Brought to you by:

vmware®

Anywhere Workspace

for dummies®
A Wiley Brand

Deliver exceptional user experiences

Deploy Zero Trust security

Enable IT modernization

VMware Special Edition

Lawrence Miller

About VMware

VMware is a leading innovator in enterprise software. We power the world's digital infrastructure and today's anywhere organizations. Our cloud, app modernization, networking, security, and anywhere workspace platforms form a flexible, consistent digital foundation. This foundation empowers businesses to build, run, manage, connect, and protect applications, anywhere — enabling technology-driven transformation without disruption.

A digital foundation built on VMware enables rapid, technology-driven innovation and continuous integration of emerging technologies. Organizations can move quickly without disrupting business operations, while maximizing return on investments in people, processes, and systems.

Anywhere Workspace

VMware Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Anywhere Workspace For Dummies®, VMware Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-1-119-79674-9 (pbk); ISBN 978-1-119-79675-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: Cynthia Tweed

Production Editor: Tamilmani Varadharaj

Introduction

Organizations around the world have adapted to a "new normal" of remote work in the wake of the COVID-19 pandemic. With many lessons learned, and perhaps many more to be learned, businesses are discovering what they must do to survive — and even thrive — in a world economy that is driven by a distributed workforce. After the initial rush to simply keep the proverbial "lights on" with their employees working from home, companies are now (or should be) prioritizing their investments in work-from-home technology to enable a highly productive and collaborative anywhere workforce today and in the future.

The anywhere workforce encompasses not only distributed people, but also distributed systems, applications, networks, data, devices, security, and customers. A weak foundation of disjointed technologies will inevitably lead to gaps in security, operations, and performance for the anywhere workforce. A unified digital foundation empowers organizations to become leaders in the new world of work.

As the challenges of the future continue to emerge and evolve, organizations need to be prepared to deliver the tools and digital experience their employees need to work productively in new and better ways. This book fills you in on the distributed workforce technologies that enable a sustainable and resilient remote work strategy through a secure, scalable, and unified digital infrastructure to ensure your business is ready for the future in a post-COVID world.

About This Book

Anywhere Workspace For Dummies consists of seven chapters that explore the following:

- How the nature of work has changed (Chapter 1)
- What technologies have emerged to be more relevant in supporting today's modern anywhere workforce (Chapter 2)
- Use cases for delivering exceptional user experiences (Chapter 3)

- How to implement Zero Trust security for your organization (Chapter 4)
- The need for IT modernization (Chapter 5)
- How workplace safety is changing (Chapter 6)
- Key outcomes you can expect when you invest in the right technologies for your distributed workforce (Chapter 7)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though I don't recommend upside down or backward).

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless!

Mainly, I assume that you're a chief technology officer (CTO), vice president, or director responsible for end-user computing technologies for your organization. I assume you have at least a basic understanding of technology fundamentals and concepts such as cloud computing, networking, and virtualization. As such, this book is written primarily for technical readers.

If any of these assumptions describes you, this is the book for you. If none of these assumptions describes you, keep reading anyway — it's a great book, and when you finish reading it, you'll know quite a lot about modern distributed workforce technologies!

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

TIP

Tips are appreciated, never expected, and I sure hope you'll appreciate these useful nuggets of information.

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!

WARNING

These alerts point out the stuff your mother warned you about. Well, probably not, but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of!

Beyond the Book

There's only so much I can cover in this short book, so if you find yourself at the end of this book, thinking, "Gosh, this was an amazing book! Where can I learn more?," just go to `www.vmware.com/solutions/anywhere-workspace`.

IN THIS CHAPTER

- **Recognizing remote work as the new normal**
- **Understanding the challenges of the distributed workforce**
- **Adapting to the modern distributed workforce**

Chapter 1
Changing the Way We Work in the Wake of the Pandemic

Once considered a flexible work option or an employee perk, remote work has now become a global imperative that is essential to business continuity and success. To enable productivity, security, and simplified management in this new normal, companies must address evolving requirements for their anywhere workforce including rapid device setup and onboarding, instant scaling, remote support, and robust security.

In this chapter, we explore how remote work has evolved and become the new normal, the challenges that organizations must address to support a distributed workforce, and how your organization can evolve into a modern anywhere workforce.

The Anywhere Workforce Is Here to Stay

The COVID-19 pandemic has forced companies everywhere to quickly deploy and support remote-working technologies to enable their employees to stay productive and to keep their businesses moving forward. For many organizations, this crisis has demonstrated that remote work is a very real and viable option now and in the future.

In *The New Remote Work Era: Trends in the Distributed Workforce* by Vanson Bourne and commissioned by VMware and Dell, several key findings are identified, including the following:

- **Leveling the playing field:** By embracing remote work, organizations and industries that were once behind the curve are leveling the playing field and finding new opportunities to innovate and be more inclusive.
- **Debunking remote work myths:** By and large, concerns about the transition to distributed work were not realized. The opposite was true: Organizations and individuals saw benefits that they'd be hard pressed to give up now that they've successfully adapted their work cultures.
- **Changing the paradigm with flexible remote-work options:** Owing to these benefits, the ability to work remotely is now more widely deemed a prerequisite even across what would be considered traditional organizations and industries.
- **Reducing costs and reinvesting in the future of work:** Organizations anticipate significant cost savings as a result of remote work. The majority of smaller (fewer than 1,000 employees) and high-performing organizations (year-over-year revenue growth of 15 percent or more) are expecting to reinvest those cost savings in key areas.

Leveling the playing field

Organizations of all sizes, across all industries, are seeing benefits from their shift to a distributed work model, with 77 percent of respondents to the Vanson Bourne survey saying that their remote work capabilities were underutilized until recently.

Smaller organizations seem to be enjoying advantages that could help them better compete with their larger counterparts. Seventy percent of all respondents agree that smaller organizations are able to adapt faster to remote work, and smaller organizations themselves agree to a greater extent than larger ones, indicating that they're experiencing the ease of the remote-work transition firsthand. Smaller organizations are also seeing the benefits of remote work when it comes to competing for top talent (see Figure 1-1).

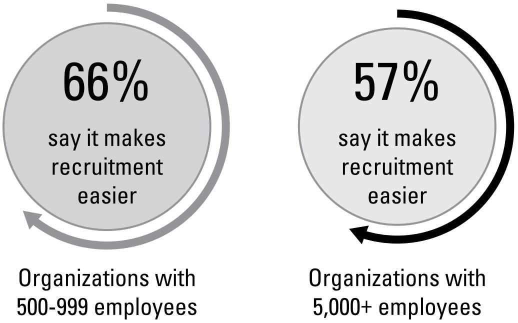


FIGURE 1-1: To what extent do you believe having a remote work option impacts the ease of recruiting top talent?

Another key outcome of the distributed workforce model has been the shift from a headquarters-centric mindset to a better integration of satellite offices and teams. After all, when no one is at the center of the action, everyone can be part of the action. Of the respondents whose organizations consist of a headquarters along with branch or regional offices:

- Seventy-three percent agree that **innovation has been coming from more places in the organization** since more employees started working remotely.
- Seventy-five percent agree that **employees in regional/ satellite teams feel more empowered to make decisions.**
- Seventy-six percent agree that **shared resourcing between offices has increased.**

TIP

The distributed workforce model has the potential to create organization-wide efficiencies and decentralize internal engines of innovation, while simultaneously boosting employee morale and feelings of empowerment.

In addition to fostering equity on an organizational level, remote work can create opportunities for individuals, both in recruitment and once inside the company. For example, remote-work options and policies are helping organizations to recruit and retain:

- Working parents (83 percent)
- Minority candidates (71 percent)
- Employees with disabilities (79 percent)
- Candidates living outside major economic hubs (83 percent)

After they're hired, employees may also find more inclusive workplaces thanks to remote work:

- Sixty-five percent feel **more empowered to speak up in video conference meetings** than in person.
- Sixty-nine percent say **the majority of their team feels more empowered to speak their mind** to leadership.
- Seventy-one percent agree that **time in meetings is more likely to be evenly shared between men and women** — with men and women agreeing to a relatively equal degree (72 percent and 70 percent, respectively).
- Seventy percent agree that **traditional advantages like physical stature are less meaningful now** that most employees are working remotely.

Having identified both immediate and future benefits to remote work, many organizations are considering how the shift to a distributed workforce can drive delivery of new business models in their industries. For example, 80 percent of respondents in health care agree that the move to telehealth has created significant challenges in the short term, but 85 percent believe it will create opportunities in the long term, including the following:

- The acceleration of remote consultations and routine checkups (87 percent)
- The need for health systems to restructure reimbursement/payment models (80 percent)
- The emergence of new health specialties and job opportunities (80 percent)

Debunking remote work myths

One of the most common remote work myths is that productivity will plummet. However, in *The New Remote Work Era: Trends in the Distributed Workforce,* Vanson Bourne found that, since going remote, more than two-thirds (67 percent) of organizations have found that productivity has either increased or stayed the same.

Another common remote work myth is that employees will lose touch with their teams. Not only has this fear not materialized, but many respondents saw improved relationships with their colleagues, perhaps resulting from teams making a more conscious effort to check in with each other. Seventy-six percent say their personal connection with at least some of their colleagues has improved, and 14 percent say their personal connection with all their colleagues has improved. Sixty-two percent of respondents also report that team collaboration has either increased or stayed the same.

Finally, there is a common misperception that morale will suffer in a remote work environment. However, 83 percent of respondents feel that they've adapted surprisingly well to working remotely. And these numbers hold relatively even when split across age and gender, although women seem to be adapting slightly better than men. Interestingly, people who consider themselves to be introverts and those self-identifying as extroverts also agreed to a relatively even degree. Additionally:

- Sixty-eight percent say their **stress levels have improved.**
- Seventy-seven percent say their **work–life balance has improved.**
- Respondents report an average of **59 minutes a day saved by working remotely,** likely as a result of not having to commute or get ready for work.

