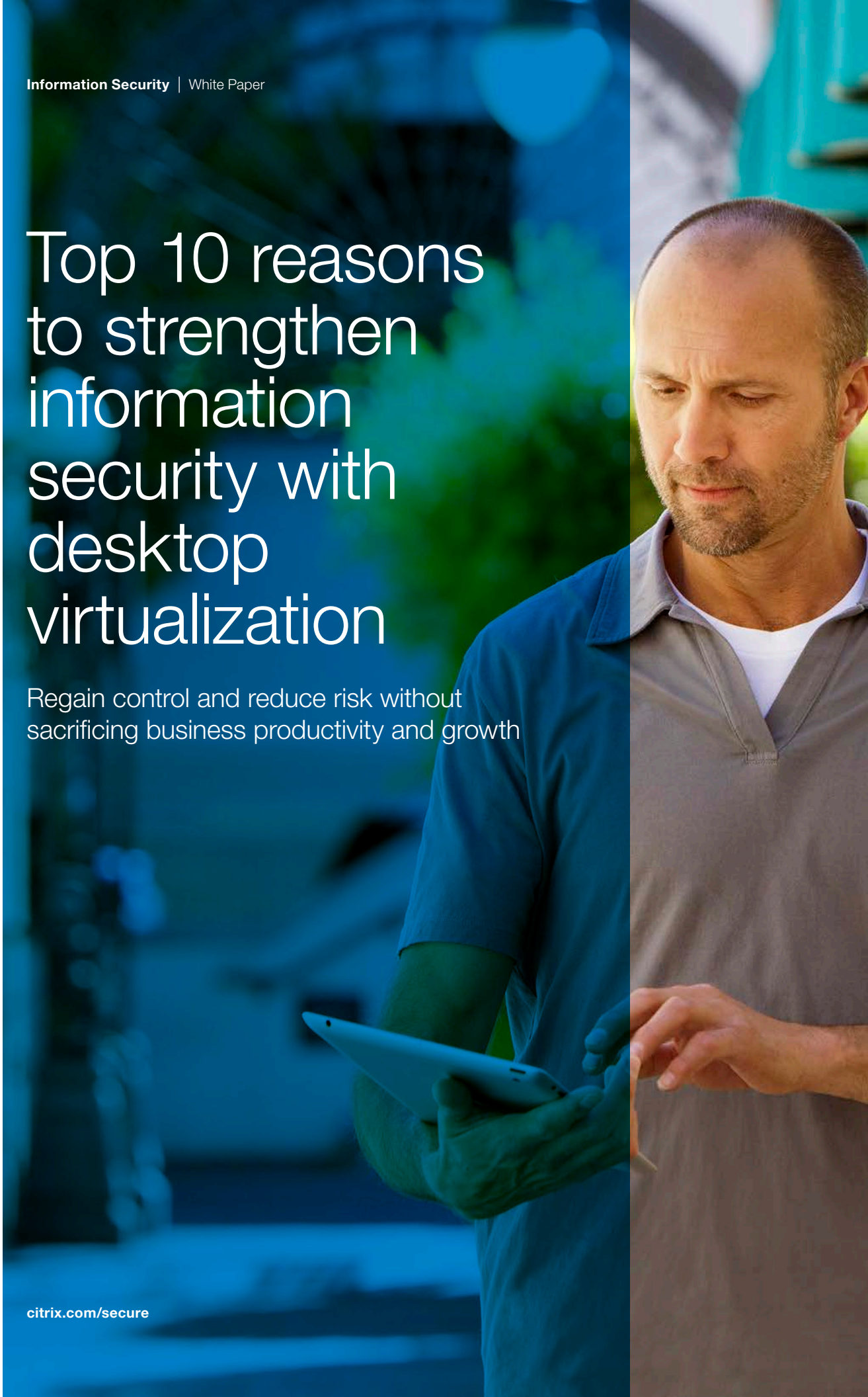
Information Security | White Paper

Top 10 reasons to strengthen information security with desktop virtualization

Regain control and reduce risk without sacrificing business productivity and growth



CITRIX®

citrix.com/secure

New ways of working call for new ways of managing risk. Mobility, flexwork, bring-your-own device (BYOD) and increased collaboration across organizations have changed the risk profile and undermine existing IT architectures. The challenge is to allow people the flexibility they need for optimal business productivity while ensuring the security and compliance required by the enterprise.

