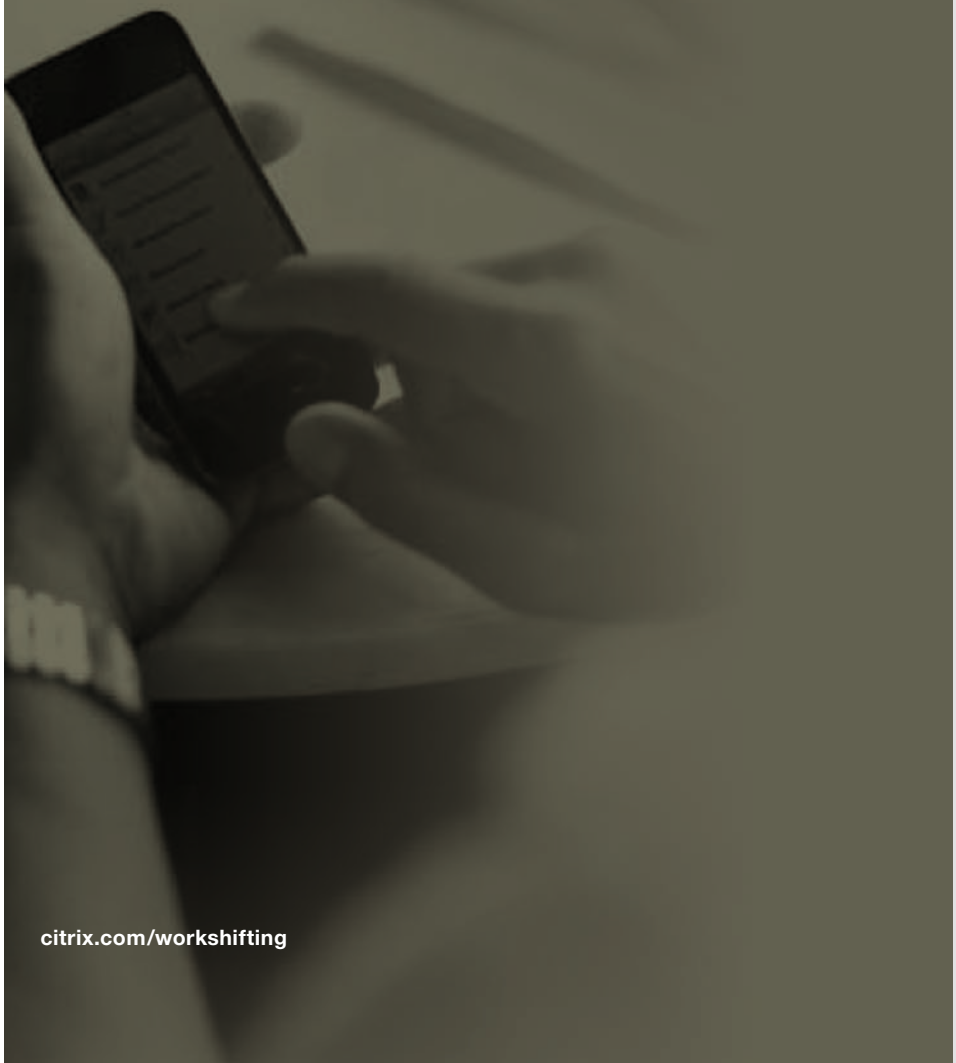
Empowering business mobility through virtualization

A guide to embracing consumerization, BYO and workshifting



CITRIX®

citrix.com/workshifting

Introduction

Organizations that optimize for mobility and architect around services-based computing best position their workforce for the future. For an optimal computing experience, a mobile and services-based design philosophy must balance user experience, total value of ownership (TVO) and governance for protection of valuable information assets.

This paper describes options for a mobile services-focused computing architecture that empowers productivity through workshifting, consumerization and collaboration.