Changing the paradigm with flexible remote-work options

Prior to the global pandemic, the ability to work remotely was widely regarded as a "nice to have," not something most employees would expect. But having seen the benefits directly, many organizations now consider a remote-work option to be a crucial component of employee experience.

Perhaps counterintuitively, older employees seem to be embracing remote work even more readily than their younger counterparts. Among Baby Boomers (born between 1946 and 1964), 22 percent reported having no concerns with remote working, whereas only 9 percent of Generation Z (born after 1996) workers had no concerns. Among the respondents who did have concerns, Baby Boomers were much less likely (39 percent) than Generation Z (47 percent) workers to worry that their team would stay on task.

REMEMBER

Despite experiencing some challenges in implementation, even the most traditional organizations are increasingly embracing remote work as the rule rather than the exception.

Reducing costs and reinvesting in the future of work

In *The New Remote Work Era: Trends in the Distributed Workforce*, the vast majority of participants (90 percent) anticipate that the shift to remote work will result in cost savings over the next 12 months. Not surprisingly, the top areas for savings include

- Employee travel (54 percent)
- Facilities overhead, such as office space (50 percent)
- Maintenance costs, such as electricity (49 percent)

REMEMBER

Regardless of the amount companies save, the true indicator of remote work's impact on the enterprise will be how effectively those savings are reinvested. For respondents who say their companies will have savings from remote work in the next 12 months, the top three areas where they plan to reinvest are:

- Technology upgrades (57 percent)
- Product or service innovation (44 percent)
- Employee programs, such as diversity, equity, and inclusion (38 percent)

Addressing New Challenges in the Distributed Workforce

As organizations quickly deploy new remote work capabilities, they must address several key challenges, including:

- **Delivering an engaging employee experience and enabling remote productivity:** Before the pandemic, organizations sought to enable mobile and remote workers to be productive on "any device, anywhere, and at any time." With practically every worker suddenly becoming a remote worker, organizations must now enable their entire workforce to be productive on "every device, everywhere, and all the time." Setting up remote employees with a device is just one issue that IT teams must address. Organizations must also ensure that remote employees can reliably use other resources, including applications and data, and get IT support as needed. It is not practical (or responsible) for IT to provide on-site support at employees' home offices. Touch-free service delivery is a much more scalable business practice for remote work and is a must for businesses to operate in the current and post-COVID world.
- **Protecting a vastly larger attack surface:** With the majority of employees in many organizations now working from home, every home office has become a branch office. However, unlike a traditional branch office in which an organization provisions reliable Internet service, creates a site-to-site virtual private network (VPN), secures the Wi-Fi network, and deploys and manages security equipment (such as firewalls and endpoint protection), as well as all connected devices, organizations have far less control of their employees' home office environments. As a result, the attack surface has grown exponentially, literally overnight, and threat actors are exploiting this new, target-rich environment. According to a study by Barracuda Networks, nearly half (46 percent) of global businesses have encountered at least one cybersecurity incident since shifting to a remote working model.

WARNING

Many organizations lack an effective management or security model beyond the corporate network to support sending corporate devices home or allowing personal devices to be used for work at home.

- **Maintaining governance and compliance:** Ensuring effective governance across a distributed workforce can be particularly challenging for organizations mired with manual workflows and business processes. Restricting where sensitive or private data is processed and stored, for example, to managed devices or back-end systems accessed via virtual desktop infrastructure (VDI), requires appropriate technologies to enforce these policies and monitor compliance. For organizations subject to regulatory requirements, such as the European Union (EU) General Data Protection Regulation (GDPR) or the U.S. Health Insurance Portability and Accountability Act (HIPAA), the governance challenge is still more critical because noncompliance can subject the organization to significant penalties, breaches of customer trust, and loss of revenue.

- **Providing instant scalability in back-end data center infrastructure:** Enabling remote work requires more than just providing devices for your employees to use in their home offices. Rapidly increasing the number of users connecting to your VPNs and remotely authenticating can utterly cripple these critical systems. Organizations must ensure their core business systems and networks can scale quickly to handle greater loads. Employees interact with many systems that need to be scaled to match the increase in demand in organizations' data centers. Many organizations with traditional client–server and three-tiered applications remain dependent on specific Windows configurations, usually requiring VDI, which itself creates unique challenges.
- **Guaranteeing performance:** Ensuring performance of the applications that employees are using, as well as the network and back-end IT and business systems is critical. If remote employees can't get the level of application performance or the network bandwidth they need to do their jobs, the business will suffer.

Evolving into a Modern Distributed Workforce

Traditional IT environments are not designed to support a workforce that is completely distributed. They're built around corporate networks and data centers that connect branch offices to headquarters locations and support a relatively limited number of remote workers. The traditional IT service delivery model provides remote support for basic help-desk issues, with more difficult issues typically being escalated to a desktop support team that often provides in-person assistance, as well as physical setup and configuration of equipment in an employee's office or cubicle.

The shift to a modern anywhere workforce has been accelerated by the global pandemic and has forever changed the way we work. Although many organizations will undoubtedly return to their pre-COVID "normal," every organization in the world should, at a minimum, understand the importance of having a robust business continuity plan supported by the right people, processes, and technologies necessary to execute it. For many organizations, the shift to remote work is an opportunity to bolster their workplace flexibility options, improve their technology investments and cybersecurity, and take another look at their operational processes.

Every business today must traverse three distinct phases in the distributed workforce journey, each requiring specific steps and actions:

- **Phase 1 – Respond (Business Continuity):** Sustain business operations in a time of crisis. Secure vital data, information, and systems. Rapidly enable remote workers and preserve customer engagement.
- **Phase 2 – Adapt (Business Resiliency):** Make targeted investments to increase automation and flexibility. Drive a return to business growth. Optimize costs, eliminate complexity, redundancy, and inefficiency. Expand workforce efficiency and capabilities.
- **Phase 3 – Accelerate (Digital First):** Focus on increasing velocity and new service delivery. Adopt a digital-first model for IT and business. Deploy new and innovate work styles. Harden the business against future challenges.

REMEMBER

Through every phase of the journey, businesses must

- Protect employees and customers
- Securely preserve vital business operations and services
- Adapt to a new reality, new ways of doing business, and new ways of engaging with customers and empowering employees
- Manage through periods of economic uncertainty

- Identify optimal investments that maximize the impact of your workforce while leveraging technology for growth and differentiation
- Accelerate long-term strategies that make your organization stronger, more agile, and better prepared for the future

Investing in a long-term distributed workforce strategy that makes your organization more resilient, more flexible, and better prepared to drive recovery and growth in the face of future challenges will have far-reaching implications beyond the current pandemic. Businesses will need to take advantage of shifting mindsets to meet work-from-home expectations today and in the future. A digital workspace environment that seamlessly supports a distributed workforce can be the foundation for a more resilient and competitive organization, based on greater flexibility and more productive ways of working.

IN THIS CHAPTER

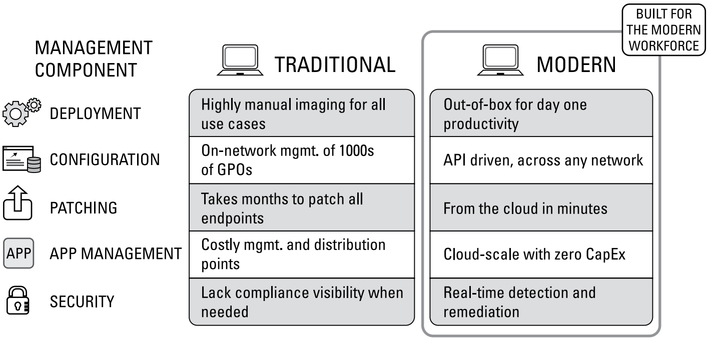
- **Enabling modern management**
- **Focusing on prevention with endpoint security**
- **Delivering virtual applications and desktops**
- **Putting employee experience first**
- **Supporting multi-modal end-user computing with IAM**
- **Protecting cloud applications and data**
- **Connecting the distributed workforce with SD-WAN and SASE**

Chapter 2
Understanding the Tech Needs of the Distributed Workforce

In this chapter, I explain which technologies you need to support the distributed workforce including unified endpoint management (UEM), endpoint security, virtual app and desktop delivery, experience management, identity and access management (IAM), cloud app security, and software-defined wide area networks (SD-WANs) and cloud gateways.

Unified Endpoint Management

Ensuring productivity, security, and an engaging user experience for the modern distributed workforce requires technologies that enable easy and intuitive onboarding, training, and remote support for end users. UEM opens the door for organizations to transform desktop, mobile device, and application management with a new cloud-based management framework. UEM represents a shift in the desktop management process to support the delivery of policies, updates, patches, and applications from the cloud. UEM further enables cloud-based delivery of security policies, configurations, and apps to support remote and mobile users and devices anywhere. These capabilities are critical for implementing a Zero Trust security model (discussed in Chapter 4) across disparate devices in a distributed workforce environment so that security teams can get a complete picture of the expanded operating environment. Figure 2-1 compares traditional and management and UEM across five core areas of PC management.



BUILT FOR THE MODERN WORKFORCE

MANAGEMENT COMPONENT	TRADITIONAL	MODERN
DEPLOYMENT	Highly manual imaging for all use cases	Out-of-box for day one productivity
CONFIGURATION	On-network mgmt. of 1000s of GPOs	API driven, across any network
PATCHING	Takes months to patch all endpoints	From the cloud in minutes
APP MANAGEMENT	Costly mgmt. and distribution points	Cloud-scale with zero CapEx
SECURITY	Lack compliance visibility when needed	Real-time detection and remediation

FIGURE 2-1: UEM is key to the distributed workforce and IT transformation.

