Refactoring sensitive data access: the benefits of desktop virtualization for security

A secure-by-design strategy to regain control over data and applications
Executive summary

Enterprises of all types and sizes, from startups to global businesses to government agencies and nonprofit institutions, have unprecedented opportunities to increase agility and productivity through strategies like cloud computing, workshifting and the consumerization of IT. First, though, they must find a way to enable these initiatives without compromising security. These trends call for a new approach to information security to meet the data protection, privacy, compliance and usability challenges and requirements of the modern era.

This paper presents a secure-by-design IT strategy based on desktop virtualization, an approach which provides both information security and optimal agility to respond to changing business needs, project requirements and market opportunities. Providing strict yet flexible control over access to enterprise information and reliable endpoint security while reducing costs through simplified management, desktop virtualization is rapidly becoming a foundational element of the security strategy for organizations of all kinds.

Introduction

With more threat vectors delivering increasingly serious threats, many enterprises, organizations and government agencies can feel as if they are under constant attack. Meanwhile, their business models, work practices and computing environments have evolved far beyond the relatively standard, predictable scenarios for which legacy access control systems and risk management strategies were designed—making organizations more vulnerable to threats than ever.

With traditional security methods strained to the breaking point, IT faces a choice: Either tighten access to the point where a worker's productivity is hindered, or loosen security policies to an unacceptable level of risk. Many IT organizations believe that security requires only the first approach, enforcing strict barriers to entry. But when access is unduly limited or cumbersome, worker productivity and business agility suffer. At the same time, methods that treat access as an all-or-nothing proposition lack the granularity and flexibility to accommodate frequently changing work scenarios, as well as the data protection, retention, privacy and compliance needs of the modern organization. Access must be specifically tuned to the sensitivity of the data being accessed and always commensurate with risk.

Desktop virtualization enables organizations to transform their security policies to focus on access to applications and data rather than just the network or the endpoint. A comprehensive secure-by-design approach incorporates several essential enabling factors:

- Data never leaves the datacenter in unencrypted form and if needed at the endpoint, remains encrypted.
- All communications are enabled to utilize a secured connection.
- Access to data and applications is entirely policy-driven and access can be revoked instantly and remotely at any time—even for use of a single application.
• Endpoint evaluation and user authentication occurs prior to entering the enterprise environment.
• Granular policy controls and built-in access monitoring, logging and auditing support compliance.

The security benefits of desktop virtualization are complemented by the inherent simplicity of its centralized architecture, which simplifies management and reduces cost. IT can centrally configure, store and maintain a single image for each application, regardless of the diversity of user endpoint devices and operating systems in the environment. New applications, upgrades, and patches need only be implemented and tested once. A simple re-publication of the updated resources then makes them available to users whenever they start their next session. User support becomes much simpler as well: IT can simply revert a worker’s virtual desktop to a previously known, “good” state to eliminate any problems that may have arisen. Taken as a whole, simplified application and desktop management can reduce TCO.

The following sections explore in depth the use of desktop virtualization as the foundation of information security, including access control and endpoint security for both online and offline users. Discussions of use case scenarios, features of the Citrix desktop virtualization solution and integrated partner technologies provide insight and guidance for leveraging this strategy within your own organization.

Desktop virtualization: anywhere, anytime access to IT resources—with full control and visibility

How do you develop a system that enables a worker to perform work while limiting unauthorized access, distribution or review of content? The answer is desktop virtualization, enabled by Citrix XenDesktop™. Desktop virtualization enables IT to circumvent physical deployment of desktops, applications and local data storage by isolating or abstracting full desktops and applications on the host server and then delivering on-demand only the resources required by the worker. By dynamically assembling these components in real time, user profiles and policy controls determine what can be accessed from where, on what device and over which network. The worker gains access through an authenticated network login to connect with a “picture” of the desktop or application; only this representation of the content is transmitted over the network, allowing IT to retain control of the content. In cases where data needs to be stored locally due to application requirements or offline use, it can be delivered in encrypted form into a fully isolated vault. The enterprise desktop and/or applications are fully segregated from any local user OS, registry, or applications and data, allowing IT to define required interaction and deny prohibited interaction.
On-demand applications

On-demand applications, a key component of desktop virtualization, streamlines security by leveraging application delivery – rather than deployment - to support compliance, data protection and security objectives. On-demand applications are created as a single application image in the datacenter, then delivered virtually and physically to devices and desktops, eliminating the need to install and maintain a separate instance of the application for each device. The end user receives only what’s needed for interaction with the application when, where and while it is needed, while the application and all of its associated data are safely stored in the datacenter under complete enterprise control. For offline use cases, or applications requiring local storage, data is encrypted on the endpoint.