Mobility, workshifting and consumerization

Mobility plays an increasingly important role in today's enterprises. For many types of workers, "always-on and connected" is now a core requirement. E-mail is no longer enough; full productivity depends upon real-time access to applications and files and on the ability to share resources, collaborate or meet from anywhere at any time. Wherever and however they work—in the office, at home or on the road—workers depend upon reliable access to a consistent, high-performance computing experience. At the enterprise level, organizations and processes are being transformed by workshifting, a philosophy of moving work to the optimal location, time and resource.

As workplace mobility increases, many workers now use consumer devices such as smartphones, tablets and laptops to support business productivity—a trend called consumerization. Consumerization often involves the use of the same mobile device for personal and business purposes, as well using worker-owned devices in the enterprise, called bring your own (BYO).

However, escalating mobility has presented many challenges to organizations and information technology (IT) departments, forcing them to rethink traditional methods of providing computing services, ensuring information security and controlling the use of enterprise technologies. The need to manage risk must be balanced with the demand by highly mobile workers for freedom of choice and personal control over their computing experience. An optimized mobile computing experience, defined through an innovative and evolutionary approach to mobility, can enable IT to meet both sets of requirements.

Optimizing for mobility

Mobile productivity depends on a high-quality user experience

Consumers typically select their personal mobile devices based on convenience, cost and coolness. While enterprise priorities and use cases for these devices can be quite different from personal uses, these principles remain important. Even as IT works to ensure the security of enterprise resources and information, these measures must not undermine the convenience and people-centric computing experience that drive much of the value of the latest smartphones, tablets and laptops. This situation calls for a more relevant, less-invasive approach to security than is allowed under traditional IT practices, which must now be updated to support today's more flexible workplace.

The proliferation of mobile devices and the increased risk posed by highly mobile data, apps and hardware would be considered frivolous and reckless by traditional IT project metrics. However, today's mobile users know that the benefits to

Mobility in healthcare

Consider a healthcare example. The healthcare workplace has evolved from the era of single practitioners and paper documentation to a distributed mobile workforce with specialized roles and technologies. While the mission of providing patient care remains the same, it has become more difficult to support due to complexity, slowness, unreliable technologies, increasingly stringent security measures and strict government regulations to ensure patient privacy. Doctors must maintain compliance—and control costs—even as they seek to streamline patient care by using tablet devices that make it simple to access and share complex healthcare information with patients. Specialists often work for several healthcare practices, purchase a personal tablet and demand that IT support it in each disparate workplace. Even in healthcare, mobile computing decisions are often made by the consumer.

productivity, collaboration and the overall computing experience greatly surpass the associated costs and risks. More and more, IT shares this recognition—a reflection in part of the emergence of TVO (total value of ownership) as a more comprehensive and meaningful measurement of the effectiveness of business enablement investments than cost alone. A recent study commissioned by Citrix and conducted by Vanson Bourne, an independent market research company, found that the ability to allow workers to use the device of their choice is the number-one driver for the adoption of a workshifting strategy cited by 1,100 senior IT decision makers at mid-size and large enterprises.

Mobility requires diligence in information governance

Mobility inherently increases risk and challenges the protection of sensitive data. While applications and data are best controlled when they remain in the protective confines of the datacenter, business needs often dictate that they be made available for offline and disconnected usage. Any competent information security professional could find dozens of reasons to say no to increased mobility. The real challenge is finding a way to say *yes*.

To do so, IT needs to leverage new thinking, processes and technology designed explicitly to facilitate mobility while providing an optimal user experience, high TVO and effective information governance.

Taking advantage of mobility while controlling the associated risks	
Say *yes* to consumerization and workshifting	Instead of indiscriminately keeping devices off enterprise networks, allow approved classes of devices to work in policy-authorized situations and allow the controlled distribution of mobile data.
Take advantage of cloud-based apps	Instead of lamenting the use of external and Software-as-a-Service (SaaS) applications, embrace the productivity offered by those applications through automated provisioning and lifecycle management.
Control true risks	Instead of requiring end-to-end ownership, use and manage personally owned computing solutions (spanning from devices to networks and apps) within risk boundaries to optimize productivity and data governance.