UEM combines the efficiency of mobile device management (MDM) and the full breadth of capabilities of desktop management to enable UEM via a digital workspace platform. The digital workspace collapses the silos between desktop management, MDM, and application management to enable all devices and applications to be managed holistically. It allows you to take a consistent approach to managing and securing all your user endpoints and all the apps and data associated with them in a single, unified management platform.

Endpoint Security

Traditional approaches to endpoint security are typically based on reactive tools, such as antivirus and malware detection. Virtual private networks (VPNs), encryption, and group policies provide additional layers of protection for users and devices. Under modern management, the security focus can shift to prevention. The ability to proactively prevent, detect, remediate, and react to new and existing threats is faster because the device syncs with the latest threat databases to prevent attacks in real time. To achieve this, security teams need to embrace a holistic security approach that links to all the components in use — device, operating system, network, user, application, and context — at any given time.

From a process perspective, endpoint security decisions move from selecting a tool for deployment to a Zero Trust posture. Zero Trust assumes the following:

- A cohesive security strategy governs the totality of environmental use instead of relying on piecemeal agent-based approaches.
- Every device is unsecured rather than trusted.
- Access and availability are governed by user permissions, profiles, and entitlements, not device type or ownership.
- Context-aware access — device location, time, security posture — is a joint process between IT security and IT administrators.
- Granular levels of security controls are applied via context and per-app VPNs.
- Device validation and identification are performed independent of ownership.

THE ZERO TRUST SECURITY MODEL

TECHNICAL STUFF

The Zero Trust security model was originally proposed by Forrester Research as an alternative to perimeter-centric security models that have become less effective in the age of cloud, mobile, and remote computing. The Zero Trust model mandates a data- and identity-centric model based on the concept of "never trust, always verify."

TIP

Implementing Zero Trust security requires that security administrators rethink how security rules and policies are defined, established, deployed, and managed. Security teams must be closely aligned with IT administrators who manage devices (including Internet of Things, or IoT, devices), users, applications, and networks.

Virtual App and Desktop Delivery

Distributed workforce technologies — often characterized by diverse and untrusted devices, multiple operating systems, and consumer-oriented applications — are creating a chaotic end-user computing environment for organizations that have traditionally maintained a highly standardized and controlled digital workplace. To meet the current and future end-user computing needs of the distributed workforce, organizations must change how they deliver Windows applications. This means rethinking Windows application delivery, management, provisioning, and enablement.

Running Windows applications solely on Windows PCs is now a limiting factor for many organizations. Tying applications to the OS on a physical device can ensure the best performance and allows the tightest control of integration with other local functions, but these are diminishing requirements: Few end-user computing applications are now performance-constrained by hardware, and the management plane of integration with other functions has shifted from devices to the cloud. With these requirements disappearing, other aspects of distributed computing have become more visible: inherent complexity in security, multiple points of failure, and reactive management.

Modern web and cloud delivery models avoid these distributed issues by pushing application execution and integration back to the data center (cloud), where applications and data are centrally managed and maintained. Dependencies on device and OS type are removed from the management equation.

By removing the desktop OS and applications from the endpoint, disaggregating them, and delivering them to the end-user device from the data center, application and desktop virtualization offer the promise of improved security, management, operations, and cost. With this flexibility, IT organizations can use a modern approach to centrally deliver applications that depend on data (such as system of record applications), while running other applications locally (such as individual productivity applications) to best meet the needs of individual workstyles.

Comparing VDI and RDS approaches

Two forms of virtual application and desktop delivery are commonly used today: virtual desktop infrastructure (VDI) and Remote Desktop Services (RDS). The most common approach to centralizing a full desktop environment is VDI. VDI leverages server virtualization so that instances of client operating systems (such as Windows 10) can be launched and run in their own virtual machines and then remotely delivered to users (see Figure 2-2).

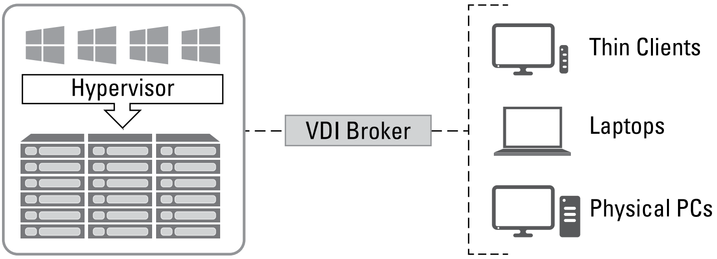


FIGURE 2-2: VDI architecture.

With RDS, applications are installed and configured on a Windows Server OS (instead of a client OS) in a multiuser environment, so that multiple users can simultaneously access the application remotely. Like VDI, RDS is a remote solution that alleviates the need for local execution of applications on an end-user device.

Both VDI and RDS are used by organizations for application delivery. VDI is commonly used for those users that require the full fidelity of Windows, so that users can install, configure, and use their desktop just as they would a normal PC. RDS is common for applications that are targeted to many simultaneous users (see Figure 2-3). It is not uncommon for organizations to use both VDI and RDS, depending on user needs and application requirements.

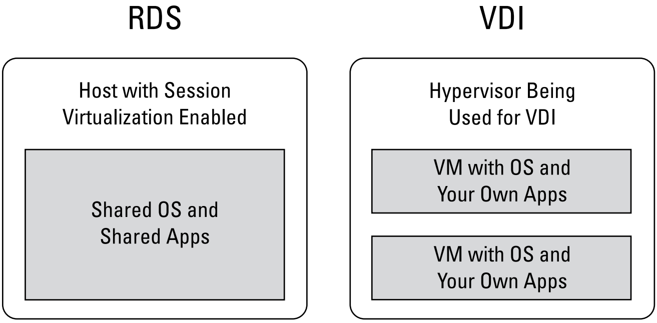

RDS
VDI
Host with Session Virtualization Enabled
Shared OS and Shared Apps
Hypervisor Being Used for VDI
VM with OS and Your Own Apps
VM with OS and Your Own Apps

FIGURE 2-3: RDS and VDI comparison.

Extending on-premises resources to the cloud

A clear advantage of remote delivery is that it enables IT organizations to centralize their applications in a corporate data center or manage them as cloud-based services. As a result, IT staff can more efficiently provision new applications or environments, simplify and standardize a broad range of desktop management tasks, and provide more robust endpoint security. Virtual desktops and applications also provide IT organizations with greater consistency across system settings and policies, meaning they can rationalize and streamline the targets of their management processes.

Virtualization has enabled IT administrators to deliver a more consistent and seamless desktop application experience to the rapidly expanding population of employees who use multiple devices for their work. Users can access the same desktop instance or application from each new session, as well as securely access corporate data and applications anytime and anywhere, through a single set of policies and log-in credentials. All of this takes place regardless of the device type, OS, or location of the user.

Looking at various delivery models

Despite the widespread use of smartphones, mobile apps, and software-as-a-service (SaaS) applications, native Windows applications are not going away anytime soon. In many cases, these applications were developed or modified in-house for specific requirements and perform business-critical functions. As organizations extend their digital workspace to the distributed workforce, they need to take these applications with them, which means they still need to provision and manage Windows-based applications as part of their overall end-user computing strategy.

Windows 10 enables organizations to simplify and improve how they manage and deploy their Windows-based applications, which can now be made available and delivered to users in a number of ways, including the following:

- **Deploying VDI:** VDI offers users the full fidelity of traditional Windows PCs, with the same look, feel, execution, and customization as running applications natively on a PC. VDI runs on servers (rather than PCs), so the operation and administration are centralized and standardized, meaning they can be simplified and optimized. IT administrators can quickly and easily refresh, update, reboot, secure, and manage Windows and Windows applications.
- **Publishing Windows applications via RDS:** RDS is used by organizations wanting to make applications (but not the underlying Windows desktop) available to users. Like VDI, the benefits of RDS include faster rollouts for updates and the ability to access corporate apps and desktops remotely from any device.
- **Applying modern management techniques using enterprise mobility management (EMM):** EMM offers organizations deploying Windows 10 a more efficient way to manage applications and Windows as compared to PC life-cycle management (PCLM). EMM offers organizations a way to provision, manage, and secure end-user computing devices.
- **Subscribing to any of the above via a cloud-based service:** Cloud-based services for desktops and published applications also offer high degrees of flexibility with the delivery and management of Windows applications. This approach frees the customer from the time, expense, and infrastructure necessary for deploying Windows (via VDI or RDS) internally.

Identity and Access Management

Your users access applications today in far more complex ways than ever before. They access enterprise and productivity applications through a variety of mobile devices, laptops, and desktop PCs. These applications may be installed on the devices themselves or in the data center, in the cloud, or perhaps in multiple locations. Finally, not all these applications are necessarily managed by IT; an increasing number of applications are installed and maintained by the users themselves or managed by line of business or non-IT operational teams — particularly as the distributed workforce, at least in the early stages of the global pandemic, found itself increasingly isolated and self-reliant.

To support this environment, most organizations have embraced a multimodal style of end-user computing that enables any user to potentially work with any application, any devices, and any infrastructure. Although this approach is beneficial in terms of productivity and user engagement, it introduces other challenges, including gaps in employee experience, complexity in access procedures, and exposure to new risks and issues.

WARNING

Threats associated with malware, phishing, credential stealing, digital hijacking, information and identity theft, and data loss have increased significantly due to "any-to-any" multimodal end-user computing.

Identity and access management (IAM) technology is a key means of supporting this "any-to-any" approach. IAM simplifies the employee experience and enables users to access the applications they need in a way that is secure, reliable, and easy to use. IAM is the system that an organization uses to manage access to its applications and content.

