TREND BRIEF

SHUT THE DOOR ON DATA LOSS

Learn about the latest trends in data protection for digital workspaces

AT A GLANCE

Limiting the apps and data that employees can use was a common security strategy, until unimpressed end users started going around IT to get what they wanted. Known as **shadow IT**, this trend created even greater risk exposure for organizations.

Top of mind with IT Leaders in 2018 is a flexible digital workspace that:

- Hosts the apps and devices needed to accelerate innovation
- Allows users to work when, where and how they choose

Welcome to the Digital Workspace

Modern organizations are made up of different types of users with different types of needs when it comes to accessing applications, data, documents, and other digital resources.

The apps and devices that employees use—PCs, laptops, tablets, and smartphones—in the office, at home, or on the road, are known as the *digital workspace*. A digital workspace champions flexible, employee-centric technology to aid productivity and unlock the potential of employees, teams, and organizations.

According to Sumit Dhawan, VMware senior vice president and general manager, End-User Computing, enterprises have two major objectives when they look to deliver digital workspace capabilities to their employees.

"The first objective," Dhawan says, is to ensure enterprises can implement and "maintain compliance and security over a wide range of endpoints, especially those they don't own and operate." These endpoints range from desktop computers to smartphones to tablets and other devices, both personal and professional.

The second objective, Dhawan says, is to "enable the workforce to successfully adopt and leverage new technologies as key participants in the digital transformation journey." The goal, he emphasizes, is to create a digital workspace that mirrors the experience the workforce already enjoys in their personal lives.

The Digital Workspace Demands Sophisticated Security Strategies

Picture it. An employee in your organization has accessed your network via VPN, and malware has found its way through the perimeter firewall and into your network.

It's likely that the person who caused the breach had no idea they did it. They might have accessed the network via VPN using a corporate-owned machine with security patches that were out of date. Or they might have logged in to their web email, unknowingly downloaded an unsafe document, and then saved that document to the corporate server.

No matter how it happened, the network has been penetrated, and now your goal is to prevent it from becoming a full-on disaster. All eyes are on you to find the source, stop the problem, and make sure it doesn't happen again.

This is a common scenario that nobody wants to experience. In today's world people, devices, and objects have become more connected than ever before, and IT teams need to secure the increased interaction between users, applications, and data.

For many years, limiting the apps and data that employees could use was a popular security strategy—until unimpressed end users started going around IT to get what they wanted. Known as shadow IT, this trend created heightened risk exposure for organizations.

DIGITAL WORKSPACES FEATURING ENTERPRISE-GRADE SECURITY SAVE IT AND END USERS TIME WITH:

Rapid Deployment – Onboard employees across devices *within one hour*.

Contextual Control – Establish access policies for any app *in one place*.

Mobile Access – Complete transactional workflows in *less than 72 seconds*.

Remote Management – Provision a corporate laptop from anywhere *within minutes*.

As a result, creating a secure, state-of-the-art digital workspace that is flexible enough to host the apps and devices needed to accelerate innovation, and accessible enough to let users work when, where, and how they're most efficient, is top of mind among IT leaders.

More than ever before, the most effective way to improve security is to provide employees with a choice of apps and devices. Doing so means that network administrators must (1) design sophisticated data loss prevention (DLP) strategies, and (2) leverage a platform solution that provides the intelligence, automation, and common rules engine necessary to enforce policies across mobile, desktop, and line-of-business applications on-premises or in the cloud.

1. Balancing portability with protection

Seemingly simple services that employees at most organizations have come to expect—such as a seamless remote-access experience—can still require IT to overcome multiple hurdles.

VPNs were introduced in the 1990s to extend a corporate LAN to employees' home offices and hotels. It meant giving employees remote access to the entire network from a controlled device in order to mirror their experience when working directly on the internal network.

VPN solutions using multi-factor authentication can be expensive and complicated to deploy. Passwords can also be hacked through brute force attacks, and the physical tokens that many of these solutions require are complex, easily forgotten, or misplaced. As a result, organizations are rethinking their approaches, using a consumer-simple, enterprise-secure digital workspace platform. They are virtualizing applications or entire desktops and automatically provisioning them to the cloud or to on-premises infrastructure. Employees can access these highly available virtual applications or desktops across any device or network at any time through a common catalog.

However, networks are accessed by different types of devices running on different platforms with differing ownership models such as corporate owned, corporate owned personally enabled (COPE), and bring your own (BYO). Employees who use their own devices to access the network via VPN pose a risk of bringing malware to the network environment without their realizing it. These devices are unmanaged, or at least untrusted, and there is nothing in the VPN connection process that assesses the state of a device. If any type of malware is on an access device, the malicious software can easily propagate across the VPN into the broader network. This represents a huge attack surface for malware.

Even corporate-owned devices can be problematic. They require remote users to be on the corporate domain to learn about and download patches to keep security protocols up to date. Remote users might spend very little time on the domain, and might not even know a patch is required until it is too late.