The tension between security and business productivity has never been so acute. To operate at peak performance and competitiveness, organizations need their people to access enterprise resources in more places and in more ways than ever before—but the resulting proliferation of work locations, types of workers and access methods has pushed traditional security strategies to the breaking point. The consumerization of IT adds further complexity as a diverse mix of laptops, tablets and smartphones enter the environment, including both enterprise-provisioned and personally-owned devices. Device diversity has led to extreme complexity, as the many combinations of OS, apps and configurations have destroyed the consistency model of the corporate managed laptop.

While technologies such as firewalls, antivirus, access control and perimeter monitoring remain an important base, they're increasingly bypassed, as today's skilled attackers directly target applications, data and devices. What's needed is a new security layer—one that makes it possible to manage risk more effectively. Desktop virtualization provides that additional security layer, allowing full freedom for organizations to embrace business initiatives including mobility, flexwork and BYOD, and to deploy personnel and resources wherever and whenever they're needed. At the same time, desktop virtualization complemented by secure file sharing and enterprise mobility management helps fortify information security and compliance across apps, data and devices in support of business and IT priorities.

This paper discusses the use of desktop virtualization to strengthen information security, including:

- The growing challenge of maintaining information security in today's evolving enterprise environment
- Key advantages of desktop virtualization as an inherently more secure computing architecture
- The top ten benefits of using desktop virtualization to strengthen information security

Rising complexity puts organizations at risk

Information security has become an increasingly critical concern for organizations of all kinds. Today's threats are more potent than ever, from the infection of corporate networks by custom malware, to targeted hacking, sophisticated phishing attacks, outright tampering or theft of assets and intellectual property and people simply forgetting their tablet or smartphone somewhere. In the CSO 2013 Global State of Information Security Survey, 13 percent of respondents reported 50 or more security incidents per year—"far above the levels of earlier years."[1] Incidents like the WikiLeaks scandal and the theft of personal information from corporations have shown the magnitude of the risks organizations face. Security incidents also disrupt the continuity of business operations, which can't return to normal until the breach has been diagnosed and stopped, and damage has been assessed and repaired.

While effective information security is vital to achieve, it's increasingly challenging to maintain. Trends such as mobility, flexwork, consumerization including BYOD, and cloud computing mean that more people, including teleworkers, mobile users, partners, outsourcing providers and other contractors are accessing enterprise applications and data from more places, on more devices and in more ways, than ever before. Consequently, business information is now everywhere: at people's homes, on enterprise and personally-owned endpoints, in public and private clouds, at partner organizations, on the factory floor—the list goes on. People with valid access credentials can easily copy, paste, print, save, email and otherwise exfiltrate sensitive information. Not surprisingly, a recent SANS survey found that "An overwhelming 97 percent thought incorporating mobile access and security policy into their overall security and compliance framework is important, with 37 percent believing it is critical and 40 percent believing it is extremely important."[2]

Securing traditional PCs across this broad landscape would be challenging enough, but IT must also now account for multiple types of devices, including laptops, tablets and smartphones, especially as bring-your-own-device strategies become more widespread. Each of these devices, as well as the operating systems and applications they run, must be kept up to date with the latest patches and hotfixes. Using traditional security approaches, it's an almost impossible feat.

Stopping the next breach is only part of the challenge. Every hour of every day, IT must maintain compliance with a myriad of security requirements spelled out in contractual relationships with customers and partners; laws and regulations on data privacy and compliance that vary across industries and geographies; and the organization's own best practices and data security, retention, privacy and compliance policies designed to protect its vital interests.

In this light, it's no wonder that many in IT feel like they're rapidly falling behind, spending more and more money on security without being able to address the inherent inadequacy of legacy security strategies for today's more complex computing environments. The fundamental question remains: how can IT regain control over data and reduce the growing risk to the business? The simplest approach is to lock down access and force everyone to work within the corporate LAN on standard devices—but this would pose unacceptable constraints on business agility and productivity, not to mention the prospect of frustrated

employees revolting against overly restrictive conditions. After all, IT is supposed to help business get things done, not make it impossible to do so. How can IT say yes to the requirements of organizations and people for more dynamic, flexible and mobile ways of doing business that support greater productivity, without compromising information security?