REMEMBER

IAM includes the policies and technologies that enable an organization to manage the digital identity and access permissions of its users. IAM provides the following functions:

- **Identity management:** The creation, management, and deletion of identities associated with users
- **User credentials:** User ID and password or credentialed access to applications, devices, and services

- **Unified access:** A system that allows a user to authenticate once to a range of applications and services without necessarily knowing his login credentials for each application or service, similar to single sign-on (SSO)

TIP

IAM offers added value in the following areas:

- **Integration:** IAM systems are typically targeted at certain types of workloads, infrastructures, or applications. IAM integration brokers to multiple unique IAM systems, so that all applications, infrastructures, and devices can be equally serviced.
- **Conditional access:** Conditional access requires that certain criteria be met before granting access to applications and data.
- **Ease of use:** IAM helps consolidate access by streamlining where and how applications are managed so that the burden of managing multiple IDs and passwords is greatly simplified (or completely eliminated) for the user.
- **Enhanced policy management:** Simplified access management introduces policy enhancements such as the ability to apply policy-based rules to specific scenarios.

Cloud App Security

Access to business-critical SaaS applications (and their associated data) for the distributed workforce must be protected. A cloud access security broker (CASB) provides IT organizations with visibility and control of SaaS application usage by functioning as a cloud-based policy enforcement point. CASB functionality is increasingly being delivered through a secure access service edge (SASE; pronounced *sassy*) solution, discussed later in this chapter and in Chapter 4.

SD-WAN and Cloud Gateway

As the workforce become more distributed, mobile, and global, IT infrastructures inevitably become more complex. With hundreds or even thousands of remote, branch, and home-office locations supporting a distributed workforce, this complexity can cause IT to lose visibility and control. To regain visibility, flexibility, and control, IT organizations need to take a fresh approach to architecting and managing their networks and infrastructures. Businesses need to adopt a cloud-delivered, software-defined model for WAN and branch locations that extends from the data center and the cloud, across the WAN, and to the edge.

Enterprises have traditionally used dedicated, private wide-area networks (WANs) to connect headquarters and branch offices, and to access applications and data in data centers. However, with the shift to a highly distributed workforce, organizations must take a closer look at more agile and flexible solutions, now more than ever, to connect their users at the edge — whether in branch offices or home offices.

Deploying a modern, flexible network and access strategy that's focused on users, identity, and consistent access is key. An integrated SD-WAN and cloud gateway solution enables organizations to deliver intrinsically secure, Zero Trust access as a service for remote and mobile workers. This solution:

- Provides consistent, reliable access and a seamless user experience
- Quickly scales to accommodate growing numbers of users
- Supports multi-region, per-application VPN service for Android, iOS, macOS, and Windows clients
- Leverages a global network of service nodes for reliable delivery

TECHNICAL STUFF

SD-WAN provides a software abstraction to create a network overlay and decouple network software services from the underlying hardware. SD-WAN separates functionality into a control plane and a data plane. The *control plane* is the part of the network that is responsible for signaling traffic and making packet routing decisions. It also includes device system configuration and management. The *data plane* is part of the network that carries application and user data.

SHIFTING TO SASE

SASE brings together network and cloud security services to provide flexibility, agility, and scale. SASE offers a much simpler secure connectivity model for a distributed workforce, bringing security functions wherever they're needed, as with other cloud services.

SASE providers (often, companies that already offer SD-WAN) build a national or global fabric of points-of-presence (PoPs) and peering relationships with cloud providers. These PoPs serve as an onramp to SaaS applications and other cloud services. When users (or devices, or applications) connect, either in a branch or via remote access, each PoP can apply the full suite of enterprise security functions, including the following:

- Zero Trust network access (ZTNA)
- Secure web gateways
- CASB solutions to apply security policy to cloud applications and data
- Cloud-based firewalls
- Identity services to establish the user's context and security posture

Just as important, SASE delivers many of these cloud-based security functions "as a service." Businesses can apply the full suite of state-of-the-art security protections anywhere, without having to maintain hundreds (or thousands) of point products for a distributed workforce.

Experience Management

Building a strong design culture around the employee experience is critical to meet the demands of the business, as well as the ability to secure corporate data. If lines of business, teams, and individuals believe that IT gets in the way and slows them down, employees will avoid adopting the tools and services designed to protect them.

IT must design and deliver an engaging employee experience to improve productivity and security in the distributed workforce. This experience must account for the different devices and form factors employees use throughout the day and the locations from which they need to work. It must also provide a level of flexibility and choice that will keep up with the demands of employees and departments.

Artificial intelligence operations (AIOps) provides IT with the ability to remotely troubleshoot end user–perceived application problems that may be caused by a number of other issues, such as Wi-Fi quality, virtual private network (VPN) connectivity, broadband Internet issues, and more. To get a complete picture of the user experience, IT must understand any issues with infrastructure and services that provide connectivity between users and their applications.

TIP

According to Forrester's Employee Experience Index, "employees are more likely to be engaged when they believe their IT departments are focusing on helping them be productive (70 percent)."

IN THIS CHAPTER

- **Getting started right on day one**
- **Providing seamless access to applications via an app catalog**
- **Ensuring reliable connectivity**
- **Giving your employees flexible device choices**
- **Empowering employees with self-service capabilities**
- **Moving toward passwordless authentication**

Chapter 3
Delivering Exceptional User Experiences

In this chapter, I look at several key aspects of the employee experience, including onboarding new employees, providing seamless access to the applications your employees need, addressing connectivity challenges, supporting your employees' preferred devices, helping your employees help themselves, and reducing the burden of managing multiple account passwords.

Onboarding New Employees Remotely

Onboarding new employees can be extremely time-consuming, particularly if an employee has multiple devices, requires different type of applications, and works in a home office or other remote location. Ensuring that new employees have access to the devices, applications, and other tools they need to be productive on day one is crucial to the new employee experience. A poor experience creates an indelible first impression for new employees about the company and its IT department.

This experience is no less important for the distributed workforce. However, it isn't practical, or even desirable, to send IT staff to your new employees' home offices to set up their digital workspaces. Instead, work-from-home employees in the distributed workforce must be more self-sufficient.

To make the onboarding experience a positive one — even for your non-tech-savvy new employees — you need to enable a touchless and seamless remote onboarding experience. Unified endpoint management (UEM) enables your IT organization to introduce rapid, automatic, self-service, and on-demand capabilities for first-time setup. Instead of going through an expensive onboarding process, you can do a simpler and cheaper provisioning that minimizes a lot of pre-employee-handover steps. You can push out all the necessary configurations and software via a secure connection to any Wi-Fi network, wherever the employee happens to be. We're talking about zero-touch setup.

It's all pretty simple: When a device first registers with IT, the rules and roles associated with the user's login trigger the UEM system to launch a seamless onboarding process that automatically installs and configures all appropriate corporate resources and applications.

A full-bodied digital workspace platform enables zero-touch setup for a wide range of devices used in the workplace — whether in the office or at home — including Windows and Mac laptops and Android and iOS mobile devices.

REMEMBER

Onboarding is a critical first milestone in every employee's journey. Provide an engagement platform that supports employees with an exceptional experience from the day they sign their offer letter to their first day of employment and beyond.

Providing Seamless Access to Apps

Software distribution is an ever-growing challenge for your IT organization. Every year, you need to distribute *more* software and *more* updates to *more* endpoints and *more* types of devices. And you need to do it all quickly to keep operating systems (OSs) and apps up to date. A UEM solution helps you streamline the process of getting the right software on your end-user devices.

REMEMBER

Providing easy access to applications and data is one of the top issues identified by employees as critical to a positive experience (see Chapter 5).

With the modern management capabilities of a robust digital workspace platform, some software may be installed as part of the onboarding process (pushing upon setup), some may be later pushed to users, and some may be made available on demand via a unified app catalog (pulling). Modern management enables you to deploy public, internal, or bulk-purchased apps to devices automatically or to an enterprise app catalog for on-demand install.

Apps that are pushed to devices as part of the onboarding process typically include those that everyone in the organization needs. Other apps pushed out in the onboarding process include those that are tied to a particular user profile, such as apps used by employees in engineering or finance.

Apps that only certain users may need or want can be made available via an enterprise app catalog. The app catalog gives your users a one-stop shop to view and download applications. Access to individual apps is based on settings you establish in the UEM console.

TIP

When you select desired apps from public app stores for distribution, you simply configure the assignment to your corporate devices smart group and then select your deployment option to automatically push the app to the enrolled devices or your app catalog.

Addressing Connectivity Challenges

With the proliferation of cloud- and web-based apps, Internet connectivity has become more critical than ever to the overall user experience, whether in the office or working from home. Enterprises generally can't do much about their employees' home Internet service, but they can ensure connectivity back to the corporate data center and cloud-based resources is as seamless as possible by optimizing application delivery (discussed in Chapter 2) and providing seamless security that does not negatively impact network performance.

For example, virtual private networks (VPNs) often require users to manually start a VPN client to access corporate resources and can introduce significant performance bottlenecks due to encryption and VPN gateway congestion, particularly if all traffic (including Internet access) is backhauled through the VPN connection. However, enabling *split tunneling* — routing corporate traffic over the VPN connection and all other traffic directly over the Internet — is often complex and can introduce new security risks.

Software-defined wide-area network (SD-WAN) devices and, increasingly, cloud-delivered secure access service edge (SASE) solutions, enable a more seamless and optimized networking and security experience at the edge.

TIP

Find out more about SD-WAN and SASE in Chapters 2 and 4.

Supporting Flexible User Choices

Whether corporate-owned or bring your own device (BYOD), organizations need to support a growing number of devices and OS platforms and versions. IT teams need to scale support and operations to ensure device health, compliance, and security that extends beyond the corporate office to the home office.