Many organizations implement desktop and application virtualization to improve client computing security and deliver greater enterprise mobility. Through virtualization, applications are centrally hosted and containerized, and the data in the application never touches the device that's using the application. Virtualization protects data at rest, prevents unauthorized application access, and provides a more efficient way to patch, maintain, and upgrade images.

UNIFIED ENDPOINT MANAGEMENT (UEM)

UEM is an approach in which desktop computers, laptops, smartphones, and tablets are secured and controlled in a cloud-connected, cohesive manner from a single platform and rules engine.

However, with desktop and application virtualization, new security concerns can arise behind the data center firewall—where hundreds or even thousands of desktops reside.

These desktops sit in close proximity to other users and mission-critical workloads, making them much more susceptible to malware and other attacks. These attacks can move from desktop to server, exposing a large attack surface within the data center.

This "east-west" threat scenario is a common one affecting many customers today, particularly those with stringent security and compliance mandates.

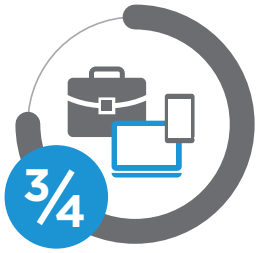
Network virtualization enables applications to run on the virtual network exactly the same as if they were on a physical network. It presents logical networking devices and services—logical ports, switches, routers, firewalls, load balancers, VPNs, and more—to connected workloads. Virtual networks offer the same features and guarantees of a physical network with the operational benefits and hardware independence of virtualization. Thus, network virtualization is a best practice that enables micro-segmentation between individual virtual apps and desktops and their connection to other hosts in the data center.

Now, as business requirements shift from connectivity to cross-platform innovation, organizations are thinking more broadly and evolving to a unified endpoint management (UEM) solution.

With UEM solutions, IT teams can determine if a device is trusted, and if so, extend more privileges to that trusted device. Should a device become lost, or its user leave the organization, the privileges can be removed. UEM solutions also include encryption to secure productivity apps like VMware Boxer™ that can encrypt and containerize email and isolate attachments. It can logically separate data between trusted and non-trusted applications.

2. Overcoming obstacles for end users

When it comes to when, where, and how work gets done, the only constant is change. Consider these statistics:



Mobile workers—telecommuters, business travelers, field workers—will make up **nearly three-quarters** of the U.S. workforce by 2020, predicts IDC[1]

Employees at the office now only spend **40–50% of their time at a desk**, reports Global Workplace Analytics[2]

71% of employees spend two hours or more each week working on mobile devices, reports Fierce Mobile IT[3]

THE DIGITAL WORKSPACE: A FOUNDATION FOR DIGITAL INNOVATION

A digital workspace platform provides the necessary infrastructure to:

- Secure access management
- Unify endpoint management
- Simplify Windows delivery

Today's workers require applications to be portable across device types, locations, and ownership models. But standard application delivery requires specific browsers, versions, and other nuances that complicate app deployment and management.

Traditional ways of accessing and managing apps and data often fall short, and have led organizations to explore alternate approaches that better meet the needs of the digital workspace.

For example, using an enterprise app catalog can facilitate the seamless delivery of all type of apps to all types of devices. And delivery of apps is only half of the equation. Users need to be able to instantly and easily access apps from any device or location. This requires frictionless access to apps and data, which one-touch mobile and single sign-on (SSO) functionality deliver. VMware solutions also include multifactor authentication across mobile devices. Its privacy-by-design approach assures users that their personal apps and data remain invisible to IT.

An enterprise app catalog can deliver the right apps to any device including:

- Internal web apps through a secured browser and seamless VPN tunnel
- SaaS apps with SAML-based SSO and provisioning framework
- Native public mobile apps through brokerage of public app stores
- Modern Windows apps through the Windows Business Store
- Legacy Windows apps through MSI package delivery or real-time delivery with app volumes
- Secure sensitive systems of record apps behind a HTML5 proxy by hosting in the data center or cloud provider with VMware Horizon® Cloud Service™
- Deliver complete virtualized managed desktops in the cloud, or in on-premises data centers

Conclusion

With applications, services, and data everywhere running on a multitude of platforms and being consumed from a myriad of devices, our approach to security must fundamentally change.

Using a digital workspace, organizations can virtualize applications or entire desktops, and automatically provision them to the cloud or to on-premises infrastructure. Users can access them from any device.

Partner Value Proposition goes here.

GET STARTED TODAY

Learn more about how to simplify Windows delivery.

LEARN MORE >

For more information contact:
Partner name, Contact Name

Partner Email

Partner Phone

Partner Website

Sources:

1. IDC, U.S. Mobile Worker Population to Surpass 105 Million by 2020, June 23, 2015
2. GlobalWorkplace Analytics.com, Latest Telecommuting Statistics, 2005 – 2015
3. Fierce Mobile IT, 2017

vmware® | PARTNERLOGO

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com