Bring-Your-Own Device | White Paper

Best practices to make BYOD simple and secure

A guide to selecting technologies and developing policies for BYOD

CITRIX®

citrix.com/byod @CitrixBYOD

Bring-your-own-device (BYOD) programs and policies empower people to choose the best device to get their work done, including personally-owned consumer smartphones, tablets and laptops. This white paper provides guidance for introducing BYOD to help people become more mobile and productive while IT adapts to consumerization in a simple, secure and controlled manner.

As consumerization continues to transform IT, organizations are moving quickly to design strategies to allow and embrace bring-your-own device (BYOD). Empowered to choose the best device to get their work done, including laptops as well as smartphones and tablets, people become more mobile and productive. A more satisfying work experience helps organizations recruit and retain the best employees. By shifting device ownership to employees and contractors, IT eases its burden for endpoint procurement and management.

This paper provides IT executives with guidance to develop a complete BYOD strategy which gives people optimal freedom of choice while helping IT adapt to consumerization—at the same time addressing requirements for security, simplicity and cost reduction. Based on a technology foundation of enterprise mobility management, Windows app and desktop virtualization and secure file sharing, as well as proven best practices for BYOD, this strategy enables your organization to:

- **Empower people** to choose their own devices to improve productivity, collaboration and mobility
- **Protect sensitive information** from loss and theft while addressing privacy, compliance and risk management mandates
- **Reduce costs and simplify management** through self-service provisioning and automated management and monitoring
- **Simplify IT** with a single comprehensive solution to secure data, apps and devices

BYOD goes mainstream: Formalizing consumerization—and getting it under control

Broadly speaking, BYOD can be defined as any strategy that allows people to use their own devices, whether occasionally, primarily or exclusively, for work. Many organizations allow people to supplement their corporate-owned machine(s) with additional devices—smartphones, tablets, laptops, home PCs—as needed for optimal flexibility, mobility and productivity. Some go further and eliminate certain corporate-owned device types entirely for eligible employees who prefer to use their own devices instead; in some cases, a stipend is provided to help defray the employee's costs. Contractors are increasingly required to use their own devices rather than being provided with corporate-owned equipment. Ideally, an organization's practices around BYOD should be detailed in a formal policy.

The reality is that many people are already bringing their own devices to work, regardless of whether the organization has a BYOD policy in place. The current average number of devices connecting to the corporate network is 5.18 per knowledge worker—4.43 devices across all workers—and predicted to rise to almost six devices by 2020.[1] In part, this reflects a shift in the nature of the endpoint environment, as the dominance of traditional desktop PCs gives way to a wider range of options that let people choose the right mix of device mobility, performance, size and weight for their purposes, whether it be a laptop, tablet or smartphone.

To date, BYOD has remained an informal practice for many organizations. In the meantime, the lack of a more coherent approach to BYOD can leave the organization exposed to risks from security and compliance gaps to escalating IT complexity. As consumerization continues its rapid rise, the need is clear for a complete BYOD strategy, encompassing both policy and technology.

From a technology perspective, the most obvious question is how people will be able to access enterprise applications and business information on their personal devices. Simply installing apps directly on the device would raise serious security, privacy and compliance risks, license management issues and support complications, as well as restricting BYOD to Windows-based devices—and leaving other consumer devices out of the picture. Many people have also started using unmanaged third-party apps and online services for work—IT needs a way to control and manage this usage and prevent these apps from introducing security risks to the organization.

The ideal approach is to enable completely device-independent computing through enterprise mobility management, Windows app and desktop virtualization and secure file sharing, supplemented by online collaboration and remote support services. With this approach, IT can provide optimal freedom for people while maintaining security and control. People gain single-click secure access to all of their Windows, web, SaaS and mobile apps through a unified app store on any device, over any network, with single sign-on and seamless session roaming across locations, networks and devices. IT gains a single point of control to provision and de-provision apps of all types quickly, whether to provide new resources or to cut off access when it is no longer needed or appropriate. In most

Guiding principles for a successful BYOD strategy

People should have complete freedom to choose any type of device for their work, including the same devices they use in their personal lives, and move seamlessly across devices over the course of the day.

