Protect sensitive data on laptops—even for disconnected users

Use local virtual desktops to secure and control information no matter where—or whether—users connect to the network
Executive Summary

Protecting and controlling data and other IT assets and ensuring compliance and policy enforcement within the enterprise network are challenging enough, but the difficulty increases significantly when users take laptops beyond the network and connect remotely—or even work offline. The problem becomes even more complex when workers use the same laptop for personal as well as business use, as they often do. As organizations seek to increase user mobility and support strategies such as workshifting (the concept associated with moving work to the optimal time and place), solving the mobile security challenge has become a critical focus for IT. Client virtualization offers a solution.

Client virtualization solutions based on local virtual desktop technology, such as Citrix® XenClient™, enable organizations to extend the security benefits of desktop virtualization to mobile users by maintaining full security and control over the applications and data they access. IT can enforce regulatory, policy and license compliance, protect business data from theft, isolate the spread of malware, prevent data loss from user error, enforce data protection policies and enable self-service recovery for every worker. Laptops also become easier to manage, helping IT reduce desktop costs and increase total value of ownership while enhancing employee productivity for the business.

This white paper presents the benefits of a security strategy for laptops based on local virtual desktops, including the ability to support workers in public sector environments with extreme isolation, security and performance requirements. Use cases from the energy, healthcare and public sectors illustrate the effectiveness of this strategy for meeting real-world security requirements.

The challenges of enabling mobile productivity

Mobile computing is a major component of today’s IT infrastructures. Laptops aren’t just for road warriors anymore; as organizations embrace workshifting, a typical enterprise workforce may include part-timers, contractors, consultants, partners and outsourcers as well as full-time employees. They may work in headquarters or branch offices; at customer, partner and vendor sites; or from home. These workers use a wide range of access methods and devices to access corporate data and applications, from a corporate desktop on the LAN to a laptop in a remote location via public hotspot. Wherever and however they connect—and even while disconnected—they expect computing performance, mobility and reliability without compromises.
However, mobility poses several challenges for IT and the business.

- Traditional PC technologies can provide mobility and flexibility for users, or control and security for IT, but usually not both. IT departments need a cost-effective way to manage laptops centrally, even as these devices travel beyond the enterprise network. The same mobility that makes laptops so useful for workers poses some of the hardest challenges for IT: how can administrators manage desktops, enforce policies and maintain compliance across widely dispersed, often disconnected devices? Laptops have traditionally posed one of the toughest endpoint security problems in the enterprise, and even modern endpoint strategies based on virtual desktop infrastructure (VDI) may not fully address all security requirements of the disconnected user while offering the flexibility and performance that workers need. What if a laptop is left in a cab or stolen in an airport, and the sensitive information it contains is put at risk? How can IT ensure that remote or mobile users are backing up their data, and how can administrators restore systems remotely following a hardware failure or crash?

- Employees often use corporate-assigned laptops to conduct personal computing activities such as checking personal mail, installing games, downloading photos and music files, participating in social media—the list goes on. Unless IT has an effective way to enforce the separation of these business and personal domains, the enterprise data on the laptop remains at risk of theft, malware or social engineering schemes. The software conflicts such personal activities can introduce can also impair the performance of business applications or crash the machine entirely, leaving users unproductive when they’re far from IT support resources.

- As organizations work to protect the data on mobile laptops, they also need to find a way to improve worker flexibility by reducing dependence on specific or outdated hardware and device drivers. By upgrading to a new laptop, workers can use the best device for their current needs—but first, IT needs to make this process as seamless and secure as possible.

- Effective backups are essential for ensuring that workers have reliable access to the business-critical data their jobs depend upon. Backup strategies often rely on users to perform certain functions to protect data, such as copying files to network shares or activating a VPN client to allow the backup agent software to send files to a backup server in the corporate datacenter. Not only is it hard to rely on users to perform these actions in a timely manner, but also laptop users often turn off the backup agent software itself in an attempt to improve system performance, leaving their data unprotected. Ideally, corporate data needs to be protected without end user intervention or knowledge.

This increasingly complex and mobile IT environment makes it harder for IT to control and secure corporate data that the workforce relies on. To empower employees for mobile productivity without sacrificing security, IT needs to enforce strict control over the corporate data and IT assets on users’ laptops, prevent policy enforcement and compliance from being compromised and simplify management of users on dispersed, often disconnected, endpoints.
Securing laptops with local virtual desktops

Desktop virtualization is already a core element of the security strategy at many organizations because it provides a way to centralize the control, management and delivery of data, applications and desktops. Local virtual desktops extend similar security benefits to laptops, giving IT a centralized delivery and management platform to enable a more comprehensive and efficient approach to security, policy enforcement, data protection and end user self-service capabilities.

