EMPOWERING INFORMATION SECURITY WITH DESKTOP VIRTUALIZATION

Since the dawn of personal computers and distributed computing, IT has faced an uphill battle to manage, control and protect enterprise applications and associated data. Recent computing disruptors—including the consumerization of IT and bring-your-own device (BYOD), flexwork where people shift work to optimal locations and times, broad mobility expectations and the advent of cloud computing—have further complicated the challenges of protecting sensitive enterprise information. These challenges are compounded by the growing sophistication and volume of information security threats against intellectual property and business data governed by compliance and privacy regulations. To control risk across the increasingly diverse computing landscape, organizations must centralize control of sensitive enterprise Windows applications, ensuring that only authorized and authenticated users have access. Desktop virtualization offers chief information security officers (CISOs) and chief information officers (CIOs) a powerful solution for today’s information security needs.
The security matrix grows in complexity

IT is often behind the curve of security requirements that arise as part of the constant evolution of computing and communications technologies, deployment models and usage patterns. The CISOs and CIOs charged with protecting enterprise information, applications and IT infrastructure struggle to keep pace with constant change and the ensuing unforeseen risks.

Further complicating matters are a variety of external security variables—ranging from regulatory, privacy, and compliance demands to an ever-more sophisticated and growing threat landscape. Changes in the makeup of both the endpoint environment and the workforce bring new challenges for IT, notes Eric Ogren, principal analyst at research firm Ogren Group. “Tablets are destined to outsell PCs in 2013, along with more powerful smartphones. As IT seeks to cost-effectively deliver traditional Windows-based applications to a mobile workforce, organizations are turning to virtualization to get out of the endpoint software installation business and to keep confidential data off untrusted mobile devices. In today’s environment, it’s not only employees that need access to enterprise resources and information; it’s also a growing cadre of contract workers, outsourcing providers and partners.”

This constantly shifting IT landscape produces an information security matrix that is as complex as it is daunting, and places enterprises at high risk for security breaches. Most recently, three business dynamics have emerged that hold great promise for boosting business growth; at the same time, they introduce new security challenges, and therefore can place sensitive enterprise information at even greater risk:

- **Flexwork and mobility:** Businesses increasingly focus on the practice of having work done at the optimal place and time. Flexwork improves the attraction and retention of people who can shift tasks to home or other locations. It enables organizations to build-out teleworking programs, hire more contract workers and other contingent labor, and take advantage of outsourcing. Mobility provides people flexibility to work anywhere and enables organizations to move workers closer to their work, customers and project sites by delivering applications, data and desktops when and where they are needed.

- **BYOD and the consumerization of IT:** Historically, new technologies deployed in enterprise environments gradually filtered out to the mass market. More recently, the flow has reversed in some instances, especially as individuals accustomed to ubiquitous, high-speed network access and powerful smartphones and tablets seek to have similar technologies and experiences at work. Some organizations are implementing bring-your-own-device strategies to accommodate people who want to use personal devices at work. The resulting proliferation of personally-owned computers, tablets, smartphones and other devices raises both secure access and data distribution challenges.

- **Cloud computing:** The rise of software as a service, infrastructure as a service (IaaS) and platform as a service (PaaS) cloud-based offerings introduced a plethora of computing environments with their own security architectures and IT control challenges. CIOs consistently list security concerns as their main impediment when considering cloud computing services, but concerns are increasingly overridden by the economic and flexibility benefits that cloud delivers.

With these three shifts adding even more complexity to the security matrix, a growing number of CISOs and CIOs are rethinking their security strategy and moving to a new foundation: desktop virtualization. With desktop virtualization, the software elements that normally reside on an individual's PC or other client device are instead run and managed centrally in the datacenter (or cloud) on server-based virtual machines. By centralizing Windows applications and associated data and by closely controlling access to them, IT improves information security control as well as overall application and desktop management. Further, organizations can sponsor initiatives that bring significant new opportunities for business growth.

Security demands drive desktop virtualization adoption

As security becomes more challenging, organizations are seeking new ways to maintain data protection and access control wherever people work, on whatever devices. In the words of Gartner, “Organizations are struggling with the cost and complexity of provisioning and supporting physical desktop and laptop computers. At the same time, employees are demanding support for new consumer devices, access from
home offices, roaming between locations and devices, and the enabling of limited access by partners using their own devices. Virtual desktop technologies are being deployed to address these needs. An industry consensus is growing around the effectiveness of desktop virtualization to address this challenge.