While eliminating risk entirely is unrealistic, there is a way for IT to manage risk to meet the organization's requirements for information security, data protection, privacy and compliance—while maximizing business productivity and allowing unfettered growth. The essence of the strategy is to enable the right level of secure access and collaboration for people, while maximizing control and protection of enterprise data, applications and infrastructure. The enabling technology for this strategy is desktop virtualization.

Desktop virtualization: secure by design

Desktop virtualization gives organizations a better way to secure their information and manage risk. The foundation of desktop virtualization is the centralization of IT resources in the datacenter—an inherently more secure architecture that makes it far simpler to control both information and access. Centrally managed virtualized Windows applications and desktops are delivered on-demand as a service, giving people an experience that looks, feels and acts like their traditional PC no matter how they access it or what kind of device they use. In the words of Gartner, "A real synergy exists between desktop virtualization and a flexible strategy for supporting 'anytime, anywhere, any device' access."[3]

A well-designed desktop virtualization solution offers important advantages over traditional security models.

- **Resource centralization** – Enterprise Windows applications and associated data are managed and secured in the datacenter and accessed securely from anywhere, rather than residing on the endpoint devices of every person in the extended enterprise, greatly reducing business risk. IT gains full visibility and control over centrally managed Windows applications and desktops, and can easily define and enforce policies over which resources specific users or groups can access, and whether or not they can install and configure applications themselves. Windows application and desktop access can be turned on and off instantly as needed in the event of new or departing staff, transfers and business continuity scenarios in which designated people need to assume increased responsibility.
- **Policy-based access control** – IT can leverage pre-configured policies to determine the appropriate level of user access to Windows applications wherever they reside: in the datacenter, in a public or private cloud—even downloaded to a local device for offline use, where full isolation, encryption, and strict control over save/copy functionality and peripheral usage prevent data from going astray. Policy-based access control supports multi-level security practices by letting IT deliver the right level of access based on the user's current profile, device, network and location. For example, a user can be allowed to access one set of resources from the office, a subset of those resources from

their own personal computer at home and a smaller subset from a rented device or while connected via a public hotspot. In addition to which resources the user may access, granular policies can be set regarding what actions they may perform on each application. For example, a policy may indicate that when using an enterprise-managed device the user can print, upload or download data; but when using an untrusted device such as a public kiosk or their personal tablet, they can only view the data.

- **Any-device access** – Because virtual Windows apps and desktops are hardware-independent, IT can enable secure access and collaboration for every employee, contractor or partner from any personal or corporate-owned device they choose to use. Rather than making distinctions between enterprise-owned and outside devices, IT evaluates every device and user according to administrator-defined criteria as people attempt to connect to the enterprise network, then grants the appropriate levels of access to each resource as indicated by the access control policies.
- **Built-in data compliance** – The centralization of resources, combined with strict access control, makes it much easier to protect against data loss and meet compliance and privacy standards by ensuring full activity logging, reporting and auditing. IT can define and implement policies to ensure conformance with the full spectrum of requirements the organization faces—both internal and external—while maintaining the flexibility to respond to new mandates as they emerge.

Citrix enables desktop virtualization through a complete solution designed to provide the centralized control and management, flexible delivery scenarios, granular, policy-based access control, endpoint protection and compliance support organizations need to manage risk without obstructing business productivity or growth. The core of the solution is Citrix XenDesktop, which enables on-demand delivery of virtual Windows applications and desktops, complemented by application delivery control, secure access control and client-side virtualization and encryption. In 2011, the Information Systems Security Association (ISSA), one of the most prestigious security associations in the world, honored Citrix with the ISSA Outstanding Organization of the Year Award in recognition of its contributions to the advancement of information security.

Security is already one of the main reasons organizations are adopting desktop virtualization, along with strategic business priorities such as mobility, flexwork, BYOD, business continuity, mergers and acquisitions, business process outsourcing and IT efficiency. By making desktop virtualization a central element of security, IT can manage risk more effectively while providing optimal flexibility to allow the business to do what it needs to do, the way it needs to do it.