XenClient, based on the Type 1 Xen® hypervisor technology, provides comprehensive delivery of a complete desktop to a device for local execution. XenClient enables businesses to virtualize worker desktops and deliver them to run locally on the employee’s laptop. A single device can run multiple virtual desktops for instant, simultaneous access to a variety of environments: for example, a locked-down business desktop, a personal desktop, a test and development environment and a temporary environment for contingent workers. When the 3D feature is enabled by XenClient, a desktop can be enhanced with high-quality video and graphics. XenClient protects the data and applications running in virtual desktops on client endpoints by providing the ability to reboot to a pristine “gold disk” corporate image. In the event a virtual desktop is compromised by malware such as a root kit, the virtual desktop can be rebooted to start from the original, clean image.

Unlike Type 2 hypervisors that typically lack centralized management capabilities, XenClient provides full synchronization between local virtual desktops and the datacenter via the Citrix® Synchronizer for XenClient, the solution’s management server backend. Acting as a centralized delivery and management platform for XenClient users throughout the enterprise, the Synchronizer enables laptops with XenClient to download centrally managed virtual desktops. It also provides full-time backup and recovery through a secure connection whenever the user connects to the Internet and enables IT to define security policies for managed laptops, disable lost or stolen XenClient laptops and restore a user’s virtual desktop on any XenClient laptop.
Citrix XenClient

- Centralized delivery of virtual desktops
- Full-time backup & rapid recovery
- Granular local policy controls & “Kill Pill”

This diagram illustrates the interaction of hardware and software layers with Citrix XenClient, a true Type 1 hypervisor that runs directly on the computer hardware to offer bare-metal performance. Multiple virtual desktops can run on XenClient, including service virtual machines (VMs) that can offload specific management services such as networking and VPN.

For IT, XenClient enables the delivery of well-managed virtual desktops with granular policy control, full isolation and security to protect corporate data. Integrated, automated backup of virtual desktops aids in business continuity planning and disaster recovery.

Virtual desktops can also be moved easily and seamlessly from one laptop to another, freeing IT to choose from a large list of supported off-the-shelf hardware systems from major PC vendors. Workers are provided with the resources they need at any time and in any scenario, whether within the corporate network, connecting remotely or working offline, and can even restore lost or damaged virtual desktops themselves.

Designed to work with industry-leading Citrix® XenDesktop® desktop virtualization solutions as part of the FlexCast™ delivery technology, XenClient is an enterprise-class client virtualization product designed to run on computer hardware for unparalleled flexibility, performance and freedom for users. IT administrators leverage the XenClient backend infrastructure for better management and security policies while enterprises can realize better economics and employee productivity from running multiple virtual computers on a physical machine, leading to protected IT investments and increased Total Value of Ownership for laptops.
Delivering improved security for the business and an optimal experience for mobile workers

XenClient helps IT get control over data and applications on mobile laptops no matter where or how they are used.

- **Centralize management and policy control:** XenClient provides a single, central platform to manage multiple client machines and the virtual desktops that run on top. IT can define and enforce granular security policies on virtual desktops that reside on local, remote or disconnected clients to control exactly what users are allowed to do in specific scenarios. IT can also selectively allow or deny access to USB storage devices, CD/DVD optical media and other peripherals to prevent loss or theft of data in highly secure or regulated environments. Centralized laptop management increases both security and IT efficiency because security updates and patches are applied to the virtual desktop images, which are then synchronized with the virtual desktops on laptops used by workers throughout the organization.

- **Protect enterprise data:** Since the multiple virtual desktops that run on XenClient are completely isolated, the risk of malware’s spreading among virtual desktops is almost non-existent. Client-side virtual machines, including business and user data, can be backed up to the datacenter automatically by policy even while users are remote; SSL ensures full protection of backup data by preventing unauthorized access during data transfer. Remote “kill pill” policy capabilities enable IT to render virtual desktops inaccessible when laptops are lost or stolen to ensure that enterprise data, sensitive information and intellectual property are not compromised.