With applications secured in the datacenter and not scattered throughout the enterprise, it is easier and more cost-effective to manage desktops, applications and their related data. Required changes result in dynamic updates to each session, ensuring all applications, security patches and updates are current. Through a single point of control, IT can establish policy-based controls to manage user access to particular applications dependent on their location, the device they are logging in from, the time of day or from which network they are accessing the datacenter.

The underlying premise of on-demand application delivery is the separation of the use of the application from where it lives, enabling the enterprise to house and protect sensitive information without undue influence of variables such as network conditions or end-user computing devices. While some use cases will continue to require offline application access or local data storage, for the vast majority of workers their physical location or choice of device is rendered irrelevant. On the other hand, with application deployment applications and their data live on an individual device, which is much more difficult to continuously secure. By implementing on-demand application delivery with desktop virtualization, the enterprise can focus primarily on fortifying security efforts at the datacenter, where security fixes and access policies are quickly and easily implemented for the entire organization.

The right desktop virtualization solution provides great insight into user activity to support the intelligent use of policy controls based on real-life scenarios and not generalized network use. Built-in endpoint scans and policy controls take into account each user’s role, device characteristics, location and network conditions to determine which applications and data they are authorized to access. These dynamic attributes also define where users may store, copy and print sensitive information. Such strong data and application security measures decrease the potential for inappropriate exposure of data, sensitive information and intellectual property, enabling the enterprise to have full control of the application and the content accessed at all times.

Both virtualized desktops and applications can be delivered from public clouds as well as private clouds. Citrix provides an on-demand cloud desktop platform that enables IT to transform Windows desktops and applications into an on-demand, cloud-hosted service. The combination of desktop-as-a-service (DaaS) and integrated apps—Windows, web or SaaS—enables cloud providers and IT organizations to deliver an enterprise-class bundle of services with cloud scale economics. Users have access to their
cloud-enabled desktop from any device, anywhere with a consistent, high-definition experience. Organizations that use a public cloud as a secondary datacenter to manage this outsourced infrastructure the same way they would their own datacenter can utilize the Citrix® NetScaler® application delivery controller. NetScaler solutions enable services orchestration, user provisioning, single sign-on and bridging datacenter environments to public clouds.

Security benefits of desktop virtualization: online and offline enterprise control of access and content

Desktop virtualization acts as an abstraction layer between user system and user access, isolating the actual virtualized desktop and application from the user client OS, or allowing the use of a zero client with no OS at all. It remotely displays the representative content of the virtual desktop and each application in an encapsulated, isolated instance, independent of whether the applications are locally executed (streamed apps) or hosted on datacenter server infrastructure. In this sense, desktop and application access security starts with a secure-by-design approach. In most cases, only screen updates, mouse clicks and keystrokes traverse the network, while content remains securely stored in the datacenter. Since no true content is sent to the end user’s device, no data is stored on the device, dramatically reducing the risk of theft, tampering or loss as well as non-compliance with data retention policies. In addition, as the application is executed in the datacenter, consistent access, encryption and logging are available for all applications and centralized patch management ensures that users are all working off of the identical patched and updated version of the applications, with all security controls and policies updated to reflect the most recent threats.

There are inherent security features built into XenDesktop with on-demand apps that enable the enterprise to further restrict the worker’s environment to prevent illegal or non-compliant data movement or storage.

- **One-way copy/paste** – The enterprise can establish policies around how data is transferred (or not transferred) between the virtual application running in the datacenter and the endpoint device. The worker can work in a rich, high-definition virtual environment but is not allowed to transfer data by copying/pasting content from a virtual application to their physical endpoint applications running in the background. Conversely, the enterprise can control copy/paste of content from the physical environment into the virtual environment. These policy-based controls are centrally managed by the IT administrator and cannot be tampered with by the end user.
Peripheral/USB access control – The enterprise can allow USB mass storage devices or other peripherals including non-USB hard drives, audio and microphones to be used in some scenarios, while restricting or disabling their use in other environments as dictated by the organization’s security practices and policies. For example, when connected to a remote enterprise work session, the use of USB devices may be prohibited to ensure content is not exposed to loss or theft. Policies such as read-only access, write access, or no access at all can be set to determine the level of access the user has to a particular application, server or environment. Specific USB device classes and other peripherals can also be allowed or prohibited. With a higher level of control, the enterprise can shut out all USB devices from being used to remove content from the protected environment.

