Trust and the Distributed Workforce

How VMware and partners can help customers overcome the obstacles to distributed workforce success
Executive summary

Nearly every organization wants to embrace a distributed workforce model, but most are struggling to solve key challenges such as fragmented or insufficient security, operational complexity, and poor employee experience. As the leader in delivering reliable remote access, endpoint security, and endpoint device management, VMware is uniquely positioned to help.

Together with our partners, VMware can provide the strategic guidance and innovative technology solutions that organizations need to transform security, modernize IT, and deliver a seamless experience to remote employees.

The rise of the distributed workforce

In response to the events of 2020, many organizations successfully spun up new technologies and rolled out new processes to enable their employees to stay connected and productive during a forced period of remote work. However, what they didn’t realize and could not prepare for was the coming change in how and where work would be done.

After a prolonged period of working remotely, many employees have come to enjoy the flexibility and don’t want to return to an office at all, or at least not 100 percent of the time. In fact, according to a recent survey commissioned by VMware, 61 percent of employees agree that remote work is no longer a perk, and 70 percent want the ability to easily work from anywhere.

Employers also are recognizing the benefits of supporting a distributed workforce model, such as the ability to recruit new employees from a wider geographic pool, helping to facilitate a better work-life balance for employees, and potentially reducing office real estate costs.

However, many organizations realize that to support a high-functioning distributed workforce for the long term, they need to address key technology-related challenges that weren’t nearly as problematic when they thought remote work was simply a short-term situation.

These organizations are now coming to grips with fragmented and insufficient security and operational complexity. They have a profound need for better ways to secure and manage the proliferation of new edge devices, provide fast access to software-as-a-service (SaaS) applications to remote workers at scale, and ensure a best-in-class employee experience to attract and retain top talent.

Fragmented, insufficient security

Protecting a distributed organization requires the ability to extend security policies to new endpoints scattered across a broad array of locations, as well as provide visibility into all distributed apps, data, devices and networks.

Zero Trust is a security approach that operates on the assumption that no device should be trusted—even if it’s connected to a managed corporate network. Secure access service edge (SASE) simplifies wide area networking and security by delivering both as a cloud service. Other innovative technologies such as VMware Carbon Black Cloud™ provide consolidated endpoint and workload protection, threat hunting, incident response, audit and intelligent conditional access to protect assets. Together, they have become the model of choice for distributed enterprises, but security leaders often struggle with the fundamental shifts in strategy and architecture required to holistically implement it.

2. IDC. “Mobile Workers Will Be 60% of the Total U.S. Workforce by 2024, According to IDC.” September 2020. PRUS46809920
Operational complexity
Many organizations had to piece together a remote workforce strategy using ad hoc solutions, which created silos and tool sprawl. The role of technology leaders has had to continuously evolve to manage outcomes, not tasks, with intelligent compliance, workflow and performance management. Greater adaptability is required for the business, driving the need to provide IT with integrated solutions that are actionable and automated, while broadening visibility, and reducing silos and operational overhead.

Employee experience
Employers need to prioritize employee experience, which means ensuring that both knowledge and frontline workers enjoy a consistent, high-quality experience in any location using their device and operating system of choice. However, since the beginning of the pandemic, more than 50 percent of remote employees have reported wrestling with technology issues, and 90 percent feel that it is their employer’s responsibility to provide the tools they need to be productive.3

Overcoming the obstacles to distributed workforce success
Technology—not geography—is a key driver of employee experience and competitive differentiation in a distributed enterprise. However, too many organizations are struggling with an assortment of technologies they quickly stitched together to support what they thought was a short-term period of remote work rather than a permanent shift to a work-from-anywhere model.

Meeting the needs of the distributed workforce means delivering uncompromised technology experiences for employees through remote work experiences, which can significantly improve satisfaction and help boost their productivity. A best-in-class digital experience for employees is one that optimizes onboarding for new team members wherever they are located; provides access to all the tools, technologies and resources they need to be productive on Day 1; and offers them flexibility and choice of platforms and devices.

