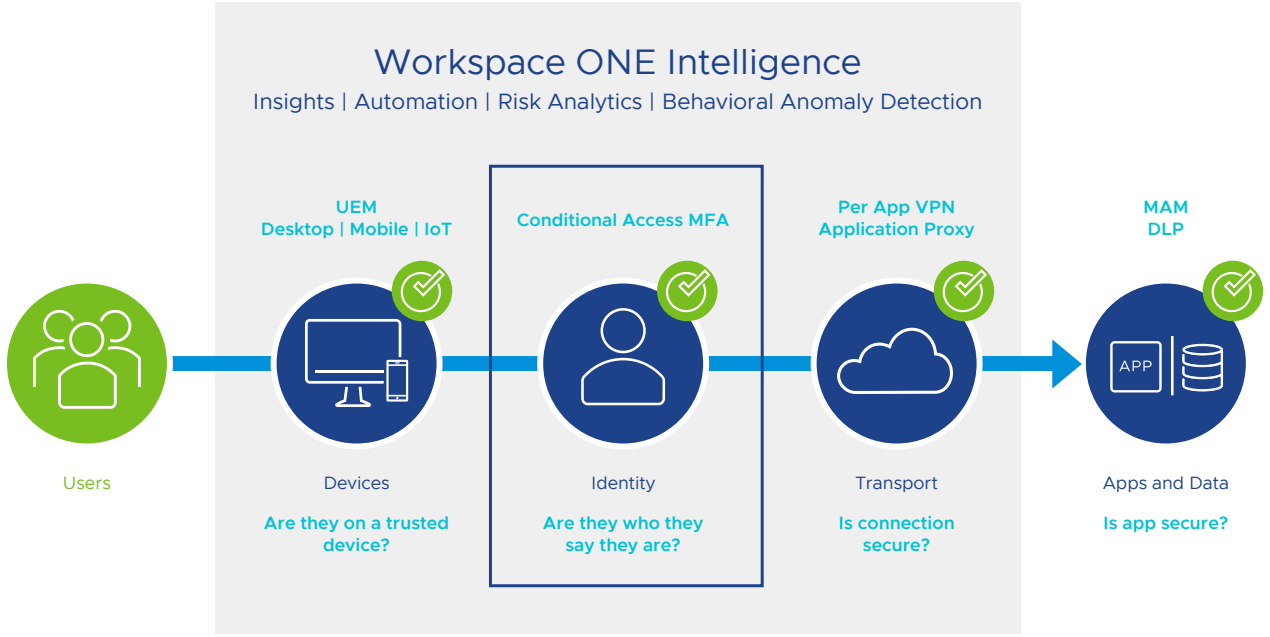
Section continues >

WORKSPACE ONE DELIVERS

- Engaging employee experiences
- Unified endpoint management
- Intelligence across the digital workspace
- Simplified Zero Trust security



Because these attributes are continually re-validated to ensure that the access is still acceptable, a user is not granted broad, long-lived access to a wide range of resources. Instead, the user must meet the requirements every time access is requested. But with modern forms of single sign-on and federation technologies, this is a seamless process. While a user may see MFA prompts when accessing high-value resources or changing to a new device or location, all validation happens in the background.



LEARN MORE

Web Pages

- *VMware Workspace ONE*
- *Workspace ONE Access*

ESG Economic Validation

- Read the *ESG paper* validating the benefits of Workspace ONE access deployed in the cloud, including improved business agility, remote worker capabilities, accelerated path to Zero Trust security, and more.

Factor #2: For Quality Without Compromise, Should SD-WAN Be the Plan?

When the network slows, frustration spikes and productivity can plummet. For remote workers, this can be a daily reality. Whether it's due to nonstop videoconferencing, virtual happy hours, or Netflix bingeing, all too often the result is a last-mile connection that is way too slow.

Another source of frustration stems from the modern apps that most employees use to do their jobs. Traditional network configurations require SaaS apps and apps with cloud connectivity to be routed back to the data center, and this can lead to VPN congestion, performance problems, and a poor user experience.

Additionally, many organizations use VDI in an effort to deliver applications more effectively to their work-from-home workforce, primarily because it provides flexibility and ease while maintaining security. But these benefits won't be realized when applications perform poorly, which can happen when virtual applications and desktops are delivered across a WAN that suffers from limited bandwidth or poor connectivity performance.