Optimizing for mobility to support consumerization, BYO and workshifting

Enabling worker mobility calls for more than just remote access capabilities. To unlock the full business value of consumerization, BYO and workshifting trends, IT must optimize the mobile environment to deliver a superior worker experience, maximum TVO and defensible information governance. These factors are defining characteristics of Citrix virtualization solutions, which include a delivery and services framework to provide end-to-end optimization.

Focus on information governance

Information governance considers all the protective needs of sensitive information in the context of supporting the enterprise and includes regulatory compliance, policy obligations and risk management. Risk recognizes that tradeoffs exist between protecting sensitive information and supporting specific business needs; these opposing demands must be appropriately balanced. As in the healthcare example, information security must be optimized to ensure that the risk to patient care is minimized.

Mobility and Workshifting	Delivery	Services
Receiver GoToMeeting ShareFile XenClient	NetScaler CloudBridge Access Gateway	XenApp XenDesktop CloudGateway XenServer CloudStack
vDisk Storefront	Web App Firewall Cloud Connectors	Cloud Portal

Citrix solution overview

Citrix helps IT get back in the driver's seat, with appropriate control over and superior visibility into people-centric computing, through a model called virtual computing. IT resources are centralized and delivered as a secure, high-definition service that enables users to work whenever, wherever and on whatever device. Citrix® XenDesktop® enables on-demand delivery of virtual desktops and applications to give users unprecedented flexibility and mobility while maintaining security. Citrix® CloudGateway™ simplifies access to the full range of enterprise and cloud-based applications on any device though a unified self-service app store with single sign-on. Citrix® Receiver™ provides access to applications and desktops delivered through XenDesktop and CloudGateway on the widest array of mobile devices. ShareFile integration with Receiver (referred to as follow me data) ensures that critical—even sensitive—data is always available and secured. Simply put, workers can easily access all the resources they need anywhere, on any device, for full productivity.

Mobile workers and IT must share the responsibility for balancing productivity and risk, with IT defining balance through the recommendations in the following table.

Optimizing for mobility: recommendations for IT
1. Enable mobility for workers, apps and data to transform business
2. Keep sensitive data in the datacenter whenever possible
3. Protect distributed mobile data in a follow me data vault
4. Enforce policies specifying what should happen under specific contextual circumstances – not just at logon
5. Control data distribution and usage through policy
6. Personalize the worker experience for optimal productivity
7. Automate both the desired worker experience and data protection needs
8. Enhance ease of use by unifying the management of accounts, passwords and access for all apps, both internal and external

Challenges and Opportunities of Mobility

Mobility brings freedom

Mobile computing frees workers to work and play from anywhere, frees their organizations to leverage the full value of workshifting and frees the enterprise from the constraints of inflexible computing. Through consumerization, mobility brings freedom to personalize your computing experience. Mobility empowers agility, productivity, innovation and work satisfaction. However, some enterprises still see the freedoms of mobility as a threat.

Mobility challenges enterprise architectures

Is the iPad® tablet the enemy? To many IT organizations, iPad tablets and other consumer-grade mobile devices present an untenable threat to network security and control, a threat that unfortunately exists by design. Traditional enterprise networks and security measures were designed around a core assumption: IT maintains full, end-to-end ownership. These traditional architectures required IT to know and approve every device, network, application and usage of computing. In the face of these constraints, though, many workers responded by acquiring their own alternative computing resources, such as personally owned devices, 4G and Wi-Fi networks and rich SaaS applications, all of which bypass IT inflexibility.

Recipe for a failed mobility project
• Use the same stale practices and tools from the past
• Treat all apps and data equally
• Over-concentrate on device security
• Rely on users to accept risks and create policies
• Attempt to manage what you don't own
• Ignore user experience—especially for security

IT organizations that see iPad or Android tablets as the enemy need to realize that the problem isn't the device itself; it's the outdated enterprise computing architecture that fails to support it effectively. The forces of consumerization, mobility and workshifting need to be seen as core design tenets to enable the next era of computing.