Supporting your employees' preferred devices is increasingly important for the distributed workforce in which organizations have less visibility and control of their employees' personal devices being used in their home offices. Particularly at the start of the global pandemic, many businesses found it necessary to allow their employees to use different personal devices including personally owned desktops or laptops, monitors, printers, smartphones, and other home office equipment, to perform work and stay productive at home. Even as businesses are now able to deploy more standardized, corporate-owned devices for their employees' home office, user choice is still an extremely important factor to consider in the overall employee experience.

TIP

Keys to supporting flexible user choices and delivering an exceptional employee experience include the following:

- **Supporting BYOD and corporate devices on a single platform:** Provide consistent experiences across mobile and desktop for access to corporate resources, no matter if employees are using personal or corporate devices in the office or at home.
- **Encouraging seamless employee productivity:** Eliminate back and forth between multiple apps by providing personalized workflows for employees alongside other corporate resources that make it easy to be productive from your employees' preferred devices.

Enabling Self-Service Support

The distributed workforce must be more self-reliant as employees working from home are more physically isolated from their peers. In many cases, millennial employees who are generally more tech savvy than others, prefer a "do-it-yourself" approach with relatively limited human interaction. Organizations can enable robust self-service support capabilities including the following:

- **A virtual assistant** to save employees time by making it easy to find information such as common office procedures (for example, how to enroll in your company's retirement plan or add dependents to receive healthcare benefits) and IT support issues (for example, ordering a new device or requesting access to an application).
- **Remote support capabilities** that allow help-desk administrators to remotely access system logs and configuration files on user devices to quickly diagnose and fix problems.
- **Self-service password resets** so that employees can reset their own passwords without contacting the help desk, for example, via an email link or after answering security questions and receiving a one-time passcode.

TIP

Minimize downtime for employees by providing access to frequently asked questions (FAQs) and a chatbot for discovery of corporate resources. Proactively remediate issues before they occur with digital employee experience management.

Reducing Password Proliferation with Seamless Multifactor Authentication

Enterprises can strengthen data protection by verifying user identity using multiple factors. To eliminate the increasingly complex task of having to set individual policies for a constantly growing number of applications, devices, and cloud services, enterprises should be able to use the end user's identity to establish security parameters while making it easy to access apps.

From the user's perspective, reducing the burden of managing multiple accounts and passwords is a critical component of employee experience. From an IT support perspective, you reduce the burden of unlocking user accounts and resetting forgotten passwords. By implementing technologies and capabilities such as passwordless authentication, single sign-on (SSO), multifactor authentication (MFA), and conditional access, organizations not only reduce user friction but also improve their IT service management by eliminating thousands of tickets for password resets and improve their overall security posture with more robust identity and access management (IAM) controls than simple username and password authentication mechanisms.

Passwordless authentication leverages biometrics and other factors to enable more seamless and secure user authentication. For example, in Windows 10, users can authenticate with a fingerprint or face scan using Windows Hello for Business. Similar functionality exists in Android and iOS devices (for example, FaceID and TouchID). By eliminating the need for passwords, organizations reduce the risk associated with users sharing or reusing passwords.

One-touch SSO allows users to access desktop, mobile, and cloud applications, avoiding the time and hassle of multiple log ins. Through SSO, the identity of a user can be verified for many apps at once, in effect, providing a single key for a single digital workspace door to open access to a variety of web, mobile, software as a service (SaaS), and legacy applications on the endpoint of choice from an app catalog.

TIP

Unify your app catalog with SSO to eliminate time spent searching for apps and remembering passwords by providing a single launch experience for all your apps.

With MFA, the identity of users and system components can be verified using multiple factors (not just simple passwords) commensurate with the risk of the requested access or function. MFA can be enabled with a hardware or software token or, more commonly, with a one-time passcode sent via text message to a smartphone. As MFA becomes increasingly common, for example, to access online bank accounts or your Amazon Prime account, familiarity with MFA techniques helps to improve user acceptance and adoption.

Conditional access allows organizations to set contextual policies based on the resources that a user is requesting access to, the device (or browser) that is being used, and other factors, such as location, time, or impossible travel (a user tries to log in from an IP address in New York and five minutes later tries to log in from an IP address in London).

REMEMBER

Password authentication is inherently vulnerable to compromise given the level of effort required to create and manage complex passwords. Perhaps ironically, implementing a combination of more robust authentication mechanisms including passwordless authentication, SSO, MFA, and conditional access provides a more seamless and secure employee experience.

IN THIS CHAPTER

- Defining Zero Trust security
- Establishing device trust
- Verifying user identity and access
- Keeping your sessions secure
- Protecting applications
- Preventing data theft and loss

Chapter 4
Deploying Zero Trust Security

In this chapter, I cover Zero Trust security and the five pillars of Zero Trust: device, user, session, application, and data trust.

What Is Zero Trust Security?

The Zero Trust security model is based on the notion of "never trust, always verify" and has become increasingly important as tradition network security perimeters have all but disappeared — particularly for the modern distributed workforce. Zero Trust is a conditional access control model that requires verification of trust before allowing application access and the access that is granted is based on the principle of least privilege.

REMEMBER

The principle of least privilege means granting only the required access to applications for the user to complete her job, and no more.

By never trusting, and always verifying, the Zero Trust approach protects your data and applications not only at the start of a session, but also with continuous verification of users, endpoints, and networks throughout an application session. Employees in the modern distributed workforce are accessing applications from practically anywhere — in the office, at home, or in a coffee shop. Zero Trust means not inherently trusting your users, devices, or applications simply because they're "on the corporate network." Zero Trust enables a single application access policy regardless of where your users are accessing your applications from.

A Zero Trust architecture requires the following:

- **Continuous verification of endpoint compliance:** For access to be granted, endpoints must be continuously verified to be compliant with your organization's security policies.
- **Conditional access control to all applications:** For a user to gain access to applications, they must prove their identity.
- **Reduction of the attack surface:** To protect your organization's applications and data, each user must be granted only the least-privilege access to get his work done, and nothing more.

Zero Trust validates the posture of endpoint devices, the identity of users, and the security of the connections to the applications prior to allowing access. These attributes are continually revalidated to ensure that the access is still acceptable. This is never trust, always verify in action.

With a Zero Trust architecture, users access applications and data from a digital workspace as follows (see Figure 4-1):

- **Users:** A user requests access to applications and data.
- **Endpoints:** A unified endpoint management (UEM) system looks at the endpoint device — such as a desktop PC, mobile device, or Internet of Things (IoT) device — and determines if that device is compliant (trusted). The ownership and management scope of the device are also considered. If the device is trusted, user identity is checked.
- **Network:** The communication method must be valid, and encryption must be in place. To reduce the attack surface further, each application can have a single secure tunnel into the data center.

- **Applications and data:** Access to applications and data must be role-based and include policies for data loss prevention (DLP). DLP includes restrictions that prevent a user from copying data to other applications. With Zero Trust, the applications and data are checked continuously. Also, the application server must be protected from remote access via the public Internet.

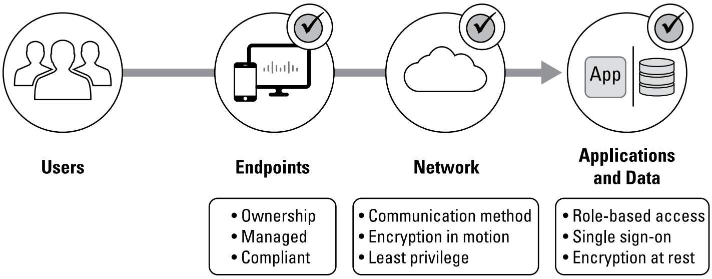


FIGURE 4-1: Zero Trust checkpoints for user access to applications and data in a digital workplace.

The Zero Trust architecture consists of five pillars — device trust, user trust, network trust, application trust, and data trust. You must establish trust in each pillar to make decisions to grant or deny access (see Figure 4-2).

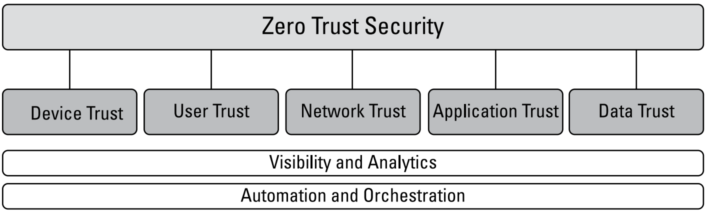


FIGURE 4-2: The five pillars of Zero Trust architecture.

Device Trust

With many organizations having to shift to a distributed workforce model literally overnight at the start of the global pandemic, millions of laptops and other devices are currently being managed using tools that were designed for on-premises environments — or not at all. In many cases, end-user devices are not being properly or reliably updated and patched.

To enable employees to work productively from home, many organizations may have given their employees privileged access to allow them to install applications themselves, connect to personal printers, and perform other device management tasks that are normally performed by on-site IT support staff.

Finally, many organizations may have allowed their employees to use their home desktop PCs rather than sending corporate-owned desktop PCs home with their employees. These personally owned devices may not be running the most current operating systems and updates, may not be running anti-malware protection, and may be shared by multiple users within the home connected over an unsecured Wi-Fi network.

This greatly expanded attack surface makes device trust more critical than ever to your overall security posture. To deploy Zero Trust security for your devices, you need to address the following device trust parameters:

- **Device management:** Device management provides control over devices including what software is installed, which versions, and under what conditions a given application may be used. To achieve these control objectives, device management capabilities include determining security policies such as how to identify the device, often using multiple authentication and authorization methods. To address changing circumstances, device management must also include the capability to continuously monitor the state of the device and its attributes so that at any time, security policies can be updated, applied, and enforced.
- **Device inventory:** Organizations must catalog all hardware devices to verify that each device is a known secure endpoint. You can then use inventory-based access controls and allow access only from devices registered to authenticated users.
- **Device compliance:** Compliance checks must be performed by collecting information from devices at both scheduled and unscheduled times. Noncompliant devices may be denied access to certain company resources. You must also have the capability to automatically respond and remediate when noncompliant devices are discovered, to quickly bring the device into compliance.