Market analyst Ogren corroborates this trend. “I’ve seen a huge increase in the adoption of desktop virtualization and Citrix: secure by design

Citrix has been providing information security solutions since its founding in 1989. Today, Citrix combines virtualization, mobility, networking and cloud computing technologies to deliver a full portfolio of offerings that enable IT to deliver on-demand applications, desktops and data to any user on any device with the best performance, security and efficiency. 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.

The Citrix product portfolio is anchored by Citrix XenDesktop. By leveraging its integral Citrix FlexCast delivery technology, XenDesktop allows IT departments to deliver every type of virtual desktop, hosted or local, optimized to meet the performance, security and mobility requirements of each individual user. FlexCast delivery scenarios include:

- **Hosted shared**: Central servers host a core set of standard applications for task workers, with limited personalization allowed.
- **Hosted virtual desktop infrastructure (VDI)**: The entire desktop environment (applications, data, user settings) runs on server-based virtual machines, with only screen images, mouse clicks and keystrokes transmitted between the hosted desktop and the client device.
- **Local virtual machine desktops**: Encrypted data can be sent to client devices for disconnected work, then automatically resynchronized with the central data store upon reconnection.
- **On-demand applications**: Specific client applications are hosted and run centrally, or streamed to client devices for local execution.

A number of other Citrix products support XenDesktop in delivery of desktop virtualization:

- **Citrix Receiver** is client-based software that allows Windows or Macintosh PCs, as well as iPad, Android and Windows tablets, to interoperate with centralized servers for XenDesktop and Citrix XenApp, the Citrix offering for application virtualization.
- **Citrix XenClient** is client virtualization software that enables users to create and run multiple secure virtual desktops on a single PC. An enhanced version, XenClient XT, further leverages Windows desktops that have Intel vPro technology, and is designed to serve in multilevel secure environments with the most extreme isolation, security and performance requirements.
- **Citrix XenMobile** enterprise mobility management software provides complete protection for mobile applications and data, and ensures end-to-end security and compliance. IT gains identity-based provisioning and control of apps, data and devices, automatic account de-provisioning for terminated users and selective wipe of lost devices.
- **Citrix NetScaler Gateway** is a highly scalable SSL VPN that can give thousands of users secure access to centrally hosted applications and data, whether in enterprise datacenters or in private or public clouds.
- **Citrix NetScaler** accelerates, optimizes and secures the delivery of applications. Offered as a hardware-based network appliance and as a software-based virtual appliance, NetScaler integrates an application firewall that protects applications and services from attack. NetScaler also enables the secure extension of the datacenter to a public cloud infrastructure, and provides a single point of control for all applications, including cloud-based services.

All Citrix products are built to be secure by design. This means customers get security as an inherent attribute of desktop virtualization deployments, regardless of which desktop delivery model they use.

---

1 Gartner, Peer Practices: Security Impacts and Benefits for Virtual Desktop Projects, September 2012
virtualization,” he says. This growth is occurring in most industry sectors, with financial services, healthcare, government, and education being among the most active, according to Ogren. “Virtually every Fortune 1000 company I talk to is leveraging desktop virtualization to reduce complexity and the data security issues of mobile devices, and the number one driver for implementing desktop virtualization for a mobile workforce is absolutely security.”

While desktop virtualization can support offline use by encrypting and isolating Windows applications and associated data on the client device, much of the technology’s security cachet comes from its ability to centralize enterprise applications and deliver them securely to any device. “We’ve let distributed computing expand beyond control,” notes Kurt Roemer, Chief Security Strategist at Citrix. “With distributed computing, you have no idea what sensitive data is on somebody’s laptop, tablet or smartphone, so you have to manage every device as if it has sensitive data.”

By giving IT the ability to keep sensitive information in the datacenter, as well as the means to control access to Windows applications and data at a very granular level, desktop virtualization can eliminate this broadly recognized downside to distributed computing. “Data owners can ensure consistency, availability, backup, and disaster recovery, eliminating the perceived default need for end-point storage of sensitive data,” Roemer explains.