Mobility can combine freedom of choice with control

IT can rest assured that freedom of device choice doesn't mean anything goes. Innovations in virtualization provide the control needed to ensure the security of the enterprise as well as the user. Applications and data can be isolated from harm and misuse, and compartmentalized to facilitate delivery, even to an ever-expanding ecosystem of mobile devices. In this way, IT can satisfy enterprise computing and business/worker requirements while streamlining the use of personally owned devices in the enterprise, resulting in optimal productivity, satisfaction/morale, cost and control.

Freedom of choice: the requirements and benefits of mobility	
Requirement	**Benefits**
Location independence	Workshifting, teleworking, business/ workforce continuity
Device independence	Anytime-anywhere productivity, mobile workspaces, bring your own device (BYO)
Personalization	Virtual work styles, profile management, personalization
Collaboration	Virtual teams, global office experience, follow me data
Command and control	Security, compliance, privacy and cost optimization
Orchestration	Policy automation of desired experience and results

Achieving and leveraging the benefits of mobility require an enterprise computing architecture that is both agile and secure. This architecture must provide an appropriate computing experience and transactional integrity; ensure that devices are suitable for the purpose and that their usage is risk-appropriate; and deliver an exceptional experience for all applications, both internal and external.

The wave of change in computing

People are at the center of today's computing experience. However, it hasn't always been this way. In the not-too-distant past, IT controlled what technology was available, maintained end-to-end ownership of the computing environment and called customers users. Over-focusing on technology and under-focusing on the optimal experience, together with traditional IT strategies and methods, often resulted in a miserable and costly computing experience.

Workers have since revolted, bypassing IT to select their own devices, applications and networks, and generally directing their own computing experience. Industry pundits comment that traditional IT has been rendered irrelevant. This seems especially true in light of the mobile devices now overrunning enterprises and frustrating IT departments everywhere.

To thrive in today's era of worker-centric computing, IT needs to manage mobility—but not in the traditional sense.

Managing mobility

To regain control over the enterprise architecture while delivering mobile-enabled computing services, IT needs to manage:

- **Grades of devices** – consumer, enterprise and mission-grade
- **Methods of usage** – online, offline/disconnected and synchronized

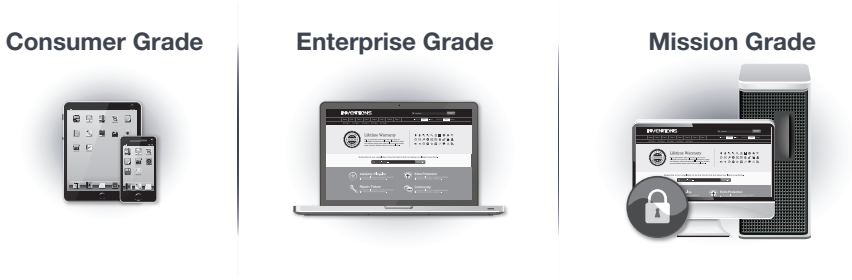
- **Data sensitivity** – public, confidential and restricted material
- **Policy** – rules defining the intersection of devices, usage methods and data sensitivity

Understanding device grades

Consumer-grade devices are designed for home and personal usage and therefore do not natively support enterprise management features. They are typically single-user account devices that are shared among multiple people in a household.

Enterprise-grade devices are designed for enterprise management and support antivirus, patch management, data encryption and other security measures.

Mission-grade devices support extended security measures required for deployment in primarily hostile situations and high-security environments



Methods of usage

Mobile devices will be used in a variety of ways:

- Online usage requires a constant network connection to resources.
- Offline usage allows a worker to be productive while disconnected. When workers need to carry sensitive information with them for offline access, the data must reside in a secure, encrypted vault.
- Synchronized usage ensures data consistency between devices and centralized storage, such as datacenter or cloud storage.

Setting data sensitivity based policy

A simple data classification that illustrates data sensitivity levels can be envisioned through Green | Yellow | Red or Public | Confidential | Restricted in the table below.