- **Device authentication:** Digital certificates provide optimal protection for authenticating your corporate devices. Certificates offer a level of stability, security, and sophistication well beyond simple passwords. Certificate management is a key capability to ensure security throughout the life cycle of a device.

You need to know your devices before you can trust them. This means having a device inventory that specifies which devices are owned and, therefore, controlled by your company. You must have a solution that effectively monitors, manages, and controls these devices.

TIP

To support bring your own device (BYOD) policies, you may need to relax your trust level on personal devices. End users aren't often eager to let their personal devices be managed by their employer.

To secure a strong level of trust in end users' devices, you may need to know, for example, whether the local disk is encrypted properly, what the anti-malware protection status is, what versions of the operating system (OS) and applications are installed, and more. Knowing all these properties increases your overall trust in the device.

Included in this pillar is the capability for automatic remediation. For example, if a device doesn't have the correct version of the OS or an application, the system should be able to remediate by pushing out the correct version or by guiding the user through the upgrade process.

TIP

Solutions such as VMware Workspace ONE UEM, VMware Unified Access Gateway, and VMware Carbon Black help organizations address Zero Trust security for devices.

User Trust

To ensure a high level of trust in the user, you must use modern and strong authentication methods. Relying on passwords alone is not sufficient. You can chain many authentication methods together, but you'll need to weigh the security benefits against any possible decline in user experience. The goal with Zero Trust is to enhance both security *and* user experience.

Certificates are ideal as the foundation of your user authentication method. With certificate-based authentication in place, you can add things like multifactor authentication (MFA) for critical systems. Today, most MFA solutions are user friendly and add minimal inconvenience to the user experience.

User trust requires a strong conditional access engine that can help make authentication and authorization decisions using dynamic and contextual data. Conditional access rules can help determine whether and when to enforce stronger authentication. By aggregating device, app, and user behavior from multiple internal and external sources and leveraging machine learning models, an intelligent conditional access engine can calculate a user risk score and enable conditional access based on device context, login risk, and user behavior (see Figure 4-3).

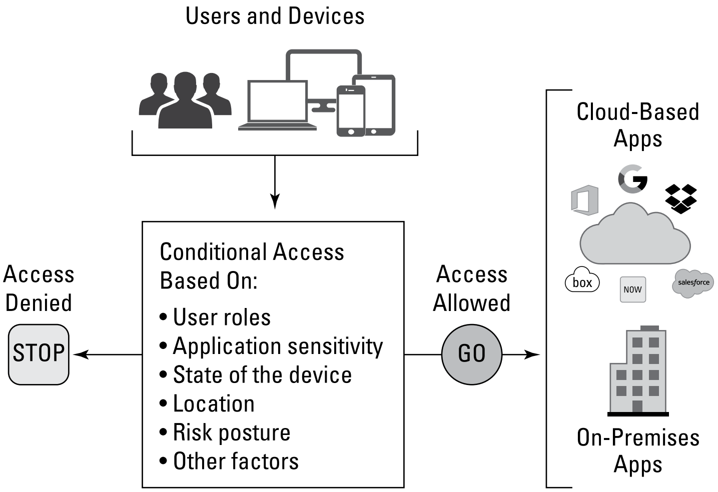


FIGURE 4-3: Conditional access.

By combining policy enforcement with access and device management, your IT team can restrict user permissions to data, applications, or devices. The same technologies can also be used to apply conditional access to mobile apps and ensure that only compliant applications can access internal systems.

User trust parameters in a Zero Trust architecture include the following:

- **Passwordless authentication:** Passwordless authentication determines the identity of a user without requiring the user to enter a password. Passwordless authentication provides an improved user experience (because users don't need to keep track of passwords) and better security (because users don't end up sharing or reusing passwords). Some common types of passwordless authentication include the following:
  - Biometrics, such as fingerprints or facial scans
  - Hardware or software security tokens
  - One-time codes or links sent to an email address or a mobile phone number
  - Piggybacking on a service that has already authenticated the user
  - Certificate-based authentication
- **Multifactor authentication (MFA):** MFA involves requiring at least two pieces of evidence that prove a user's identity. These pieces of evidence are usually some combination of the following three factor types:
  - Something the user knows, such as a password or the answer to a security question
  - Something the user has, such as a hardware or software security token or a certificate
  - Something the user is, which may mean a scan of the user's fingerprint, iris, or face
- **Conditional access:** With conditional access, you chain multiple authentication methods to build a strong trust level in your user based on contextual information about the user, device, location, and other factors and assigning a dynamic risk score.

TECHNICAL STUFF

Passwordless authentication uses strong authentication factors (for example, fingerprint or facial recognition, such as Windows Hello for Business and FaceID/TouchID for iOS), MFA (for example, a one-time passcode sent to a mobile device via text message), conditional access, and dynamic risk scoring to enhance security while reducing user friction.

Network Trust

Network trust ensures the security of the network connection between your user devices and applications, data, and other resources.

Traditional enterprise wide-area network (WAN) architectures typically rely on private network connections between headquarters, branch, and data center locations. Mobile and remote connections were typically secured via a virtual private network (VPN) between the endpoint device and the enterprise network. However, many enterprises are finding that their existing network and security infrastructure is unable to handle the VPN load of a largely distributed workforce. According to one 2019 survey, remote work has grown by 400 percent over the past decade — and that was before COVID-19 forced millions to spend months working from home. Backhauling Internet traffic from home-office PCs to a corporate headend over a VPN connection consumes bandwidth and introduces significant performance issues.

WARNING

Enabling *split tunneling* on a VPN client, in which only corporate traffic is sent over the VPN tunnel while all other traffic directly traverses the remote workers' Internet connection, is one solution to alleviate VPN load issues — but it introduces additional security risks to the endpoint as well as the corporate network.

Software-defined wide area network (SD-WAN) solutions solve many of the performance and efficiency problems associated with antiquated WAN architectures, and most include a built-in stateful firewall. But remote workers and cloud-based application traffic just weren't designed to provide the full-featured security stack available in the enterprise data center — until now.

The new secure access service edge (SASE) enables organizations to deliver simplicity, scalability, flexibility, low latency, and pervasive security to a distributed workforce. SASE integrates the following core functionality into a cloud-native solution:

- Secure access
- Cloud web security
- SD-WAN gateway
- Cloud firewall

SASE can be delivered to branch edges, mobile and remote users, campuses, and IoT devices (see Figure 4-4).

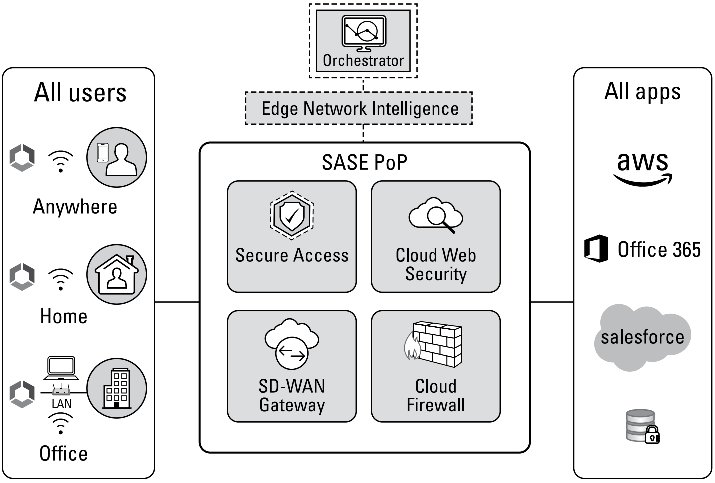


FIGURE 4-4: A cloud-native SASE architecture.

Transport/session trust parameters in a Zero Trust architecture include the following:

- **Micro-segmentation:** Micro-segmentation enables organizations to logically divide the data center into distinct security segments down to the individual workload level (if desired or necessary), and then define security controls and deliver services for each unique segment. This restricts an attacker's ability to move laterally in the data center, even after the perimeter has been breached. With remote employees accessing resources in a corporate data center over potentially thousands of individual network connections, micro-segmentation takes on renewed importance for overall data center security in the modern distributed workforce.
- **Least-privilege access:** Least-privilege access means giving users only as much access as they need, which minimizes each user's exposure to sensitive parts of the network. Least-privilege access provides granular role-based access to sensitive resources. For example, users who belong to the HR department would get access to only the HR applications and only the servers and data required for HR job functions.

Non-HR employees wouldn't have access (or would have only limited access) to these applications, servers, and data.

- **Transport encryption:** End-to-end certificate-based encryption is used to avoid data theft during transit. When every packet is encrypted, even within the same data center, you don't need to take into consideration which packets traverse the Internet and which packets do not.
- **Session protection:** A *session* is a temporary connection between two devices or between a user and a computer during which information is communicated and exchanged. To avoid having a session hijacked:
  - You must have an effective authentication system.
  - Communication must be encrypted, so that even after the user is authenticated, no one will be able to steal the session ID used to pass subsequent traffic back and forth.
  - An expiration period must be defined, limiting the amount of time malicious actors can make their hijack attempts.

TIP

Solutions such as VMware Unified Access Gateway, VMware Horizon, VMware NSX SD-WAN, and VMware Secure Access help organizations address network trust.