IT should be able to deliver on-demand files, apps and desktops to any device, anywhere, over any connection, while maintaining uniform and efficient security, policy enforcement, compliance and control through a single point of management.

scenarios, business information remains secure in the datacenter; in cases where it has to reside on the endpoint, it is protected through isolation, encryption and remote wipe mechanisms.

In this way, IT can simplify management and reduce costs while empowering people to work easily, securely and seamlessly across any type of device, regardless of ownership. By leveraging the ability to granularly manage data, session and application information, sensitive data can be securely accessed on personally-owned devices. 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.

BYOD policies can vary significantly from organization to organization depending on your priorities and concerns, and should be designed in consultation with HR, finance, legal and IT security teams. Guidelines and best practices for policy development appear in the following section.

Elements of a complete BYOD strategy	
Technology and systems	• A self-service app store providing unified, secure access and single sign-on to mobile, web, custom and Windows apps on any device, over any network • Enterprise mobility management to secure both mobile devices and the business information they are used to access • Secure on-demand delivery of apps and desktops to any device—personal or business—with tracking and monitoring to support compliance and privacy • Secure file sharing and sync from any device • Collaboration including online meetings in HD video and collaborative workspaces, available on any device • Remote support for people and technologies in any location
Policies	• Eligibility • Allowed devices • Service availability • Rollout • Cost sharing • Security • Support and maintenance

Considerations and best practices for BYOD

A successful BYOD initiative combines simplicity for people with effective security, control and management for IT. While the temptation can be strong for IT to develop specific policies for every conceivable scenario, the reality is that most considerations can be addressed through the application of a few simple, consistent principles. In most cases, IT can think about how to manage and provide people secure access to applications, data and files, complemented with role-based management, configuration and security of personally-owned devices to protect the organization against threats, data loss and non-compliant usage.

Eligibility

Organizations should make clear who in the organization is allowed to use personal devices, whether on an ad hoc basis to supplement a corporate endpoint, as a permanent replacement for a corporate device or anything in between. This can be seen as a privilege to be earned, a response to employee demand, a requirement for certain types of roles, an excessive risk for some use cases or, most likely, a combination of these things. “In keeping with our open workplace philosophy, Citrix allows anyone to bring in any type of device for work with no restrictions,” says Paul Martine, chief information officer at Citrix.

Programs that involve the replacement of a corporate endpoint with a personally-owned device, often with a stipend provided to the employee, involve their own set of considerations. One way to determine who should be eligible for this type of program is to apply criteria such as worker type, frequency of travel, performance or whether an individual requires offline access to sensitive data. “At Citrix, anyone who has already been determined to be eligible for a laptop can participate and receive the appropriate stipend to replace their corporate device, provided they have manager approval,” says Shawn Genoway, senior director of IT at Citrix. However eligibility is defined on a broad level, managers should always have final approval over which team members are appropriate candidates to receive a stipend to replace their corporate device with one of their own choosing. Managers can also be advised to apply BYOD within the context of other departmental incentives, privileges and disciplinary measures.

Contractors are generally ideal candidates for BYOD. Many organizations already expect contractors to bring their own devices, and requiring them to do so aids independent contractor compliance.

Allowed devices

In a scenario where applications are installed directly on endpoints, IT has to determine and mandate minimum specifications for OS and application support, performance and other device-specific criteria. Desktop virtualization eliminates these considerations by making it possible to run a full Windows desktop and applications on any kind of device. With enteprise mobility management, IT can enroll and manage any device, detect jailbroken devices and perform a full or selective wipe of a device that is out of compliance, lost, stolen or belongs to a departed employee or contractor. At Citrix, where people bring in any device they choose, there are already over two thousand personally-owned laptops and nearly

Citrix employees follow these BYOD guidelines:

1. Connect via Citrix Receiver
2. Access provisioned apps through a secure, unified app store
3. Share, sync and secure files via Citrix ShareFile
4. Use proper antivirus software
5. Contact vendor to address hardware issues
6. Follow all corporate policies including oversight of device security

Citrix employees can replace their corporate laptop with a personal laptop:

1. Manager approval required
2. $2,100 stipend (minus applicable taxes) for a laptop and three-year maintenance contract
3. Stipend is pro-rated if employee leaves company before one year

two thousand personally-owned tablets in use throughout the organization, in addition to over four thousand personally-owned smartphones including iOS and Android devices used for everything from email to full application access via Citrix Receiver.