Print control – Application delivery provides the enterprise with a greater level of control over user printing, including:

- Printing turned on or off per application
- Network/local printing control
- Print screen key (or applicable key combinations) control
- Windows 7 snipping tool defeat

Profile management controls – By implementing application delivery architecture, an added security benefit is the ability to control and manage all profile attributes. One such advantage is the ability to allow the user profile information loading to be postponed until the logon process is completed. Once the golden images for desktops and applications have been loaded and security checks have been run, user profile information is loaded and security checked. The user profile can be set to:

- Load settings on-demand
- Pre-cache files of specific sizes (download in background)
- Cache entire profile after logon (download in background)
- Update modified settings to the profile intermittently without requiring logoff

Encrypted data plug-in for offline usage – If locally stored data is necessary to perform one’s workload while offline or while using a device that is not enterprise-owned, the enterprise can consider extending the delivery infrastructure to manage a segregated partition on a disk drive and remotely manage the access to this data. Administrators can encrypt relevant application data in a dedicated workspace, while seamlessly accessing, storing, sharing and transferring data safely from the local endpoint to the enterprise data store.

Partner technologies:
McAfee
McAfee® Management for Optimized Virtual Environments (MOVE) platform, supporting XenDesktop, provides security management tailored to virtualized environments. Rather than running an endpoint security agent in each virtual machine, MOVE AntiVirus delivers a special-purpose virtual appliance that consolidates scanning processes and signature updates outside of the VMs, efficiently protecting all virtualized desktops.

Partner technologies:
Trend Micro
Trend Micro offers a host of security solutions to work in concert with Citrix. Trend Micro provides individuals and organizations of all sizes with smarter security solutions that protect against a wide range of insidious threats and combined attacks including viruses, spam, phishing, spyware, and botnets. Trend Micro develops, delivers, and supports proactive solutions designed to safeguard critical information and protect personal and corporate reputations.
Policy enforcement and compliance
Managing policies and profiles through Active Directory provides a trusted root for compliance and data privacy management benefits. Security controls can be defined and enforced centrally by the enterprise for each individual application to ensure compliance with the full spectrum of legal, industry and corporate mandates. Rich role- and context-based features enable dynamic security for fine-grained control over exactly what users can do with particular data in specific scenarios, while complete logging, reporting, alerting and auditing capabilities help IT maintain and prove compliance.

Secure user access
The security inherent in desktop virtualization is complemented by another key element of the Citrix desktop virtualization solution: SSL VPN access via Citrix Access Gateway™. Used with XenDesktop, Access Gateway provides secure access for both virtual desktops and applications through a highly secure, hardened appliance. Access Gateway gives IT a single point of granular control to enforce security policies in a uniform manner no matter how and by whom desktops and applications are accessed. Granting the appropriate granular access to resources instantly for a new worker is very simple, as is shutting off access to applications or desktops when an employee departs, a contractor transfers projects or a device is reported lost or stolen, to reduce the risk of data loss and unauthorized or inappropriate access to enterprise data.

Securing the endpoint
Some projects and collaborative environments require the use of local endpoint resources to support demanding applications or offline system usage. In some cases, users may need to access enterprise resources from endpoint devices that are managed and owned by other organizations or by the workers themselves. From the organization’s perspective, these unmanaged client systems are the highest risk points, presenting security concerns such as:

- How can IT trust a non-owned/managed endpoint device that accesses the datacenter?
- How can the organization maintain control over client-side applications and data?
- What can be done to prevent users from being able to save data locally via client drive mapping and special folder redirection?
- What happens to locally stored data when the client system disconnects from the datacenter?
- Will contractors and external organizations expose application and data risks?
- Will lost or stolen devices expose locally stored data?
- How can IT regain control of data upon worker separation/end of project?

Partner technologies:
RSA
The RSA solution offers seamless data protection for both virtual and physical infrastructure and includes comprehensive tokenless and token passed authentication on XenDesktop, Citrix Access Gateway, Citrix Receiver and NetScaler. The RSA Data Loss Prevention (DLP) Suite enables organizations to discover and classify their sensitive data, educate end users to ensure data is handled appropriately, and report on risk reduction and progress towards policy objectives.