Application Trust

Ideally, all applications would be designed from the ground up based on the principles of Zero Trust. However, this occurrence is unfortunately very rare today. Application and desktop virtualization enable organizations to rapidly deploy full-featured, personalized digital workspaces leveraging just-in-time delivery. User authentication is modernized and simplified, allowing single sign-on (SSO) across all desktop and application services, with contextual, granular, role-based policies that connect user, device, and location information.

For traditional applications that are not designed for Zero Trust, organizations need to add protection in the form of isolation through application virtualization.

Application trust parameters include the following:

- **SSO:** A user authenticates to a system once and can then access many related but separate systems without having to re-authenticate for the duration of the session. SSO has many benefits, including improving the user experience, reducing help-desk requests, and centralizing directory management.
- **Application access from any device:** Enabling employees to access any application, including traditional Windows applications, securely and seamlessly from any device is key to creating a digital workspace for the distributed workforce and enforcing Zero Trust. With flexibility of work tools and freedom of access from anywhere at any time, digitally empowered employees become more engaged and productive. They can collaborate with team members more easily and make faster decisions.

Data Trust

The ultimate target for attackers is your organization's sensitive data, and the ultimate goal of your security efforts is to protect this data, including the confidentiality, integrity, and availability of the data.

Sensitive data must be identified and properly classified, and then protected at rest with encryption and appropriate access controls. Data integrity must also be protected through appropriate backups and other technologies to prevent unauthorized modification or destruction (for example, due to a malware infection or ransomware attack).

Data trust parameters include the following:

- **Protecting data at rest:** *Data at rest* is data that is being stored on a persistent medium such as a hard drive, laptop, flash drive, or some other storage device. With the Zero Trust model, software-defined perimeters are increasingly being used — along with anti-malware protection, encryption, and firewalls — to create a protective casing around data access.

- **Integrity:** Regular data backups remain an important component of data protection, particularly given the explosive growth of ransomware attacks in recent years.
- **Data loss prevention (DLP):** DLP helps to ensure that sensitive data doesn't leave the organization whether accidentally, intentionally, or maliciously. DLP tools typically prevent sensitive data — such as financial information, Social Security numbers (SSNs), and other personally identifiable information (PII) — from being compromised or stolen via unauthorized file transfers, emails (and attachments), and data copies.

IN THIS CHAPTER

- **Managing endpoints holistically**
- **Improving user productivity with performance and experience management**
- **Using a cloud-native solution for unified endpoint management**
- **Gaining deep insights with analytics**
- **Leveraging automation and orchestration for real-time threat remediation**
- **Maintaining device compliance**

Chapter 5 Enabling IT Modernization

Modern PC management allows your IT team to manage desktops and laptops over the air in the same way you manage mobile devices, using a common management platform, called *unified endpoint management* (UEM). In this chapter, I explain the key capabilities in UEM that enable IT modernization for the distributed workforce.

Unified Control Point Management and Governance

UEM is a key part of any digital workspace strategy. With a digital workspace approach, your IT organization can securely deliver and manage any app on any device by integrating access control, application management, and multi-platform endpoint management.

UEM is the backbone for the digital workspace. It eliminates the need to use a hodgepodge of point solutions to manage mobile, desktop, and Internet of Things (IoT) devices. With a comprehensive UEM solution, you can use a single platform to manage every device and every operating system, across any use case, with a consistent set of policies across all device types and operating systems.

UEM solutions provide a holistic and user-centric approach to managing all your endpoints. They combine the traditional client management capabilities for desktop PCs — such as operating system (OS) deployment, configuration management, software distribution, and OS patching — with a modern enterprise mobility management (EMM) framework that includes efficient mobile device management (MDM) capabilities. A comprehensive UEM solution enables your IT team to deliver a consistent experience across all endpoints, to secure and manage the full device life cycle, and to do it all from a central console.

Performance and Experience Management

Employee experience is emerging as a strategic imperative as a growing number of studies are finding a direct correlation between a positive employee experience and business outcomes (see Figure 5-1). When employee experiences are meaningful and fulfilling, employees are more engaged and productive. And in fact, a link between employee job satisfaction and customer experience is also emerging. Conversely, companies that don't invest in employee experience are finding it difficult to recruit and retain employees, which negatively impacts the business overall. Addressing employee experience holistically — from hire through retire — must be at the heart of every company's digital workspace design and is paramount to workforce transformation success.

Previously, many organizations held HR solely accountable for employee experience. However, increasingly more companies, especially those well on their digital transformation journey, embrace employee experience as a cross-discipline activity that requires the support of other departments including line of business, IT, facilities, and legal. Additionally, as employee experience is influenced by three primary factors — company culture, technology, and physical experience — and given that technology contributes to all three of these areas, IT must be an active participant.

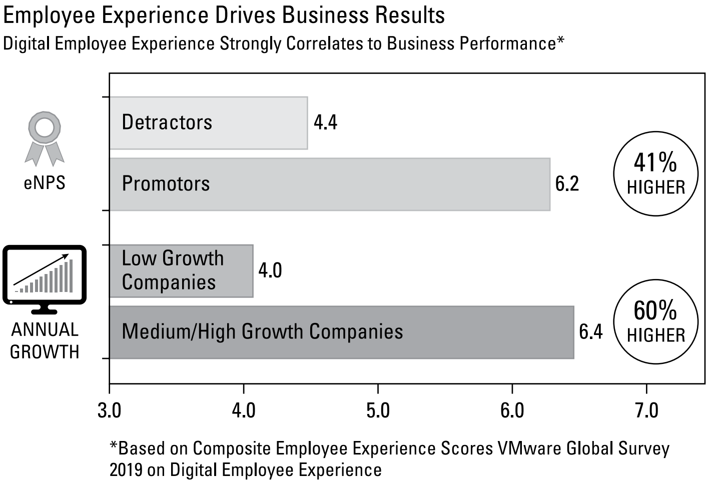


FIGURE 5-1: VMware research shows a direct correlation between digital employee experience and business performance.

REMEMBER

IT is well positioned to address the top issues identified by employees as critical to a positive experience:

- Easy access to applications and data and device choice
- Collaborative and meaningful work
- Flexible work options

Cloud-Native Management

Digital infrastructures are central to driving successful business outcomes, and cloud adoption is how organizations standardize platforms and reduce time to market. By taking a modern, cloud-based approach to the unified management of endpoints and business processes, organizations can

- Standardize and automate operations across multiple platforms
- Improve efficiency and increase the speed of innovation

WARNING

Most cloud-based modern management solutions are not cloud native, meaning they aren't designed for or built in the cloud. Cloud ready is not the same thing as cloud native. A cloud-ready solution simply connects on-premises management infrastructure to the cloud for visibility, but not for modern management. A cloud-native solution is designed for and built in the cloud to support unified modern management of all endpoints from one place.

Analytics

The core power of UEM can be extended with a consolidated pool of data and analytics tools that enable smarter endpoint management. This next-generation approach gives your IT team the ability to leverage data captured from across the digital workspace environment — from the device to the apps to the identity of each user — to gain deep insights into what's really going on across your distributed workforce.

From the UEM console, you can search and query your environment to analyze data, identify patterns, and detect anomalies. With custom dashboard views and historical reports, you have quick access to the information you need to make the right data-driven decisions based on a clear view of the following (and more):

- Device types
- OS distribution
- App deployment
- App adoption
- App usage
- App versions
- App licensing

With a modern management platform, your IT admins can easily run reports to identify assets with vulnerabilities that need to be patched, monitor critical Windows security status across your environment, see the installation progress for app deployments, and perform software and device inventories.

Automation

With visibility and analytics, you can build automation and orchestration. You need a platform that will allow you to collect contextual information from across the entire environment. This contextual awareness feeds intelligence, allowing you to make just-in-time decisions, and use automation for threat remediation.

Aggregated application deployment, usage, device security, and employee experience details help you better understand the performance and security of your digital workspace environments. The built-in intelligence engine in a modern PC management platform delivers automated actions, accelerates planning, enhances security, and improves employee experiences. It also delivers ongoing security risk monitoring and rapid mitigation responses for the distributed workforce.

Compliance

With conventional approaches to asset management and reporting, IT admins struggle to get any on-demand visibility into the installed updates on end-user systems. They may even have to write massive queries to get simple reports on update status.

A modern management platform solves this problem with patch intelligence and reporting that helps you stay on top of your information security requirements. For example, you can now receive detailed reports on inventory and perform compliance auditing of individual Windows updates across a fleet of end-user devices.

REMEMBER

In a modern management platform, the data from endpoint audits is tied to a powerful rules engine that enables you to automate the following:

- **Compliance:** Immediately quarantine noncompliant endpoints from company resources.
- **Remediation:** Deploy patches over the air to get the endpoint into a compliant state.

IN THIS CHAPTER

- » **Promoting a safe return to the office with contact tracing and social distancing**
- » **Providing cross-functional capabilities across teams**

Chapter 6
Rethinking Workplace Safety

The COVID-19 pandemic continues to disrupt businesses in countless ways. The quick transition to remote work came first. Now, as countries, states, and cities reopen, companies are facing a whole new set of challenges in working from the office, including allowances for social distancing, setting up in-office shifts, and monitoring occupancy limits. Leaders must consider how to ensure workplace safety while keeping collaboration opportunities available.

In this chapter, you learn about some of the relevant use cases that are emerging and the technologies that will help companies bring employees back to the office with confidence, as well as the key roles within your organization that must work closely with IT to help ensure a safe return to the office.

Enabling New Use Cases with Technology

Working from home became second nature for many people during the pandemic. Organizations learned that remote work can be productive for many job functions, but some roles require people to be physically in the office.