	BYO	Enterprise-owned		
	Any Grade Device	**Consumer Grade Device**	**Enterprise Grade Device**	**Mission Grade Device**
Restricted	Access denied	Access denied	Virtualized read-only access (data remains in the datacenter)	Follow me data Enabled
Confidential	Virtualized access only	Virtualized access only	Follow me data Enabled	Follow me data Enabled
Public	Follow me data Enabled	Follow me data Enabled	Follow me data Enabled	Follow me data Enabled

- **Green/Public data** has no distribution restrictions. Public data could be displayed on the company website or distributed with no disclosure impact.
- **Yellow/Confidential data** requires diligence to protect and would have a moderate impact if disclosed. Examples include information posted just for employees on the company intranet, vendor presentations marked “company confidential” and information falling under a regular nondisclosure agreement.
- **Red/Restricted data** would have a material impact on the company and may require breach notification if disclosed. Examples include personally identifiable information (PII), personal healthcare information (PHI) and payment card industry (PCI) data, as well as merger and acquisition plans, unreleased financial information, materially strategic plans and certain legal agreements. Usually, only employees in a small and well-defined set of roles have access to restricted data.

Many governments have their own data classification systems that greatly expand on this simple model.

Citrix mobility technology

Citrix provides a multi-tiered, secure-by-design approach for optimized mobility with virtual computing products spanning the desktop, network and datacenter.

On the desktop

Citrix Receiver

Citrix Receiver is the heart of mobility. Available as a free download for leading platforms, it is the most visible Citrix presence on mobile devices. Citrix Receiver coordinates the delivery of applications and data with a detailed knowledge of device characteristics, such as screen dimensions, input methods, local storage and location services. Applications and data accessed by the Citrix Receiver client are sandboxed from applications and data on the device, reducing the chance of data contamination and loss.

Citrix ShareFile

Citrix® ShareFile allows enterprise and personally managed file sharing and synchronization to be combined. When a ShareFile account is created, encryption keys are established to protect sensitive data in storage and transit. ShareFile is integrated with Citrix Receiver and allows data to follow workers across the various devices they use. ShareFile integration makes it easy for third-party developers and vendors to incorporate common data services such as search, share, sync, secure and remote wipe into their solutions through a set of open APIs. A platform approach also makes it easier to create dynamic mashups that extend secure data-sharing services to both new and existing apps and ensure user data can be accessed easily and securely from millions of enterprise and consumer devices.

ShareFile enables follow me data by allowing content to be local to a device or situation and permitting offline usage, synchronization and usage when network conditions are degraded. This increases the ability to work from anywhere, ensuring documents and e-mail are appropriately available and protected.

vDisk

The personal vDisk enables personalization for a seamless user experience across devices as well as the capability for user-installed applications. Personalization capabilities are controlled by policy, allowing workers to install apps without the need for admin rights, which reduces the chance for system-wide malware.

Citrix XenClient and Citrix XenClient XT

Citrix® XenClient™ enables a multi-tenant laptop with hardware-assisted security isolation through Intel® VT and vPro™ features, including TPM and TXT. The security isolation feature allows work and personal environments to run on the same laptop with total separation. Virtual disks (VHD format) are encrypted via AES-256 and further protected through centralized policy management, including synchronization and kill pills.

XenClient XT is the most robust solution, designed for military and defense applications that require highly sensitive data to be encrypted and managed offline. XenClient XT delivers boot attestation and mission-grade security.

Over the network

CloudGateway

CloudGateway provides a secure, consistent app store that displays all of a worker's authorized apps—Windows®, web and SaaS—on any device. Workers leverage Citrix Receiver to gain access, and once logged into the app store they select their desired (authorized) apps. For IT, CloudGateway provides a single point of management and control—including provisioning lifecycle management for internal and external Windows, web and SaaS applications. More than just single sign-on and application access, CloudGateway enables IT to provision new workers, perform role-based lifecycle access management and de-provision departing workers, ensuring that workers always have access to the applications they require and have no access to de-authorized applications. Workers need only maintain and remember their network access credentials; they are unable to establish weak, insecure passwords for app access. IT gains total access control as well as visibility into application usage, optimization of service level agreements, licensing and workflow for internal and external apps.