Whether organizations are planning a 100 percent return-to-office strategy, are pivoting to 100 percent remote, or want to support a hybrid work model that enables employees to shift seamlessly between the two, ensuring a best-in-class digital employee experience also requires the intelligence needed to provide the right access to the right workers right when they need it, wherever they need it.

To strengthen the security and compliance posture for more effective risk mitigation in increasingly distributed work environments, IT teams need to change traditional security models that do not scale. That means consolidating vendors to reduce security fragmentation and silos, and get the visibility and management they need to make Zero Trust work. Finally, IT teams that are overwhelmed by operational complexity need ways to automate the workspace completely, in a manner that is driven by outcomes and not just tasks.

The partner perspective

Combining key elements of SASE, endpoint security technologies, unified endpoint management, and desktop and app virtualization can give organizations the confidence they need to fully embrace distributed work at scale. However, few organizations are in a position to rip and replace their security, networking and end-user computing technologies all at the same time.

This is a key reason why IT leaders are looking to partners for strategic guidance as well as assistance designing, implementing and managing the type of technologies that will put them on the path to becoming a true Zero Trust distributed organization. They need innovative solutions that can accelerate outcomes and that also align with their business priorities, budgets and technology refresh timelines.

With VMware Anywhere Workspace, partners have an unprecedented opportunity to create new and ongoing revenue streams by providing customers with the technologies and expertise required to make it easier to implement a Zero Trust approach across the distributed workforce.

In fact, Anywhere Workspace is the first and only architecture that combines the capabilities of SASE, digital workspace, and endpoint security technologies required for highly engaged and productive employees, end-to-end Zero Trust security, and simplified IT modernization. IDC analyst Phil Hochmuth called it “a smart combination of three critical technologies for successfully supporting a remote/hybrid workforce.”

Anywhere Workspace combines three key VMware technologies:

- VMware Workspace ONE® for unified endpoint management, desktop and app virtualization, endpoint security technologies, and a variety of employee experience, productivity and security-related solutions.
- VMware SASE Platform™ for Zero Trust network access.
- VMware Carbon Black Cloud for cloud native endpoint and workload protection.

The VMware advantage

No other vendor provides this type of convergent infrastructure that allows for connected visibility and context across all vectors, which ensures that security coverage is broader and more effective, following users, data and apps wherever they are. Because of this holistic approach, VMware can leverage these synergies to simplify processes with optimized, intelligent workflows that allow IT to drive business outcomes and reduce tools, silos and operational overhead.

However, customers don’t need to implement the entire solution to realize value, nor do partners need to have established practice areas for each of the three core technologies to help customers make meaningful, ongoing progress toward becoming a Zero Trust distributed organization.

For example, end-user productivity is a top-of-mind topic for all customers, and the ability to work from anywhere is a primary component of it. End-user productivity has wide applicability across traditionally siloed teams in IT, security and networking, and lines of business. This is one reason why it’s critical to start the conversation at the CXO level and articulate the value of an integrated solution covering remote access, optimized bandwidth and security. Partners with an end-user computing practice can use Workspace ONE as an entry point to customer engagements while they become experts in the additional Anywhere Workspace technologies and the opportunities presented by the integrations among them.

---

Anywhere Workspace also provides VMware partners with an unprecedented opportunity to create new and ongoing revenue streams by enabling a true multimodal experience through offerings such as device as a service and experience as a service to customers via a single channel from an integration and support perspective. It’s a highly relevant solution that is applicable to all customers, segments and industries that have expressed interest in improving employee experience and productivity, want to secure the distributed edge, or are looking to modernize and automate their workspace through digital employee experience management, intelligence and application performance.

**Take the next step**

As organizations double down on efforts to embrace a distributed workforce model, they are looking to technology partners to provide domain expertise and deliver the innovative technology solutions required to strengthen security, streamline operations, and provide a best-in-class employee experience.

VMware is committed to helping partners help their customers build trust in the distributed workforce. To learn more, visit the [VMware Anywhere Workspace solutions page](#) or contact your Partner Business Manager.