New technologies such as the following will help support the safe return-to-office needs of businesses:

- **Contact tracing:** Privacy-centric mobile apps will create a high-tech and privacy-focused way to assist businesses in contact tracing if an employee becomes ill. Employees can privately notify administrators and colleagues that they have tested positive. Using wearables, such as a smart watch, employees can recall their whereabouts, allowing the company to notify other employees who were in the same area at the same times as the affected employee. Employees can be notified of potential exposure while the privacy of their sick coworker is protected. Leadership can also use the information to prioritize deep cleaning in areas where the ill employee spent the most time.
- **Social distancing:** Advanced resource scheduling can be used to support booking of desks and meeting rooms and office wayfinding. These capabilities will be of immense value as organizations rethink their physical office layouts to promote social distancing and enforce safe occupancy limits.
- **Touchless badging/physical authentication:** Integrate with physical access control vendors such as HID Global to enable physical access for employees using their mobile devices to badge into buildings, printers, and other services.
- **Touchless services:** Increased use of mobile apps will enable organizations to offer more touchless services to customers, such as self-checkout or mobile checkout in retail businesses. Disinfected mobile devices can also be assigned to one employee during a shift, for inventory control, shipping, retail checkout, and other uses, instead of requiring multiple employees to share a single workstation or register.

Aligning Strategic Roles

Most organizations that offered flexible work options during the height of the pandemic have now formed cross-functional "return to site" committees that are sifting through the many legal, compliance, privacy, culture, and experience challenges as they're planning for a safe return to the office in phases. These organizations must align their teams across IT, physical security, crisis management, legal, HR, and operations to address a variety of issues, including the following:

- Automatic exposure notifications based on location data from wearables
- Manual contact tracing efforts through integrations with partners
- Occupancy limits and physical distancing
- Omnichannel communication strategies
- Digital badge for entry, kiosks, printing, and more
- Desk and conference room booking
- Office navigation

Some of the key roles leading efforts to safely return to the office include the following:

- **In-office technology managers:** This role is primarily focused on ensuring a positive employee experience (for example, providing employees with appropriate technologies to be productive and efficient in the office, such as room booking apps, contactless entry, and group computing devices). Due to the increased number of remote workers, the responsibilities of in-office technology managers must also extend to at-home and remote workers. Feedback gathered through surveys and other tools regarding employee experiences with various office spaces and configurations will provide invaluable information to incorporate into planning. Here are key questions to consider:
  - Are your current in-office platforms able to handle requirements to ensure employee productivity and collaboration in the next crisis?
  - Is your organization ready to support the needs of the new in-office workplace and ensure productivity, safety, and engagement when employees return?

  - Are the solutions you're evaluating able to address employee requirements for productivity and efficiency while ensuring scalability and security?
  - What types of productivity, collaboration, and efficiency benefits can the technology provide in the office facility and with remote workers?
- **Facilities managers:** As employees return to the office, facilities managers must be increasingly focused on technologies and contactless solutions to facilitate the health of employees in the office. Key questions to consider include the following:
  - Are you able to right-size and configure your facilities fast enough to meet the rapid workforce changes?
  - What are the technology priorities for the office facility space and the employees working in that space?
  - What type of technology, space, and physical infrastructure requirements are necessary to support employees in the building and operational processes occurring in the building?
  - What kinds of productivity, safety, and health benefits can the technology provide for our office facilities with in-office workers, hybrid workers, and visitors?
- **HR managers:** Priorities for HR managers include addressing the increase in remote and hybrid workers from the pandemic while ensuring employee happiness, wellness, and productivity working outside the office. Key questions to consider include the following:
  - Does the technology provided to employees position your company to hire and retain talent better than your competitors?
  - Does the technology empower your employees to be successful?
  - How can your technology solution differentiate the employee experience and enhance their ability to be productive and effective in their roles?
  - What improvements in recruiting, employee satisfaction, performance management, and talent development can technology deliver?

- **Identity and access management (IAM) architects and Security Operations (SecOps) managers:** IAM architects and SecOps managers have critical roles in security that must evolve to protect access for large remote workforces across distributed, hybrid IT environments. Here are key questions to consider:
  - How can consistent access control policies be applied across many different types of workers accessing different types of corporate-owned and personal devices?
  - How can you extend incident response and other SecOps processes to your remote workforce to maintain a strong security posture across hybrid environments?
  - How can you ensure that your users and their associated devices accessing your corporate data are secure and comply with corporate policies and regulatory requirements?

IN THIS CHAPTER

- » Improving morale, recruiting and retention while driving productivity
- » Achieving work–life balance and enabling a global workforce
- » Increasing business agility through IT modernization
- » Keeping the distributed workforce secure
- » Protecting the environment
- » Ensuring business continuity and promoting workplace safety
- » Looking to the future of work

Chapter 7 Ten Key Outcomes of Investing in the Anywhere Workspace

The distributed workforce is here to stay. Investing in the right technologies for your distributed workforce will help your business reap the benefits of remote work beyond the pandemic as working from home becomes the new normal for many businesses. Here are ten benefits of making smart technology investments today to support your distributed workforce.

Creating a Superior Employee Experience

Giving your employees access to the right tools to do their jobs is key to improving morale, recruiting, and retention. Read Chapter 1 to learn how creating a superior employee experience for the distributed workforce has helped companies and their employees thrive while working from home during the pandemic.

Increasing Productivity

Armed with the right technologies, your distributed workforce can be productive from anywhere — in the office, on the road, and increasingly at home. Many companies report that productivity and team collaboration have either remained the same or increased for their employees while working from home. Turn to Chapter 1 to learn more.

Maintaining a Good Work–Life Balance

Working from home can blur the lines between work lives and personal lives. On the positive side, many employees have found that working from home allows them to spend more time with their families, reduces commuting and other daily expenses, and provides more flexibility to take care of personal matters when needed. However, working from home also presents challenges such as staying focused on work, defining the start and end of the workday, and engaging with other remote team members. The right technologies can help your employees to better manage this important balance.

Working from Anywhere with a Diverse Global Talent Pool

The right technologies enable your employees to be productive from anywhere, which means your recruiting efforts don’t necessarily have to be geographically limited. You can recruit from an incredibly diverse global talent pool to find the best employees for your company from anywhere in the world.

Enabling IT Modernization

IT modernization isn't about having the latest and greatest technology. It's about enabling business agility through digital transformation with innovations like unified endpoint management, modern PC life-cycle management, and virtual application and desktop delivery to provide touchless support for the distributed workforce. Secure access service edge (SASE) further enables IT modernization by revolutionizing the way organizations operate at the edge. The security-driven networking approach of SASE enables organizations to move away from siloed IT environments and integrate networking and security in a unified, comprehensive IT infrastructure. The cloud has made all this possible with on-demand access to resources and services that drive digital transformation initiatives.

Ensuring Security with End-to-End Zero Trust Security

Zero Trust security invokes a "never trust, always verify" approach to security that extends from users and devices to transport/session, applications, and data. In today's increasingly hostile and sophisticated threat landscape, Zero Trust is the right approach to ensure a strong security posture across the distributed workforce.

Reducing Carbon Emissions

The environmental benefits of remote working have long been touted by teleworking advocates. Understandably, with fewer vehicles making the daily commute to work, carbon emissions will decrease. But how much of an impact remote working can have on the environment has always been somewhat subjective. However, an October 2020 article by Nature Communications `https://via.vmw.com/EQQz`. found that global carbon emissions decreased 8.8 percent in the first half of 2020 compared to the same period in 2019, corresponding to mandatory lockdowns in response to the global pandemic.

Improving Disaster Recovery and Business Continuity Capabilities

Disaster recovery and business continuity plans are no doubt being feverishly updated based on lessons learned during the global pandemic. Many companies were able to continue normal business operations without missing a beat, but far more were unpleasantly surprised by the disruptions caused by outdated plans that did not sufficiently account for the pandemic and lockdowns. And many businesses have shut down permanently as a result. The right technologies can enable the distributed workforce to work productively from anywhere so that disasters and other events — whether natural or manmade, regional or global, catastrophic or otherwise — won't disrupt your business.

Promoting Workplace Safety and Well-Being

A distributed workforce can also help organizations promote workplace safety and well-being. Following the September 11, 2001, terrorist attacks on the United States, insurers began adjusting their risk portfolios to account for mass casualty events. Corralling your workforce in large office buildings puts your employees at risk from disasters such as fire, severe weather, terrorism, and civil unrest, as well as global pandemics. Investing in the right technologies enables your employees to work from anywhere and can also improve workplace safety and well-being in the office with technologies that enable contact tracing, heat maps, and other innovations. (Turn to Chapter 6 to learn more.)

Redefining the Nature of Work

We all learned at a young age in physical science classes that work equals force times distance. But this formula doesn't mean that the further you commute, the more work you get done! The global pandemic has required businesses everywhere to redefine the nature of work and refocus on the true meaning of work. It's about producing a desired output; it's not a destination. For successful companies, the distributed workforce can be a force multiplier, enabling work to be done more effectively and productively by a highly motivated and diverse global workforce with the right technologies.

Modernize IT to support today's anywhere workforce

While the COVID-19 pandemic has forced companies to switch to remote working very quickly as a response to state and local government directives, it has also served as a wake-up call for many companies. Remote work is proving to be a very real option for many companies to continue operating in these challenging times. The current crisis provides an opportunity for organizations to perhaps bolster their workplace flexibility options, improve their technology investments and cybersecurity, and take another look at their operational processes.

Inside…

- Discover new trends in today's anywhere workforce
- Evolve into a modern distributed workforce
- Onboard new employees remotely and seamlessly
- Support flexible user choices and self-service
- Keep your anywhere workforce secure and safe
- Ensure workplace safety through innovation

vmware®

Lawrence Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 200 *For Dummies* books on numerous technology and security topics.

ISBN: 978-1-119-79674-9
Not For Resale

9 781119 796749

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT