10 Reasons to Strengthen Security with App and Desktop Virtualization

Regain control and reduce risk without sacrificing business productivity and growth

By using virtualization, organizations can pursue top priorities such as mobility, flexwork and consumerization while effectively managing risk, securing information, supporting global compliance and strengthening business continuity planning.

CITRIX®

With the increased popularity of mobility, flexwork, and bring-your-own-device (BYOD) initiatives, the IT risk profile has changed. New ways of working and collaborating require new approaches to managing risk. Organizations face a balancing act: giving people the flexibility they need for optimal business productivity while ensuring the security and compliance required by the enterprise.

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.

A new layer of security

The consumerization of IT is inevitable, as diverse laptops, tablets and smartphones, including both enterprise-provisioned and personally owned devices, enter the environment. Device diversity has led to extreme complexity, as the many combinations of operating systems, 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 are increasingly being bypassed as today's skilled attackers directly target apps, data and devices. What's needed is a new security layer that makes it possible to manage risk more effectively.

Desktop virtualization provides that additional security layer, giving organizations full freedom 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 app and desktop virtualization to strengthen information security, including:

- The growing challenge of maintaining information security in today's evolving enterprise environment
- Key advantages of app and desktop virtualization as an inherently more secure computing architecture
- The top 10 benefits of using app and desktop virtualization to strengthen information security

Rising complexity puts organizations at risk

Information security has become an increasing critical concern for all organizations. Today's threats are more potent than ever, ranging from the infection of corporate networks by custom malware to targeted hacking, sophisticated phishing attacks and outright tampering with or theft of assets and intellectual property, not to mention people simply forgetting their tablet or smartphone somewhere. 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 achieving effective information security is vital, maintaining a high level of protection is increasingly challenging. Trends such as mobility, flexwork and IT consumerization including BYOD and cloud computing, mean that more people, including teleworkers, mobile users, partners, outsourcing providers and other contractors are accessing enterprise apps 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-issued and personally owned endpoints, in public and private clouds, at partner organizations, on the factory floor—the list goes on.

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 BYOD strategies become more widespread. Each of these devices, as well as its operating system and apps, must be kept up to date with the latest patches and hotfixes. Using traditional security approaches makes this effort almost impossible.

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

It is no wonder that many in IT feel like they're rapidly falling behind: while they spend more money on security, they fail to address the inherent inadequacy of legacy security strategies to protect 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 impose unacceptable constraints on business agility and productivity, not to mention employee dissatisfaction against overly restrictive conditions. After all, IT is supposed to help people get business done, not hinder their productivity.

While eliminating all risk 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 growth. The essence of the strategy is to enable the right level of access and collaboration for people while maximizing control and protection of enterprise data, apps and infrastructure. The enabling technology for this strategy is app and desktop virtualization.

App and desktop virtualization: secure by design

App and desktop virtualization gives organizations a better way to secure their information and manage risk. The foundation of app and desktop virtualization is the centralization of IT resources in the data center—an inherently secure architecture that makes it far simpler to control both information and access. Centrally managed virtualized Windows apps and desktops are delivered on demand as a service to any device, providing an experience that looks, feels and acts like working on their traditional PC.

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

- **Resource centralization –** Enterprise Windows apps and associated data are managed and protected in the data center and accessed securely from anywhere, rather than residing on the endpoint devices of every person in the extended enterprise. This model greatly reduces business risk. IT gains full visibility and control over centrally managed Windows apps and desktops, and can easily define and enforce policies regarding which resources specific users or groups can access, and whether or not they can install and configure apps themselves. Windows app and desktop access can be turned on and off instantly, as needed to accommodate new, transferring or departing staff and business continuity scenarios where designated people need to assume increased responsibility.
- **Policy-based access control –** IT can leverage preconfigured policies to determine the appropriate level of user access to Windows apps wherever they reside: in the data center, 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 a personal computer at home and a smaller subset from a rented device or while connected via a public hotspot. In addition to controlling which resources the user may access, granular policies can determine what actions they may perform with each app. 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 a personal tablet, the person 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 personally-owned 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 level 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® leads the market in app and desktop virtualization through a complete solution that provides 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 XenApp® for app virtualization and Citrix XenDesktop®, which integrates the full power of XenApp, for

comprehensive app and desktop virtualization. This solution enables on-demand delivery of virtual Windows apps and desktops, complemented by application delivery control, secure access control and client-side virtualization and encryption.

Security is one of the key reasons why organizations are adopting app and desktop virtualization. By making app and desktop virtualization a central element of security, IT can manage risk more effectively while giving the business optimal flexibility to do what it needs to do, the way it needs to do it.

10 reasons to strengthen information security with app and 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 the ability to access apps and information, as well as share data, collaborate or join meetings, anywhere and at any time. Flexwork has become a key enterprise strategy as organizations move work to different locations, times and resources to ensure it is done by the right people, in the right place and at the right time. Flexwork can include everything from teleworking and desk-sharing programs to relocation of business processes or entire departments. Benefits include increased productivity and continuity of business operations, as well as reduced real estate, travel and labor costs.

XenApp and XenDesktop help organizations maintain information security while providing flexible 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. At a moment's notice, IT can give anyone secure access 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 without requiring 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, app and desktop virtualization makes mobility and flexwork initiatives simpler, less costly, faster to implement and more secure so the company can realize the full value of this strategy.