What SD-WAN can do

SD-WAN can help overcome the performance-dragging impact of latency, packet loss, and bandwidth limitations that cause virtualized applications and desktops to perform poorly or become unreliable across the WAN. With roots in the software-defined networking practice of decoupling network software services from the underlying hardware, SD-WAN simplifies branch office—or home office—networking. It also can help extend the quality of service for critical business apps and solve for slow last-mile connections.

IS SD-WAN THE RIGHT CHOICE?

Organizations should consider implementing SD-WAN to help optimize remote employees' extended network if:

1. Home users experience productivity challenges to stay connected to their office applications.
2. Helping home users get connected to the workplace is overwhelming IT.
3. Connecting users to the growing number of SaaS apps and apps deployed in the cloud is challenging.
4. Home office security needs are top focus areas.

VMware SD-WAN by VeloCloud

Not all SD-WAN solutions shine equally as brightly. With *VMware SD-WAN by VeloCloud®*, organizations can provide reliable, remote access to any type of application (on-premises or cloud) without compromising the quality of experience from the home office. VMware SD-WAN is the industry-leading WAN edge services platform for both branch and at-home users, delivering simple, reliable, intrinsically secure, and optimized access to traditional and cloud applications.

VMware SD-WAN by VeloCloud delivers:

Assured application performance

By constantly monitoring the state of WAN links, VMware SD-WAN ensures that a user session is always steered over a low-latency path. The solution classifies and prioritizes real-time applications over other applications during network congestion or brownouts.

Self-healing

VMware SD-WAN performs dynamic remediation during brownouts on WAN links and addresses packet loss with real-time forward error correction (FEC). Each packet can be duplicated over Internet links using FEC to help ensure that home users don't have to reset their conference calls or drop and reset an ongoing VDI session.

Path optimization

A key differentiator is the VMware SD-WAN Gateway, which is highly available and hosted strategically at nearest entry points to applications in the cloud such as Zoom, Salesforce, and VMware Horizon® on public cloud providers like Microsoft Azure. Home users have instant access to all the cloud applications through a VMware SD-WAN Gateway.

Section continues >

Simplified operations for IT teams

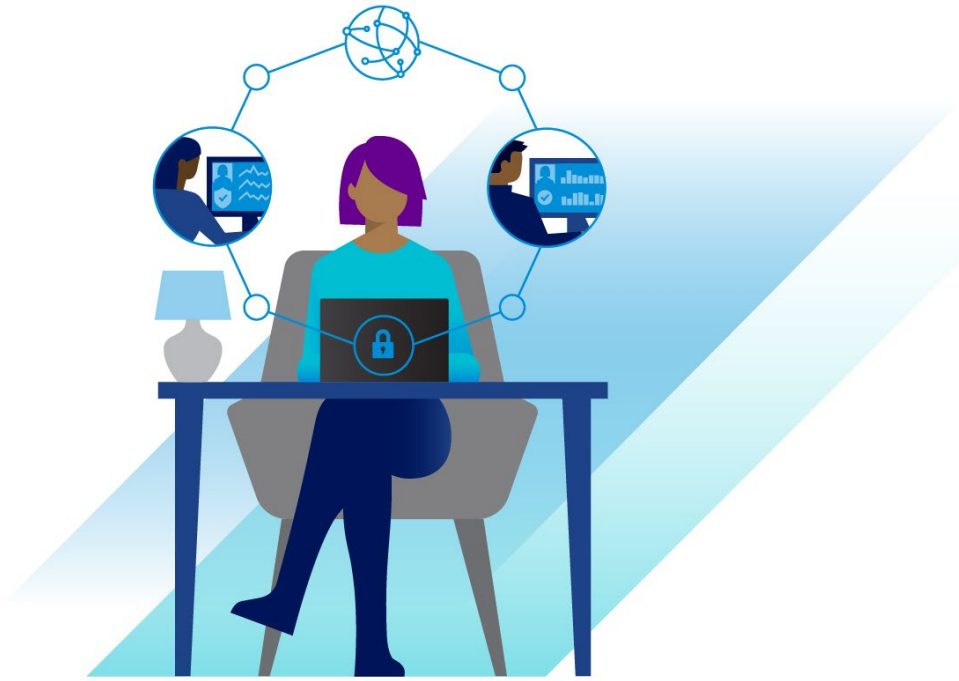
Get visibility into application performance, set policies from a central location, and troubleshoot application delivery issues without in-home IT visits. The VMware SD-WAN Orchestrator makes it easy to monitor devices and the performance of applications on the network.

Intrinsic security

Benefit from flexible options for network security including a built-in firewall, the option to use firewalls from a third-party security vendor deployed in a virtual machine on the SD-WAN Edge as a virtual network function (VNF), or directing specific applications to Cloud Web Security providers using the SD-WAN Gateway.

LEARN MORE

- Visit the *product* webpage
- Explore *awards and accolades*



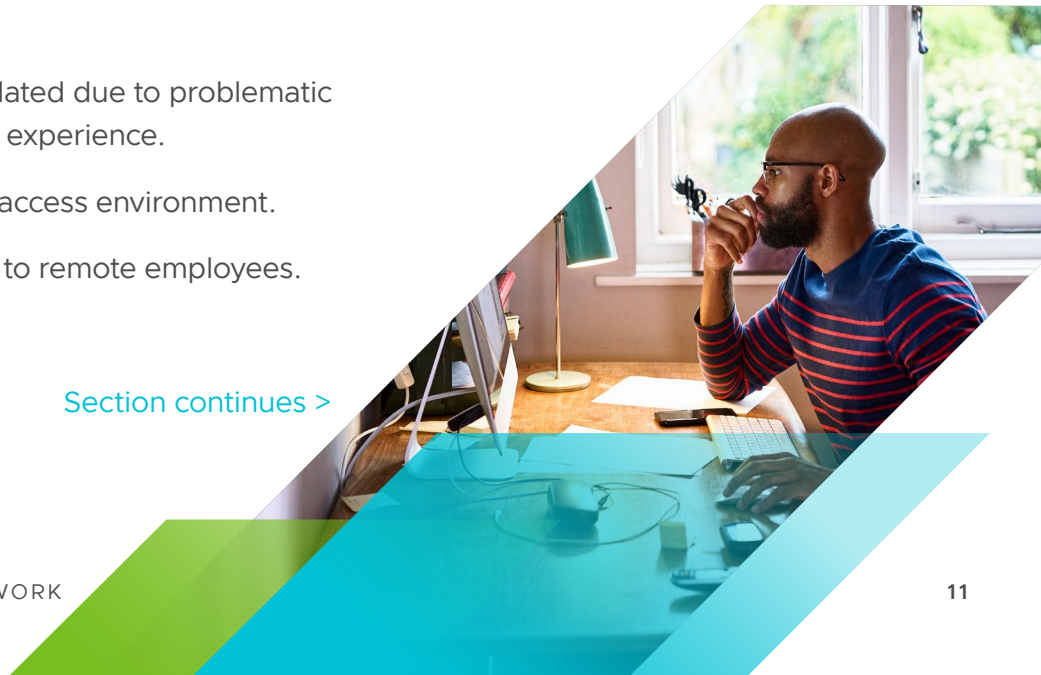
Factor #3: Is Now the Time for Modern Management, Endpoint Security and VDI?

Traditional PC lifecycle management (PCLM) tools were built for a world when users and devices were always on-premises and not on an extended employee network. The majority of workflows were designed to happen in one location. Imaging and provisioning new devices, patching and updating operating systems from on-premises servers, receiving Group Policy Objects, managing users' identity and passwords on devices, and distributing large applications all relied on network access. While some of these management tasks can be completed during times when users are connected to the network via VPN, issues arise when all devices suddenly must be serviced via an already overcrowded VPN connection.

IT teams trying to use these tools to distribute apps, deploy updates and patches, and troubleshoot user problems at the edge wrestle with multiple issues, including:

- Remote device security due to poor visibility, especially when users don't regularly connect via VPN.
- Security patches that aren't implemented and apps that aren't updated due to problematic VPNs, which leads to security and compliance risks and poor user experience.
- Challenges making access decisions in a Zero Trust or conditional access environment.
- Difficulties provisioning new devices and providing timely support to remote employees.
- Users being denied access to their devices.