The top 10 reasons to strengthen information security with desktop virtualization

1. Support workplace flexibility and mobility

Mobility is vital for today's enterprise workforce. No longer bound to their desks, an increasing number of people routinely work at partner or customer sites, at home, on the road and in other locations outside the office. Wherever they work, their productivity depends on anywhere, any time access to applications and information, as well as on the ability to share, collaborate or join meetings from anywhere at any time. On an enterprise level, flexwork has become a key strategy, as organizations move work to different locations, times and resources to ensure work is done by the right people, in the right place at the right time. This can include everything from introducing teleworking and desk-sharing programs; to moving business processes or entire departments to new locations. In this way, they can increase productivity; reduce real estate, travel and labor costs; and improve business continuity.

Citrix XenDesktop helps organizations maintain information security even while allowing anyone access to IT resources from more locations. Centralized application and data management and granular access control policies allow only authorized users to connect to enterprise resources. IT can provide secure access to anyone, anywhere, at a moment's notice, to a specific set of resources, and can modify and terminate access just as quickly. People can use any kind of device to access their virtual Windows applications and desktops, from laptops to tablets and smartphones, without the need for IT to configure individual endpoints—a key advantage when the endpoints in question are at the user's home, at another company or on the other side of the world. Taken as a whole, desktop virtualization makes mobility and flexwork initiatives simpler, less costly, faster to implement and secure so the company can realize the full value of this key strategy.

2. Say yes to consumerization

Consumerization, including both consumer devices purchased by the organization and those owned by individual staff, coupled with readily available high-speed connections across the globe, has greatly increased the ability of people to do their work in the most convenient, productive manner possible. Whether people bring the laptop of their choice into the office, work on a tablet while offsite or check in via smartphone to respond to business needs while in transit, consumerization is a win-win for people and the organization—but it greatly complicates the security picture for IT. Different devices may have different types of security software in place, or none at all; many popular devices don't support antivirus, personal firewalls or other legacy control measures. IT needs a way to securely partition business and personal data on consumer-grade mobile devices.

Desktop virtualization frees IT from the prospect of managing security complexity across a virtually unlimited range of user devices. It helps prevent data from residing on endpoints by centrally controlling information in the datacenter. Windows applications, data and desktops are delivered to the endpoint only in virtualized form, isolated from any personal data or applications on the device, and cannot be moved out of the centrally controlled data store. Even if a virus infects the personal content on a device, the organization's isolated virtual desktop

minimizes the impact the virus has on business resources. Policies can keep unmanaged (and potentially compromised) devices from interacting with sensitive data to further mitigate risk. In addition to virtualized Windows apps and desktops, Citrix offers Worx Mobile Apps and mobile device management to provide enhanced control and protection for virtualized resources accessed on mobile devices.

3. Prevent data loss, ensure privacy and protect intellectual property

For optimal productivity and speed to market, organizations need to enable collaborative access to sensitive data and intellectual property across both the value chain and the supply chain. Partners, suppliers, contractors and other third parties need to be able to access and share applications and data with the organization's staff to keep operations running at peak performance, but without being given free rein within the firewall. IT needs to not only prevent data loss and protect intellectual property but also ensure data privacy and client confidentiality, honor contractual commitments and maintain compliance.

By centralizing resources in the datacenter, desktop virtualization lets IT manage and secure Windows applications and associated data more simply and effectively in a single location rather than in thousands of different locations across the organization and beyond. Instead of worrying about data being saved on removable media such as USB drives, emailed among users, printed out or otherwise exposed to loss or theft, IT can set policies to control the ability to save, copy, print or otherwise move data through a central point of administration. For usage cases that require offline or locally installed resources, Citrix allows IT to encrypt data within a secure, isolated container on the endpoint which can be wiped remotely, helping to ensure security even if the device is lost or stolen. XenClient enables Windows laptops with these capabilities and XenMobile enables similar isolation on mobile devices.

4. Maintain global compliance

Compliance with national and international laws, industry regulations and organizational policies is both a rising burden and a moving target. With little ability to control the distribution of sensitive data and a lack of session-specific location data, IT has struggled with trans-border compliance issues. Apply a full set of controls, and information usage is overly restrictive. Apply a minimum set of controls, and the result may not map to the organization's own unique security needs and risk tolerance.