Citrix Access Gateway

Citrix® Access Gateway enables SmartAccess for application-level VPN connectivity. Instead of taking the usual all-or-nothing approach to access, SmartAccess uses identity, request and location policy to determine access to specific applications. Using SmartAccess, a worker would automatically be restricted from accessing sensitive applications on a personal device while at home but would have those applications automatically available on the enterprise device when in the office.

In the datacenter

XenDesktop

XenDesktop with on-demand applications allows access granularity and isolation to define and enforce a security boundary around an individual application. XenDesktop defines a security boundary around the desktop and incorporates Citrix® XenApp™ application isolation. Because applications are separated from each other, the file system and the Windows Registry, a security event affecting an application can be confined to that application. Citrix recommends isolating sensitive applications (such as those accessing restricted financial data) and often-attacked apps (such as browsers and PDF readers). SmoothRoaming™ technology ensures that applications and data move with users as they change locations, networks or devices, so they can pick up exactly where they left off, without interruption.

Citrix Mobility Pack and Mobile Application SDK

The XenApp 6.5 Mobility Pack enables native device experience and tablet-optimized desktop features, which allow Windows applications delivered by XenApp to take advantage of mobile device capabilities such as auto keyboard pop-up, local selector controls and auto scrolling. This feature pack and Citrix Receiver for Android 3.0 are required to enable these enhancements.

The Mobility Pack also makes the unique capabilities of a mobile device, such as GPS, camera and other sensors, available to application developers who may use it in conjunction with the XenApp 6.5 Mobile Application SDK to create custom, mobile-friendly applications hosted by XenApp in the datacenter. Note that the Mobility Pack requires an online usage model.

Policy

Sensitive data can be restricted by application policy to remain in the datacenter by disallowing a user from cut/copy/paste/print/save/email vectors for data exfiltration. This policy can be granularly applied to applications: each application, depending on data sensitivity, can either allow or deny specific capabilities. XenDesktop policy enforces these restrictions to protect sensitive data and keep it from being exfiltrated to mobile devices. Policy granularity allows a single application or Citrix® FlexCast™ delivery technology to be specified and controlled. SmartAccess further allows enforces device and identity-based policies. The following table shows what a sample policy for mobile data access can specify.

Sample policy for mobile data access	
Policy objective	**Policy elements**
Centralization of resources	• Keep sensitive data in the datacenter to facilitate backups, reduce storage needs, reduce data exfiltration risk and enable applications and data for e-discovery • Allow offline access to public and confidential data by enterprise-grade systems with location specificity • Enforce online managed access to restricted data by enterprise-grade systems with location specificity • Enable workforce continuity for critical applications
Managed mobility of sensitive data	• Enforce Synchronizer usage for backup in the event of loss or unintentional modification • Require FMD management to copy data to work offline (vault) • Restrict consumer-grade device access to public data on the device, confidential data as a controlled online experience and deny access to restricted data • Allow offline access to restricted data with XenClient XT or enterprise encryption such as BitLocker
Personalization	• Enable customization and settings to follow the worker between devices • Allow installation of personal applications in a sandbox
Device-based access	• Deny jailbroken devices access to apps • Verify device health before allowing enterprise access • Only allow managed devices access to sensitive apps • Consider consumer-grade and BYO as outsiders, requiring virtualization and/or VPN for access to enterprise resources • Remotely wipe lost or stolen devices
Location-based access	• Allow access to enterprise applications and data in approved locations • Deny sensitive application access to printers, external disks and other peripherals unless device is in a company office
Orchestration	• Automate the desired experience and security • Provide workflow and approval for application usage requests

Mobile application management

Mobile device management (MDM) is often cited as a way to enforce device-based policies and manage devices as required by contracts, regulations or governance. MDM enables capabilities to require and set passcodes, device encryption, data wipe policies and more, either for the entire device or just for enterprise-managed apps and data. However, if MDM is leveraged to manage the entire device, it is recommended that the enterprise own these managed devices; wiping a worker's personal device is an unacceptable and highly discouraged management practice.