Participants should be required to buy their personal devices through normal consumer channels rather than an organization's purchasing department. This helps maintain clear lines of ownership as well as ensures that participants have a direct relationship with their hardware vendor. You may want to make employee discounts available to them, if covered under your corporate vendor relationships. Some people may need or wish to supplement their device with peripheral equipment such as monitors or keyboards while at the office. In this scenario, make sure to specify who will procure and own each item.

Service availability

BYOD doesn't have to be an all-or-nothing proposition. You should think about the specific services you want to make available on personally-owned devices and whether this will differ for specific work groups, user types, device types and network utilized.

For people who want to install apps directly on their computer for their personal use, organizations can consider offering employee discounts for Office Professional for Mac and PC through Microsoft Software Assurance. This way, licensing compliance is entirely the individual's responsibility and the company can avoid risk or liability for violations.

Rollout

Once your BYOD initiative has been designed, communication is vital to a successful implementation. People should receive guidance to help them decide whether to participate and how to choose the right device for their needs. They should also understand the responsibilities that come with bringing their own device, including how data can be accessed, used and stored. Work and business data should be kept strictly segregated on a personally-owned device to support e-discovery requirements and data retention policies; similarly, work emails should never be sent from personal accounts. Acceptable use policy should apply the same way on personally-owned devices as they do on corporate devices.

Cost sharing

One of the primary benefits of BYOD is the ability to reduce costs by having people pay part or all of the cost of various devices used for work, and getting IT out of the business of procuring and supporting an expanding array of hardware throughout the enterprise. This is especially true in cases where a corporate-owned laptop or device will no longer be provided. In a recent survey, the vast majority of organizations with a BYOD policy already in place or planned said they compensate employees who use their own devices for work purposes, either in part or in full. Providing compensation can also give organizations some control over consumerization, a factor cited by 61 percent of those surveyed as the main reason for their stipend or financial contribution.[2]

"The Citrix bring-your-own-computer program, which allows people to replace their corporate device with a personal device, is designed to yield 18 – 20 percent savings," says Martine. "This amount is discounted from the total cost of the standard corporate device that would otherwise be provided, including OS and three-year maintenance and warranty, plus estimated tax withholdings, to calculate the stipend provided." Participants should also be aware that the stipend will be treated for tax purposes as income. In regions with higher personal income tax rates, you may want to increase the stipend accordingly to keep the net subsidy consistent for all participants. Any BYOD policy, with or without cost-sharing, should make clear who will pay for network access outside the corporate firewall, whether via 3G, public Wi-Fi or home broadband.

If you choose to provide a subsidy, it should reflect the full participation lifespan of each individual. Subsidies should be renewed at a regular interval, such as the typical three-year hardware refresh cycle, to ensure that personal devices do not age beyond what would be expected for an enterprise device. If a participant leaves the company during a BYOD cycle, you may want to reclaim a portion of the current stipend. At Citrix, people who leave the company or the program within a year of enrolling in BYOD are responsible for repaying a pro-rated portion of their stipend.

Cost sharing has implications for the introduction of BYOD in the organization. An all-at-once rollout can increase cost as people sign up—and claim their stipends—at all points in the endpoint refresh cycle. Offering the program to people as they come to the end of their device lifecycle will spread out the impact, typically over three years. Organizations that do not offer a stipend can encourage full participation from day one.