Partner technologies:
RSA
The RSA solution offers seamless data protection for both virtual and physical infrastructure and includes comprehensive tokenless and token passed authentication on XenDesktop, Citrix Access Gateway, Citrix Receiver and NetScaler. The RSA Data Loss Prevention (DLP) Suite enables organizations to discover and classify their sensitive data, educate end users to ensure data is handled appropriately, and report on risk reduction and progress towards policy objectives.
Citrix desktop virtualization offers several ways to secure data on the endpoint to ensure that offline use and local data storage do not create information security vulnerabilities.

**Local safe zone**

How does IT protect the information and applications accessed from these unmanaged clients without making computing difficult to use or otherwise negatively impact the work at hand?

- Virtualize the applications and information so that all processing happens in the datacenter.
- Implement centralized policies to prevent access to client-side storage (local drives, USB storage) and printers.
- Control data access from unmanaged devices.

For data and applications that have to exist on the endpoint system, it’s not feasible to encrypt and attempt to manage the entire hard drive of a system the enterprise does not own. What is feasible, however, is to encrypt only the data accessed in the enterprise datacenter, creating a managed vault on the client system. Citrix XenVault™ does just that, creating an encrypted data “safe zone” for the applications and information owned by the enterprise, delivered via XenDesktop on-demand apps or Microsoft App-V application virtualization.

XenVault extends the enterprise’s security perimeter to the unmanaged endpoint system with:

- AES-256 level encryption of data for the encrypted library and drive on Windows 7 endpoints
- Prevention of the organization’s information from being copied outside the safe zone to another directory on the endpoint system or the external organization’s network and vice versa
- Secure offline access to safe zone when not connected to the enterprise
- Central configuration, deployment and management
  - If the user logs in through Citrix Receiver™, IT can remotely lock and wipe encrypted data on the local device in cases of system loss or user separation (access to enterprise information no longer required)
  - Control which applications are allowed access to encrypted data
  - Advanced protection with safe zone password complexity policies, password reset and recovery
- Transparency to users when accessing, storing and sharing application virtualization data, minimizing the possibility that the user will attempt to work around protective measures and increase the risk to the enterprise’s information
Bare metal hypervisor

Client-side, bare metal hypervisor virtualization represents the next generation of desktop computing. The ability to leverage the power of both hardware and software to provide multiple instances of a full OS workload from the same device, while enabling the enterprise to have full control and awareness of the platform, provides for the richest security platform. The use of a Type 1 hypervisor offers key advantages for security, such as:

- No OS underneath hypervisor to be compromised and maintained
- Enhanced isolation between desktop VMs
- Hardware-enforced security measures
- Direct access to underlying graphics subsystem hardware to support graphically intensive applications

Enterprises must support a wide variety of user, business or project needs and must be flexible enough to support even the most demanding and unique requirements presented. To adequately support the enterprise, IT must be flexible enough to support even the most taxing and demanding graphics or computationally challenging applications, including providing full access to the endpoint’s local hardware such as the GPU, or to peripherals. Each worker may be tasked with supporting multiple special programs that require full separation of workloads while enabling collaborative environments. In scenarios such as these, a client-side bare metal hypervisor provides the information protection needed to fully extend the attributes of datacenter-managed desktop virtualization with end-to-end trust.

Enhancing endpoint security with the Citrix XenClient bare metal hypervisor

Citrix XenClient™ protects information and applications on desktop VMs running on the endpoint with the ability to reboot to a clean “gold disk” image, in a similar manner to how Citrix provisioning services can boot all enterprise datacenter desktop and server VMs from a single, read-only image. In the event that a desktop VM is compromised, the desktop can be rebooted from a known, pristine image.