- **Deploy purpose-build virtual desktops:** IT can create and deliver separate virtual desktops to employees for business and personal use, as well as providing multiple virtual desktops to address different use cases, all on the same laptop. Virtual desktops can also be designed to run for specific lease periods for contractors or interns so that automatic time-out periods enforce policies without human intervention. At the end of the engagement, the virtual desktop automatically becomes inaccessible and inoperative.

- **Improve compliance for mobile laptops:** XenClient helps IT meet corporate and regulatory mandates by providing a way to standardize corporate-defined desktop images can be enforced on every laptop provided to mobile employees across the company. IT can also get reporting on the number of XenClient users and the virtual desktops provided to them.

- **Increase IT flexibility:** Because XenClient runs directly on hardware, there is no need to install additional device drivers, freeing IT from constant updates. Virtual desktops can be moved seamlessly across different laptops, even machines from different vendors, so IT can meet the requirements of individual workers and use cases more easily and efficiently.
For mobile workers, XenClient enables a high-quality user experience in any scenario without compromise.

• **Optimize high-definition graphics:** XenClient provides direct access to a laptop’s graphics subsystem hardware to support graphically intensive applications on virtual desktops. Without the need for an underlying host OS, as is typical for Type 2 hypervisor products, XenClient can deliver high-definition graphics performance for the virtual desktop. XenClient fully supports OpenGL, Microsoft® DirectX® and Windows® Aero® for optimal graphics performance. This provides a rich visual experience that can greatly enhance a customer demo or a mobile worker’s experience with demanding applications.

• **Allow self-service recovery:** By empowering employees with self-help recovery services for their own backed-up virtual desktops, businesses can greatly reduce costly help desk calls while helping workers recover more quickly and easily from hardware failures, damaged laptops or infected virtual machines, even when they are far from the office.

• **Improve stability:** Because a Type 1 hypervisor runs directly on the bare metal of a computer, there is no underlying OS to be compromised, making XenClient more stable than legacy Type 2 hypervisors and less susceptible to any underlying OS problems.

Advanced technologies throughout the XenClient architecture provide the highest levels of security for the organization.

• **Client-side encryption and access control:** Virtual desktops reside in separate, individual VHD files that are fully protected with high-performance AES-XTS disk encryption accelerated with Intel® Advanced Encryption Standard New Instructions (AES-NI) hardware encryption technology. Two-factor authentication technology with password challenge and PIN registration challenge ensures that workers can download and use only the virtual desktops assigned to them. Microsoft® Active Directory® integration unifies user authentication within corporate policy.

**Meeting extreme requirements for isolation, security and performance**

For environments such as government, military, security and intelligence entities that require extreme isolation, XenClient XT, a version of XenClient designed to meet the most demanding security requirements, takes advantage of hardware-assisted security functions built into the latest generation of Intel® Core™ vPro™ processors to protect the integrity of the computer. Beyond the security features in XenClient discussed above, XenClient XT leverages Intel® Trusted Execution Technology for a measured and trusted launch of the client hypervisor at machine boot time to determine whether the hypervisor has been tampered with or malware has been inserted into the hypervisor. A compromised system will either be prevented from booting or will present a warning message to the user as predefined by company policy. The Intel® Trusted Platform Module is used...
to seal the encryption keys of the hypervisor configuration. By using Intel functionalities inherent in the client CPU hardware to offer proof of the XenClient hypervisor’s integrity on every boot of the platform, IT can be confident that if a compromised client system is detected, it will be isolated before the hypervisor can boot up.

In XenClient XT, the networking aspects of the individual virtual desktops can be separated and isolated. Network isolation gives users the highest levels of confidence and trust that their communications on different networks are uncompromised and fully reliable. XenClient XT uses Service VMs to move, separate and isolate the network stack for “out-of-band” management.

Key security features of Intel Core vPro processors leveraged by XenClient XT:

- **Intel Virtualization Technology hardware virtualization support**, which enables OS virtualization and accelerates graphics performance by enabling a virtual machine to gain dedicated access to Intel HD Graphics hardware

- **Intel Trusted Execution Technology**, which enhances security by detecting attempts to compromise system integrity and verifying the integrity of the hypervisor on every boot

- **Intel Advanced Encryption Standard New Instructions**, which implements complex and performance-intensive encryption and decryption steps in hardware to improve performance and minimize user impact

XenClient XT further enhances security for the endpoint by deploying additional Security-Enhanced Linux® (SELinux) and Xen security modules to harden the hypervisor platform. The Xen security modules are used for low-level isolation enforcement and to control the fine-grained privileges for Service VMs, which are separate VMs used to offload and de-privilege services such as networking, VPN and security scanning from the hypervisor for further isolation and to offload the workload to the hardware for better performance. The Service VM architecture in XenClient enables offloading of certain management functions, including networking and security management services, from VMs to dedicated, centrally managed appliances to further improve the performance of virtual desktops while maintaining endpoint security.