Citrix, the leading provider of virtualization solutions, has been solving customer challenges around delivering applications—including those that handle complex and sensitive data—to a distributed workforce for more than 20 years and for more than 260,000 customers. With the introduction of desktop virtualization technology and the need to meet heightened information security challenges, it is no surprise that many of the world’s leading corporations, educational institutions and government entities are now turning to Citrix to meet evolving information security needs.

Among the many companies taking advantage of desktop virtualization benefits is Clark Builders. The company performs commercial, institutional and industrial construction throughout Canada. Security at the widely spread, often isolated locations was a particular concern for Clark Builders. At one job site, burglars broke in and stole two computers. “Two years ago that would have been a major crisis, because of the sensitive and competitive information that could be compromised,” said Dean Doige, chief information officer at Clark Builders. “Now, with information centrally stored and protected, data is completely secure at all times, with the only loss being $1,000 worth of computer equipment, not our intellectual property.”

Bolstering security without hindering people or the business
Desktop virtualization has been an eye-opener for the world of information security, because it means IT can easily increase security without imposing undue burdens on the business. Indeed, desktop virtualization can simplify the jobs of IT administrators and position IT as a strategic enabler of business growth. “Even though it’s our mission to provide cutting-edge security, we also want to enable the business, not hinder it,” says Mike Emerson, senior director of infrastructure services at Citrix, expressing an objective shared by most CISOs and CIOs.

Of the many benefits desktop virtualization affords, a fundamental security benefit is the technology’s ability to bring client applications and associated enterprise data back into the datacenter. In effect, desktop virtualization counters the risks of data distribution and possible loss, tampering and corruption by delivering Windows applications and desktops on-demand to any worker, anywhere on any device while all the management is handled in the datacenter with complete IT control and visibility.

For Citrix customers, this centralization allows IT to implement password control, multifactor authentication and other techniques to ensure people can only access information and other business resources appropriate to their roles. It also allows Citrix customers to establish policies that control the level of access granted from different devices, locations or networks. Desktop virtualization can leverage Active Directory or other directory data to automatically determine and assign the proper access rights. In addition, with Windows applications centralized, administrators can easily manage, support and upgrade applications and apply security patches to ensure that every user is working with the most current and secure software available.

“Keeping endpoint applications and operating systems patched and up-to-date is daunting, but it’s extremely important for us and for any organization,” says Emerson. “IT organizations would often take something down to patch it rather than leaving it vulnerable to hacking.” Desktop virtualization makes the
update and patching process—an onerous and tedious undertaking involving hundreds or thousands of distributed PCs—a much more straightforward and effective procedure, Emerson says.

Virtualized desktop environments can also optionally be set up to counter the introduction of viruses or other malware during any user session. In this model, each time users log off, their virtual desktops are refreshed back to the initial template. When the users log back on to their virtual desktops, they see a clean environment derived from the base template.

The elevated level of control desktop virtualization offers provides significant business value to another Citrix customer, Budd Van Lines. The company provides executive relocation services to streamline the process of moving one or many corporate employees from one location to another. “Citrix desktop virtualization lets me lock down desktops, eliminate CD drives, disallow employees from installing applications and prevent viruses so every worker’s device is completely secure,” says Doug Soltesz, vice president of information systems and technology at Budd Van Lines.

Desktop virtualization also dramatically reduces the challenges associated with supporting a diverse set of enterprise and personally owned client devices. Devices of all major brands and types can be easily equipped with client-based software, part of the Citrix desktop virtualization solution, that ensures the devices have secure access to centralized Windows applications and desktops. Applications and associated data are either stored centrally at all times and protected during transmission, or if selectively distributed to client devices, are encrypted and isolated when stored on the device. IT doesn’t need to worry about data exposure or pilferage if devices are lost or stolen, and can automatically resynchronize data when the client devices reconnect to the centralized data stores. Citrix also provides complementary enterprise mobility management capabilities to safeguard and partition business apps and data accessed on mobile devices.

A partner ecosystem for comprehensive information security solutions

Citrix offers an extensive portfolio of desktop, mobility, collaboration, networking and cloud products that can greatly simplify the way enterprises deliver IT services. In conjunction with its technology partners, Citrix is changing the way people work by delivering applications and data and desktops whenever and wherever they’re needed to support the business.