The centralized, granular policy control enabled by desktop virtualization lets IT stop handling compliance and data privacy in a reactive manner and allows them to develop the right information security strategy for their own industry, business needs and risk profile. A single set of policies can govern whether users can add applications, copy data, access peripherals and other actions depending on their location and other factors. Industry-specific rules can be applied to business units and worker types that fall under specific industry regulations, such as European Union (E.U.) privacy mandates, the Health Insurance Portability and Accountability Act (HIPAA) in healthcare, PCI for the Payment Card Industry and the Sarbanes-Oxley Act.

In other cases, the centralization at the core of desktop virtualization greatly reduces the burden of achieving compliance and data privacy. For example, the European Union protects the movement of data belonging to its nationals across E.U. borders. With desktop virtualization, the data can be accessed from literally anywhere in the world without actually leaving the datacenter, allowing IT organizations to fine-tune access to restricted information. Citrix helps organizations demonstrate compliance through full activity logging, reporting and auditing. As new regulations and standards emerge, the Citrix solution makes it simple to define new policies to ensure compliance within the same coherent framework.

5. Empower contractors

Businesses are making more use than ever of contractors, temps, consultants, outsourcing partners, offshoring resources and other contingent workers. While this can increase flexibility and efficiency, it also presents a challenge for IT: providing the resources these contractors need quickly and easily—and deprovisioning them just as effectively once the engagement is over. The devices to be used by contractors can be problematic as well. Allowing them to use their own equipment would reduce cost—but IT can't be certain that their devices will be able to run all the applications required for their work.

Desktop virtualization provides a solution to both of these problems. Windows applications and desktops can be provisioned and deprovisioned instantly from a single, central point of administration, even for contractors on the other side of the world. Apps and desktops can also be delivered to any type of device, whether owned by the contractor, a business partner or the enterprise, or even a rented device. Following the engagement, access to resources can be turned off instantly with no apps or data left behind on the device.

6. Increase the value of existing security investments

Trying to manage security for hundreds or thousands of individual endpoint devices is extremely challenging and time-intensive, leading to inevitable delays and oversights. In fact, studies have shown that an overwhelming proportion of successful attacks took advantage of previously known vulnerabilities for which a patch or secure configuration standard was already available.

By centralizing maintenance, desktop virtualization simplifies and accelerates endpoint security. Patches, antivirus updates and hotfixes can be installed on a single master image, then deployed almost instantly throughout the organization. Similarly, XenMobile centralizes security and control for mobile devices. Freed from the time and expense of endpoint-by-endpoint OS, application, and security updates, IT can focus more effectively on what matters most: protecting data in the datacenter and responding quickly to new security requirements. Citrix complements the inherent security of desktop virtualization with strong partnerships with industry-leading security vendors to deliver a complete, multilayered security solution. Citrix Ready security solutions provide additional security customization and freedom of choice for protecting sensitive data assets.

7. Safeguard information and operations during a disaster or other business disruption

A business disruption, whether planned or unplanned, natural or man-made, can be a time of great vulnerability for an organization as ordinary practices change, people access applications and data in new ways, and perimeter or endpoint security measures may be compromised. When a disaster occurs, organizations need to be able to ensure not only that data and applications remain secure, but also that business operations can continue in as close to normal a manner as possible to avoid reputation damage, financial losses, damaged customer and partner relationships, lost productivity and other consequences.

Desktop virtualization provides an approach to business continuity encompassing both the datacenter and the people who rely on it. The centralization of resources supports a dual datacenter strategy in which people will automatically be switched from one to the other quickly and transparently to continue working. Meanwhile, IT can focus on protecting Windows apps and data centralized within the datacenter, and on securing, provisioning and controlling access to these resources via XenDesktop and XenMobile, rather than having to manage local apps and data on myriad user devices throughout the organization. Endpoints that may no longer be secure—such as laptops left behind in an evacuation—hold no data in usable form. IT can easily turn off their ability to access virtual Windows applications and desktops and even wipe data remotely. The same applies for mobile devices, which can be wiped selectively using XenMobile. For people, virtual applications and desktops can be accessed using any available device in any available location, without the need to move data onto a USB drive or by email, or the risk that data will be left behind on a rented or borrowed computer.

8. Minimize the impact of information security breaches

No strategy can guarantee perfect information security in perpetuity. An essential part of risk management is being able to limit the damage caused by any incidents that do arise.