**Summary**

Organizations seeking to leverage the business value of increased worker mobility need to make sure the laptops these users carry do not place enterprise information and other IT resources at risk. Local virtual desktops based on XenClient provide an effective and trusted way to maintain security and control over laptops as they travel beyond the enterprise network, even while disconnected. Virtual desktops are created centrally and then delivered securely for execution within client-side VMs. Complete isolation allows multiple virtual desktops, such as dedicated desktops for personal and business use, to run on the same laptop without the risk of conflicts or the spread of malware from one to another. Granular policies, centrally defined and managed, give IT the same level of
control over user activity as for desktop PCs within the network. For users, bare-metal performance and self-service recovery deliver a high-quality experience even for the most demanding applications. Advanced capabilities for network isolation, encryption and access control meet the requirements of extreme security environments. Based on open technologies, XenClient combines a comprehensive approach to laptop security with ample flexibility and free choice over endpoint products.

Combining multiple point solutions can lead to compatibility issues or implementation difficulties. XenClient provides a way to extend the same high level of security across remote and disconnected workers that is maintained within enterprise networks—providing a secure foundation to support a new generation of flexible workforce models.

“Running separate Windows XP and Windows 7 virtual desktops with XenClient on my laptop showed no noticeable differences from running the OS environments on the laptop directly. I am impressed with the performance and ease of use of XenClient and what it can do for any business.”

Erik Gilreath, IT Consultant & System Administrator
Grand Rapids, Michigan

Industry use case: energy

Field engineers and consultants for energy companies often travel internationally to conduct business. The laptops they carry contain CAD programs and design specifications for new power plants—vital intellectual property. To protect the organization, this data must be backed up reliably to the enterprise datacenter and secured on the endpoint to prevent unauthorized access if the laptop is lost or stolen in transit.

XenClient enables IT to encrypt virtual desktops so that unauthorized persons cannot access data. Automated backups are managed by the Synchronizer for XenClient, the solution’s server management component, and delivered via encrypted communication to the enterprise datacenter.

Industry use case: healthcare

Medical field sales representatives and healthcare workers who make home visits use laptops to collect and provide patient information. These mobile users want performance without compromises and need to know that their apps and data will be available when needed. At the same time, the confidential patient data on these laptops must be secured and protected to comply with the Health Insurance Portability and Accountability Act (HIPAA).
XenClient empowers healthcare employees to be mobile and productive when travelling to meet customers and patients, even when disconnected from the network. Automatic, secure backup ensures that patient data will be available when needed, while secure communication and encryption protect this information from compromise. A sandboxed virtual desktop can be set up for field sales reps to conduct product demos without exposing corporate data, e-mail or applications.

Industry use case: public sector

Local, state and federal agencies may require extreme isolation due to the exceptionally confidential information they work with. As a result, users may have to work on multiple, inter-agency networks in the course of business; some agencies even use separate systems for each network, creating complexity for users and the high costs and administrative overhead of a sprawling endpoint environment for IT.

XenClient lets government agencies consolidate multi-level desktops on a single physical computer that can accomplish the work currently done by multiple systems. A hardened hypervisor helps meet the most stringent requirements for security and reliability.

Key takeaways

- Local virtual desktops give IT a way to implement comprehensive and efficient security, policy enforcement, user administration and support for laptops—even for users who work offline.
- Multiple virtual desktops can run on the same laptop in complete isolation to provide instant, simultaneous access to different environments.
- Since XenClient is based on a Type 1 hypervisor, it provides bare-metal performance. The Synchronizer for XenClient enables central security policy enforcement and data backup, as well as the ability to remotely disable lost or stolen XenClient laptops.
- Workers can restore lost or damaged virtual desktops themselves without IT assistance for convenient self-service.
- XenClient XT leverages the security features of the latest Intel® Core™ vPro™ processors to meet the extreme isolation requirements of public sector customers.
- Improved manageability and flexibility help improve IT efficiency, while users receive the high-performance experience they need for optimal productivity.