The Citrix Ready program leverages industry-leading alliances across the Citrix partner ecosystem to meet a wide variety customer needs, and currently incorporates over 750 partners who have demonstrated more than 24,000 product verifications. 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 information assets:

- **Identity management and authentication**: Products in this category not only help IT administrators reduce risk and reduce help desk calls, they allow employees greater mobility, secure remote access, and simplified login experiences such as single sign on.
- **Malware and attack prevention**: A broad collection of products that not only counter malware and other attacks, but also help companies meet compliance and regulatory requirements.
- **Data protection and compliance**: These products are often complementary to the malware and attack prevention category, and also ensure compliance and regulatory demands by protecting against data corruption, misuse or loss.
- **Cloud security-as-a-service**: Products here include both cloud-based security services offered as subscription-based services, as well as products designed to ensure security within public and private clouds.

With its industry-leading suite of desktop virtualization products and technologies, Citrix can deliver the foundation on which corporations, healthcare providers, educational institutions, governments and other organizations can secure their data and applications in a highly automated, centralized, cost-effective and nonintrusive fashion. And, in collaboration with its many partners, Citrix can help customers address virtually every information security requirement and objective.
With Windows applications fully under IT control, administrators can monitor and log all data access events, both to identify potential threats and breaches and to meet the data protection, privacy and reporting requirements of regulations such as Sarbanes-Oxley, PCI DSS, HIPAA and the E.U. Data Privacy Directive. Application centralization enables organizations to adhere to mandates for personal and other sensitive data to remain within geographical boundaries, by centralizing control and automating secure access within defined boundaries.

The centralized management enabled by desktop virtualization makes it much more straightforward for IT to provision new employees, modify their access rights as appropriate during the course of their employment based on changes to roles, and immediately deprovision their access rights when they leave the company. The same granular control can also be applied when granting and removing access to outside contractors, and in instances when a device may have been lost or stolen—where IT wants to prevent the missing device from accessing business resources.

One other critical benefit—business continuity—flows directly from desktop virtualization. Once applications and desktop infrastructure are centralized, people can access these resources even during a business disruption, whether stuck at home in a snowstorm, dislocated during a natural disaster such as a hurricane or earthquake, or simply unable to reach the office or work site for some other reason. Should the person’s normal client device be damaged or unavailable, they can use another device (personal, shared, newly purchased, etc.) to gain immediate access to their business applications. Additionally, should the datacenter facility face a disruption, critical applications and desktops can be easily transferred to other servers or if needed to a backup facility, then securely accessed by the distributed worker base.

“When roads close or power goes down, people can work remotely from home, and we still have complete control and security over the resources they access,” says Soltesz at Budd Van Lines.

While all of these benefits of desktop virtualization help CISOs and CIOs and boost business productivity, the technology also pays dividends for employees, contractors and other workers, who no longer have to keep track of multiple passwords and access methods for different corporate and cloud computing resources. For example, passing through a single Citrix authentication and authorization engine allows them to reach their desktop and all of the applications and data for which they’re approved with a single sign on. Mobile device and application management technologies help IT provide simple, secure access to apps and data across mobile devices.

Companies with desktop virtualization in place can also more easily support BYOD strategies, which are increasingly popular as the number of tablet and smartphone users grows. Allowing employees—and contractors—to use their own devices has the added benefit of reducing the IT budget, since the company doesn’t need to purchase client hardware for these workers. And people quickly come to appreciate the anywhere, anytime, any device access to their work environment.

Perhaps most important from the workers’ perspective, “Desktop virtualization removes the need for every consumer to be their own IT manager and their own security officer,” says Roemer. “By automating data protection and freeing people from mundane and time-consuming data management responsibilities, desktop virtualization provides for greater productivity and happier users.”

Desktop virtualization as the foundation for information security
For many organizations, desktop virtualization has become an essential foundation for a layered information security strategy. Any such strategy must include a careful assessment of risk, followed by a cost/benefit analysis of how to best manage risk while supporting broader enterprise objectives. Comprehensive information-security solutions entail a mix of technologies, processes and training programs, and also require administrative awareness that the matrix of security threats and challenges is a constantly moving target.

Within this environment of evolving technologies, changing worker demographics, pressing competitive demands and escalating security challenges, desktop virtualization has emerged as a star. Desktop virtualization is rapidly assuming a central operational and security role. Given its broad portfolio of mature products and solutions in this area, Citrix is the vendor best positioned to support its growing customer base with desktop virtualization solutions. Products and solutions in this area, Citrix is the vendor best positioned to support its growing customer base with desktop virtualization solutions.