Security and Compliance

Many CIOs worry that further consumerization of IT will lead to greatly increased business risks. This is a reasonable concern, and one raised frequently by Citrix customers seeking guidance on BYOD. While the installation of applications directly on non-corporate devices can increase risk, a BYOD program based on enterprise mobility management, Windows app and desktop virtualization and secure file sharing manages and reduces risk. All business information remains secure within the datacenter, residing on the endpoint only when absolutely necessary. In cases where data does need to reside on the endpoint, it can be protected through isolation, encryption and remote wipe mechanisms. To prevent exfiltration, IT can implement policies to disable printing or access to client-side storage such as local drives and USB storage. Participants should also ensure that antivirus/anti-malware software is appropriately installed and updated on their endpoint. Citrix provides antivirus protection to employees participating in the BYOD program at no cost to the employee.

On mobile devices, access to apps and data can be controlled, secured and managed with policies based on device ownership, status or location. IT can enroll and manage any device, detect jailbroken devices and perform a full or selective wipe of a device that is out of compliance, lost, stolen or belongs to a departed employee or contractor. Application security is ensured through secure application access via app tunnels, blacklisting, whitelisting and dynamic, context-aware policies.

To protect the enterprise network, some organizations apply network access control (NAC) technology to authenticate people connecting to the network and check whether their devices have up-to-date antivirus software and security patches. Citrix takes a different approach, allowing BYOD program participants to use the Citrix network to access their on-demand data, apps and desktops through Citrix NetScaler Access Gateway, following two-factor authentication, but not allowing them to join the personally-owned device itself to the network. "This allows the least restriction on the individual's personal device while ensuring the security of our network, and reflects the open computing culture at Citrix," says Genoway. NetScaler Access Gateway can also be used to provide granular, policy-based browser access to apps and data. Single sign-on and strong passwords allow both convenience and security.

Outside the firewall, virtualization and encryption can allay most of the security vulnerabilities of Wi-Fi, WEP encryption, open wireless, 3G/4G and other consumer-grade access methods. Network security capabilities provide visibility into and protection against internal and external mobile threats; blocking of rogue devices, unauthorized users and non-compliant apps; and integration with security information and event management (SIEM) systems.

In the event that a BYOD participant leaves the organization, BYOD policy is breached or a personally-owned device is lost or stolen, IT should have a mechanism to terminate access instantly to data and apps, including automatic de-provisioning of work-related SaaS accounts and selective wipe of lost devices.

Instead of allowing open BYOD approches, in which people can bring any device to access enterprise apps and data, some organizations choose a managed approach. In this scenario, IT manages the personally-owned device directly, including registration, validation, authorization and device resource access.

Device support and maintenance

A BYOD program often reduces the total maintenance required for each device because the user is also the owner. "As any rental car customer will attest, people treat their own equipment better than they do someone else's. A personally-owned device is much less likely to show up at IT with salad dressing in the keyboard," says Genoway.

This being said, a BYOD policy should spell out explicitly how various support and maintenance tasks will be addressed and paid for. When a personally-owned device has replaced a corporate endpoint, there may be a higher expectation of IT support—but this should be defined narrowly to avoid exposing IT to greatly increased complexity and workload.

In keeping with the simplicity that guides the Citrix BYOD policy, the company takes a hands-off approach, providing support only for wireless connectivity, antivirus/anti-malware software and the Receiver client on personally-owned devices. Citrix employees bringing their own computer have the option to request a Citrix loaner device for 10 days should their device need repair. All other support is through the community BYOD discussion board, which includes a self-help section.

While some IT organizations create an entire team dedicated to supporting BYOD, Citrix has dedicated just 10 percent of one staffer's time to the entire program, including writing the BYOD blog, answering questions and handling payroll submissions for program stipends. Just as most consumer devices come with a single-sheet quick-start guide, Citrix focuses on making it simple for people to download Receiver on any device and get it to work quickly.

A secure technology strategy for BYOD

Citrix enables organizations to support BYOD by offering a unified app store and secure access to business information. Citrix BYOD solutions include enterprise mobility management, Windows app and desktop virtualization, secure file sharing, collaboration and remote support. Through this approach, IT can make enterprise apps and secure file sharing and sync available on any device people bring in to work while maintaining security and control.

Citrix BYOD solutions address all the key capabilities required to make BYOD simple, secure and effective for any organization.