Another emerging approach, which is highly desirable in today's world of BYO, is called mobile application management (MAM). MAM entails managing the delivery of apps and data to mobile devices in an appropriate manner rather than taking over the entire device. For this approach, individual applications are delivered with wrappers that indicate access and usage policies, as well as encrypt the application and data delivery. These wrappers allow IT administrators to control data sharing and remotely wipe all enterprise apps and data on demand (e.g., when users leave the organization) without impacting personal apps and data.

Both MDM and MAM are complementary to Citrix virtualization solutions, but clearly MAM is far more viable when users expect to work from their personally owned devices without having IT impact their personal content.

Taking IT mobile

Virtualization benefits security

Successful organizations can achieve greater flexibility and agility by taking advantage of the security benefits of desktop virtualization to optimize mobility, embrace consumerization and increase workshifting. The following table outlines how virtualization can help your organization meet core security needs.

Meet core security needs with virtualization	
Protect sensitive data at rest	Keep sensitive data in the datacenter. Users can interact with sensitive data but it never hits the endpoint device. When required, manage sensitive data in a vault for offline usage on authorized endpoint devices. Deliver a consistent set of patched and configured applications to any device. Configure OS, desktops and apps once as golden images; deliver them for online and offline usage; and keep them up-to-date without user action.
Protect sensitive data in transit	Enforce encryption, strong authentication and logging to protect access to sensitive applications and data. Enable granular access based on multiple access factors, including user credentials, role, device characteristics, location, thresholds, approvals and workflow. Eliminate the risk of a single actor exceeding his access or authority, thereby protecting sensitive transactions and administrative actions.
Protect sensitive data in use	Isolate sensitive applications and data that would otherwise be co-mingled and restrict access to authorized users for authorized usage. Further sandbox applications that would otherwise present greater risk and/or security vulnerabilities, such as browsers and PDF readers. Provide automated data classification boundaries around applications, using policy to enforce security specific to the disparate needs of public, confidential and restricted data. Allow for multiple classes of devices, including consumer, enterprise and mission-grade devices. Allow for multiple classes of usage, including desk workers, road warriors, contractors, outsourced workers, suppliers and BYO participants.
Optimize access and handle security threats	Integrate third-party security solutions and apply them to all sensitive apps. Technologies include MAM, data loss prevention and whitelisting. Isolate and protect access to administrative interfaces, management utilities and consoles. Privileged user access can be further isolated to keep sensitive operations separate from normal activities. Respond to disaster recovery situations, enable instant rollback of failed patches and react to security threats by updating all users simultaneously.

Virtualization: optimize for mobility to support consumerization, BYO and workshifting

Mobility is one of the most visible and rapidly expanding forces in computing today. Citrix enables customers to deliver an optimal computing experience, balancing user experience, TVO and information governance for protection of valued information assets.

As workers are encouraged to embrace mobility, BYO and workshifting across a broad range of use cases, they unlock new forms of business value and gain firsthand experience that can be shared throughout the organization. IT gains reassurance that traditional obstacles and risk factors posed by mobility can now be addressed effectively, and develops new mobile strategies and best practices for supporting the business. Far more than an incremental change in enterprise computing, mobility has the potential to transform the way business is done and open the door to tremendous new opportunities for growth and productivity. Helping enterprises realize this potential is now central to IT's mission—and a core focus for Citrix.

Additional Resources

Whitepapers

Deliver IT to the virtual workforce

Refactoring sensitive data access

An insider's look at security strategy

Workshifting how IT is changing the way business is done

Website

Visit www.citrix.com/workshifting

CITRIX®

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix

Citrix 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.

0312/PDF

citrix.com/workshifting