The XenClient architecture includes centralized management of client and desktop VMs to enforce organization security policies per desktop VM even on remote or disconnected clients. This centralized management also includes the ability to:

- Transparently patch/update all desktop VMs on all clients to minimize exploits by securely synchronizing them with datacenter-hosted images
- Centrally create and manage policies for desktop VM access to USB and other types of peripherals to deny access to USB storage devices and DVD drives to prevent the loss or theft of data via these routes
- Protect all locally created and stored information by transparently backing up all data back to the organization’s datacenter
XenClient allows the consolidation of multiple physical Windows desktop systems onto a single physical desktop computer. Each physical Windows machine becomes a local, virtual desktop sharing the resources of a single physical system, enabling users to run virtual desktops in different security domains on the same system with complete, secure isolation for each. A thin, next-generation Type 1 client hypervisor with hardened components and network isolation Service VMs allows multiple security domains and multiple networks on the same system for the highest level of desktop isolation. High performance disk encryption accelerated with Intel AES-NI offloads encryption to the hardware platform while protecting the worker experience. High levels of network isolation both on and off the box, complemented by encapsulated, unique, encrypted network streams for each virtual desktop prevent problems from spreading and allow use of a single physical network connection to the desktop. Virtual desktops can only connect to authorized backend infrastructure and communication is encrypted with VPN clients so that VMs are completely isolated from cyber-attack.

XenClient XT is an enhanced version of XenClient that further augments endpoint security to protect desktop VMs through the use of Xen Security Modules to harden the hypervisor platform and enable other advanced security features. The Xen Security Modules are used for low-level isolation enforcement and to control fine-grained privileges for Service VMs. Service VMs are used to offload networking from the hypervisor for further isolation. The network isolation Service VM protects critical elements of the platform from network-based attacks, plus it delivers high levels of network isolation both on and off the box and can encapsulate unique encrypted network streams for each virtual desktop. The Service VM architecture also enables the offloading of certain management functions, including security management functions from VMs to a dedicated, centrally managed security appliance, improving performance of virtual desktops while maintaining endpoint system security.

By leveraging an end-to-end trusted ecosystem architecture, the enterprise can garner greater control over its content, its distribution and overall protection without compromising performance. With a fully managed endpoint workload, built and updated centrally by the enterprise, as well as managed applications and virtual workloads, the enterprise gains full control of every element of its environment.
Use case examples

**Enterprise**

**Embrace consumerization** by maintaining effective security across computers, smartphones, tablets and other devices of any make and operating system.

**Enable secure mobility** by allowing secure access from any location, over any network connection. No data resides in unencrypted form on the endpoint, eliminating the risk that data will be compromised if an endpoint is lost or stolen.

**Empower contractors** such as outsourcing providers and contingent workers with direct access to apps and data via non-persistent virtual desktops while maintaining full control over access. Access to virtual desktops can be turned off instantly at any time, such as when an engagement has been completed.

**Control privileged user access** by providing isolated, authorized access to resources by administrative users and logging administrative activity.

**Government**

**Support secure collaboration** by enabling members of different organizations to share data without the risk of information leakage to unauthorized users. A single endpoint device can run both a normal work desktop and a separate desktop for collaboration in full isolation from each other.

**Isolate disparate communities** by establishing dedicated virtual desktops secured through centrally managed policies which control who users can communicate and share data with, and how.

**Establish a trusted platform** by managing policies and profiles through Active Directory, leveraging a known trusted delivery protocol and creating a more trusted backend environment with dedicated VPN connections available per virtual machine, per workload and per user.

**Control privileged user access** by providing isolated, authorized access to resources by administrative users and logging administrative activity.

### Conclusion

Today’s enterprises need to support strategies like workshifting, consumerization and cloud computing while meeting the requirements of workers of all types. To meet these requirements while achieving effective data protection, ensuring data privacy, protecting intellectual property and maintaining compliance, IT must look at a layered defense approach. Legacy security controls are set for failure—it’s time to refactor sensitive data and information access to reflect today’s realities. With desktop virtualization, IT can manage risk while providing optimal flexibility to both workers and the organization by delivering resources on-demand according to comprehensive, granular policies based on the worker’s specific scenario, work requirements and security profile. This multi-tiered approach for delivering desktops, applications or entire workloads frees the enterprise from the compromised productivity and distractions associated with legacy security methods.

### Security delivers value

The following strategies evolve the value of security to the organization:

- **Prevent Loss** – Keep sensitive data in a vault
- **Optimize Productivity** – Maximize security quality of experience
- **Facilitate Workshifting** – Enable secure follow-me services
- **Maximize TCO** – Match service levels to data sensitivity
- **Actively Manage Risk** – Automate lifecycle orchestration
- **Evolve IT** – The “Innovation Services” department
Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2010 was $1.87 billion.

©2011 Citrix Systems, Inc. All rights reserved. Citrix®, Citrix XenDesktop™, Citrix XenApp™, Citrix XenClient™, Citrix GoToMeeting® and Citrix GoToAssist® are registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.