Section continues >



Fortunately, there are three alternative approaches to consider:

Modern management

Unlike traditional PCLM, modern management is cloud-first and built for a distributed ecosystem. IT teams can provide remote workers with a seamless user experience on company-owned or personal devices.

Unified endpoint protection (EPP) and next-gen antivirus (NGAV)

In a virtual world, endpoints are the new perimeter, and EPP and NGAV can help to disrupt advanced attacks in a perimeter-less and continually evolving threat landscape.

VDI

An alternative to VPN as a means of remote access, VDI can simplify the management and delivery of virtual desktops in the cloud, and also boost the performance of legacy or client-server apps.

KEY CONSIDERATIONS

Not all of today's tools take the same approach. Here's what to consider:

1. Does the UEM solution support different types of devices?
2. Does the UEM solution provide modern management for Windows 10 devices from the cloud rather than via VPN?
3. Will the UEM solution integrate with an access management platform to support Zero Trust or conditional access?
4. Does the UEM solution provide full visibility into devices that are not on the corporate network or VPN?
5. Will the UEM solution enable distribution of large OS patches and app updates to remote devices without crippling the VPN?
6. Does the VDI platform deliver enterprise-class management features such as hybrid and multi-cloud support?
7. Does EPP or NGAV integrate with the device management platform for threat remediation?
8. Can the solution reduce the mobile access footprint to the data center to minimize the attack surface?

VMware Workspace ONE enables modern management to simplify IT operations, harden security, and deliver ready-to-work experiences across every app and endpoint—physical or virtual. Over-the-air management with Workspace ONE ensures IT can reach every endpoint and keep them always up to date on policies, patches and app versions.

Compared to legacy PCLM, Modern Management with Workspace ONE UEM offers:

- Multiple deployment and provisioning options that skip high-touch imaging
- Real-time configuration from silicon to software
- Intelligent automation for always-up-to-date patching
- Cloud-scale distribution for all apps
- Persistent security, hygiene and compliance

VMware Workspace ONE UEM also integrates with VMware NSX®, meaning that mobile applications that connect to internal networks can connect only to specified data center resources. Bringing speed, security and simplicity to networking, the integration between VMware NSX and VMware Workspace ONE Tunnel can enable IT administrators to create policies that dynamically follow mobile application resources, without the need for time-consuming network provisioning. The integration allows for segregating traffic from application to specific workloads in the data center. This substantially reduces the attack vector of malware and viruses that could do significant harm to the organization, an aspect that is increasingly important for the distributed workforce.

Conclusion

Remote work is no longer an option or an initiative. Almost overnight, a distributed workforce has become a global imperative and essential to a business continuity plan. New IT priorities including rapid setup, instant scaling, support, and security are examples of the emerging considerations under this new normal.

VMware Future Ready™ Workforce Solutions—Workspace ONE, Workspace ONE Access technology, and SD-WAN by VeloCloud—provide the digital foundation needed for current and future remote work use cases. With VMware solutions, you can:

- Leverage existing identity management investments and provide multi-factor authentication and conditional access to any application, from any device with the Workspace ONE digital workspace platform featuring Workspace ONE Access technology.
- Provide reliable, remote access to any type of application (on-premises or cloud) without compromising the quality of experience from the home office with SD-WAN by VeloCloud.
- Enable modern management to simplify IT operations, harden security, and deliver ready-to-work experiences across every app and endpoint—physical or virtual—with Workspace ONE.

Take the Next Step

The trusted infrastructure provider of choice for more than 500,000 customers globally, VMware's progressive technologies not only pioneered virtualization but now deliver a uniquely consistent platform for cloud and business mobility. As a proven leader, we help organizations across the world run, manage, connect and secure applications across clouds and devices in a common operating environment, delivering both freedom and control.

Reach out to your local *VMware representative* or *partner* for more information, or learn, evaluate and validate *VMware network and access optimization solutions on the Pathfinder Trial Experience page.* >

Join us online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: FY21-5890-VMW-REMOTE-FIRST-BUYER'S-GUIDE-EBK2-USLET-WEB-20200730 7/20