2. Say "yes" to consumerization

Consumer devices purchased by the organization and owned by individual employees, coupled with readily available high-speed connections across the globe, have 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 huge benefit for them and their organizations. However, it greatly complicates the security picture for IT. Different devices may have different types of security software, or none at all; and many popular devices don't support antivirus, personal firewalls or other legacy control measures. To properly protect business data, IT needs a way to securely partition it from personal data on consumer-grade mobile devices.

App and desktop virtualization frees IT from the daunting prospect of managing security across a very broad range of user devices. It helps prevent data from residing on endpoints by

centrally controlling information in the data center. Windows apps and desktops are delivered to the endpoint only in virtualized form, are isolated from any personal data or apps 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 containerized virtual desktop minimizes the impact of the virus on business resources. Policies can keep unmanaged (and potentially compromised) devices from interacting with sensitive data to further mitigate risk.

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

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

By centralizing resources in the data center, app and desktop virtualization lets IT manage and secure Windows apps 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 users' ability to save, copy, print or otherwise move data through a central point of administration. In use cases that require offline or locally installed resources, the Citrix solution allows IT to encrypt data within a secure, isolated container on the endpoint, which can be wiped remotely, helping to protect data even if the device is lost or stolen.

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. Applying a full set of controls to information usage is overly restrictive. Applying a minimum set of controls may fail to map to the organization's own unique security needs and risk tolerance.

Centralized, granular policy control enabled by app and desktop virtualization helps IT stop handling compliance and data privacy in a reactive manner and instead allows development of the right information security strategy for the organization's industry and business needs and risk profile. A single set of policies can govern whether users can add applications, copy data, access peripherals and perform other actions, depending on their location and other factors. Industry-specific rules can be applied to business units and worker types that fall under regulations such as European Union privacy mandates, the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act in the United States and the PCI information security standard for the payment card industry. Citrix XenApp and XenDesktop are recognized as compliant with Federal Information Processing Standards (FIPS) and have achieved the evaluation milestone for Common Criteria.

In other cases, the centralization at the core of app and 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 Member State borders. With app and desktop virtualization, data accessed from literally anywhere in the world remains in the data center without crossing borders and causing potential issues.

Citrix technology 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 greater use of contractors, temporary workers, consultants, outsourcing partners, offshoring resources and other contingent workers. While contracting can increase flexibility and efficiency, it also presents a challenge for IT: quickly and easily providing the resources these workers need, and de-provisioning them just as effectively once the engagement is over.

The devices used by contractors can be problematic as well. Allowing them to use their own equipment can reduce costs—but there is no guarantee that these devices can run all the apps required for the engagement.

App and desktop virtualization provides a solution to both of these problems. Windows apps and desktops needed by contractors—even those located on the other side of the world—can be provisioned and de-provisioned instantly from a single, central point of administration. Virtualized apps and desktops can be delivered to any type of device, whether owned by the contractor, a business partner or the enterprise, or even leased for a project. 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 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 implementing the latest protections. 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, app and desktop virtualization simplifies and accelerates endpoint security. Patches, antivirus updates and hotfixes can be quickly installed on a single master image before being deployed throughout the organization. IT can focus more effectively on what matters most: protecting data in the data center and responding quickly to new security requirements.

To strengthen the inherent security of Citrix app and desktop virtualization, the company has forged strong partnerships with leading security vendors to deliver a complete, multi-layered 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 apps and data in new ways, and perimeter or endpoint security measures risk compromise.

When a disaster occurs, organizations need to ensure not only that data and apps remain secure, but also that the business can operate as normally as possible to avoid reputation damage, financial losses, neglected customer and partner relationships, lost productivity and other consequences.

App and desktop virtualization provide an approach to business continuity encompassing both the data center and the people who rely on it. Centralization of resources supports a strategy that automatically switches people from the primary to the secondary data center quickly and transparently so they can continue working. Meanwhile, IT can focus on protecting Windows apps and data hosted within the data center, and on securing, provisioning and controlling access to these resources via XenDesktop, rather than having to manage local apps and data on a myriad of 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. Further, IT can easily turn off their access to virtual Windows apps and desktops. Meanwhile, people working in temporary offices or at home can continue to access virtual apps and desktops using any available device, without the need to transfer data via USB drive or email. They also avoid 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 limiting the damage caused by 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 apps 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 becomes 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 would not have access to the Windows registry and file system as in a non-virtualized system. Browsers can similarly be protected and isolated from causing widespread damage due to a security 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 merge with or acquire another company, an overly complex, distributed security model can delay time to value while employees wait for IT to secure each endpoint.

App and desktop virtualization provides the ability to extend the organization's existing security model to new locations, people and groups quickly, easily and cost-effectively. It simplifies remote office and branch management in several ways such as local lockdown, rapid setup and high availability—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.

10. Get security out of people's way

Traditionally, security has been enforced at the expense of users. They've been forced to work in a limited number of places, to access restricted resources, to rely on standard corporate equipment, to sacrifice mobility and to spend more time authenticating into systems and managing their passwords. In response, even the most loyal employees 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 apps, ignoring network access policies and using their own devices and apps without restriction.

App and desktop virtualization turns this model on its head. Instead of dealing with endless details of endpoint security, people simply sign on once to a virtual desktop containing their virtual apps and receive on-demand access anywhere they need to work, on the device of their choosing. They are free to do their work while IT handles security centrally in the data center. The ability to work anywhere and use personally owned devices improves productivity and satisfaction 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 behind in the attempt to get their information security practices under control. App and desktop virtualization provides a secure-by-design solution to simplify access and promote business productivity, flexibility and growth while protecting intellectual property, ensuring data privacy, meeting compliance requirements and managing risk.

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

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

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

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.