Centralized management enables IT to take fast action in the event of a security breach or misconfiguration. The first line of defense is using virtualization to isolate sensitive applications and data and run them on user privilege accounts (instead of user controlled machines), minimizing the impact of the breach of a single component. Even if the machine does get infected, the second line of defense resets the image through virtualization upon machine reboot. For example, a rogue PDF file would only impact the virtualized PDF reader's functionality, and wouldn't have access to the Windows registry and file system as it would in a non-virtualized system. Browsers can similarly be protected and isolated from causing widespread damage due to a compromise. If the integrity of a user is compromised, such as in a zero-day attack, IT can quickly take the user's environment offline and restore it to an uncompromised state by reverting to a golden image. With security measures installed and enforced on every virtual system, damaging attacks are prevented from spreading to every other system in the environment—and IT can update access policies across the environment at a moment's notice.

9. Support rapid business growth

When organizations open new branch offices, expand existing locations or combine operations with or acquire another company, an overly complex, distributed security model can delay time to value as IT works to secure each person's endpoint.

Desktop virtualization provides the ability to extend the organization's existing security model to new locations, people and groups quickly, easily and cost-efficiently. It simplifies remote office and branch management in several ways such as local lockdown, rapid setup and high availability—all enabling IT to provide instant access to virtual desktops with no need for network integration. Adding new users to existing groups according to their security profile and work requirements means that the right policies are applied from day one. As rapidly growing organizations turn to flexible work styles such as leveraging contractors, outsourcing and teleworking to scale their operations, they can provide secure application and desktop access to any type of worker in any location on any device without being constrained by a rigid or inefficient security model—all the while keeping tight control over exactly how and where data is accessed.

10. Get security out of the way of users

Traditionally, security has been enforced at the expense of users. They've been allowed to work in limited places, access minimal resources, rely on standard corporate equipment, sacrifice mobility and spend more and more time authenticating into systems and managing their passwords. In response, even the most loyal employee can take an adversarial view of security and look for ways to circumvent or subvert the rules—such as copying data onto a forbidden USB drive to work at home, installing unauthorized applications, ignoring network access policies, and using their own devices and applications without restriction.

Desktop virtualization turns this model on its head: instead of having to deal with endless details of endpoint security, people simply sign on once to a virtual desktop with their virtual applications, delivered on-demand anywhere they need to work, on the device of their choosing, and they're free to do their work while IT handles security centrally in the datacenter. The ability to work anywhere, use consumer devices and even bring their own device improves productivity and satisfaction—all while minimizing the risk of a security breach. Policies are specified by IT and automatically enforced—regardless of user or access method.

Conclusion

Organizations can't afford to fall further behind in the attempt to get their information security practices under control. Desktop virtualization provides a secure-by-design solution to simplify security, protect intellectual property, ensure data privacy, meet compliance and manage risk while promoting business productivity and growth.

With desktop virtualization, Windows applications, data and desktops are centralized and secured in the datacenter, rather than distributed across hundreds or thousands of endpoints, and delivered on-demand with full control and visibility. The organization can enable secure access and collaboration for every employee, contractor or partner while allowing the right level of access based on their user profile, device, network or location. Centralized data management and granular access control policies help prevent data loss, ensure privacy and safeguard business assets—even for data stored on local devices or in the cloud—while comprehensive activity monitoring, logging and auditing support compliance efforts. Any-device access facilitates consumerization, as people can use virtually any laptop, tablet or smartphone to access their virtual applications and desktops without adding management complexity or introducing vulnerabilities.

The compelling benefits of desktop virtualization have already made it a top agenda item for most IT organizations. By leveraging it as a security layer, organizations can support key priorities such as mobility, flexwork and BYOD while managing risk more effectively. Applications and associated data are no longer scattered beyond IT's control because they remain where they belong—in the datacenter—where they enable greater business value than ever before.

For more information about Citrix solutions for information security, please visit www.citrix.com/secure.

Additional resources

- CSO Magazine: Empowering information security with desktop virtualization
- Secure by design: 5 customers use desktop virtualization for security
- An insider's look at security strategy based on desktop virtualization
- IT security solutions from Citrix Ready partners

1. CSO 2013 Global State of Information Security Survey.
2. SANS Survey on Mobility/BYOD Security Policies and Practices, October 2012.
3. Gartner Peer Practices: Security Impacts and Benefits for Virtual Desktop Projects, September 2012.

CITRIX®

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.