App store *powered by Citrix Receiver*
People can access the apps they need on the devices they choose, including Windows and Mac desktops and laptops, iOS, Android and Windows-based mobile products, Google Chromebooks and BlackBerry mobile devices—all with seamless roaming and a high-definition experience across devices, locations and networks. A unified app store provides single-click access to mobile, web, custom and Windows apps, including integrated file sharing and productivity apps.

Secure access *powered by Citrix NetScaler Access Gateway*
A unified management framework lets IT secure, control and optimize access to apps, desktops and services on any device. Access control, auditing and reporting support compliance and data protection.

Enterprise mobility management *powered by Citrix XenMobile*
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. Business apps and data, whether developed by IT or a third party, reside in a container, separated from personal apps and data on the device.

Citrix offers secure by design BYOD solutions

- Enterprise mobility management, Windows app and desktop virtualization and file sharing support security, data protection and IT governance as effectively for personally-owned devices as for corporate devices
- All enterprise data is hosted and backed up in the datacenter
- Confidential business information is delivered to endpoints only in isolated, encrypted form to prevent loss or tampering
- When use cases require data to reside on personally-owned devices, IT can isolate, encrypt and if needed wipe the data remotely
- Data centralization and on-demand, any-device computing facilitate business continuity and disaster recovery
- Records management, information management and data retention policies for documents and email are applied and managed centrally
- Comprehensive monitoring, activity logging and reporting ensure data privacy and aid compliance

Windows app and desktop virtualization *powered by Citrix XenDesktop and Citrix XenApp*
IT can transform Windows apps and complete desktops into on-demand services available on any device. Because apps and data are managed within the datacenter, IT maintains centralized data protection, compliance, access control and user administration as easily on personally-owned devices as on corporate-owned endpoints—within the same unified environment.

File sharing *powered by Citrix ShareFile*
People can securely share files with anyone and sync files across all of their devices. Flexible storage options, policy-based control, reporting, data encryption and remote wipe help keep business content secure.

Collaboration *powered by Citrix GoToMeeting and Citrix Podio*
People can initiate or join meetings from anywhere in seconds, on any device, with HD video for true face-to-face interaction. Similarly, Citrix GoToWebinar and Citrix GoToTraining enable people to conduct larger seminars or training sessions online. Social activity streams, custom apps and collaborative workspaces help people work together more effectively.

Remote support *powered by Citrix GoToAssist*
IT can centrally support people and technologies in any location to ensure uptime for PCs, Macs, mobile devices, servers and networks across the organization.

Conclusion

As a strategy at the nexus of powerful IT trends like consumerization, workplace flexibility, mobility and cloud computing, BYOD will continue to transform the way people and organizations work. The right strategy, enabled through the delivery of on-demand data, apps and desktops to any device, will:

- **Empower people** to choose their own devices to improve productivity, collaboration and mobility
- **Protect sensitive information** from loss and theft while addressing privacy, compliance and risk management mandates
- **Reduce costs and simplify management** through self-service provisioning and automated management and monitoring
- **Simplify IT** with a single comprehensive solution to secure data, apps and devices

As a leader in flexible, mobile workstyles, as well as an early adopter of BYOD in our own organization, Citrix provides complete technologies backed with proven experience and best practices to deliver successful BYOD programs. Citrix BYOD solutions are already helping many organizations of all sizes realize the full benefits of BYOD.

For additional information, please visit www.citrix.com/byod or read our other related papers.

Additional resources

- Delivering enterprise information securely on Android and Apple iOS devices
- Enterprise Mobility Management: Embracing BYOD Through Secure App and Data Delivery
- Bring-Your-Own Device Starter Kit

1,2 Citrix, Workplace of the Future: a global market research report, September 2012.

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 (NASDAQ:CTXS) is the cloud computing company that enables mobile workstyles—empowering people to work and collaborate from anywhere, accessing apps and data on any of the latest devices, as easily as they would in their own office—simply and securely. Citrix cloud computing solutions help IT and service providers build both private and public clouds—leveraging virtualization and networking technologies to deliver high-performance, elastic and cost-effective services for mobile workstyles. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations of all sizes achieve the kind of speed and agility necessary to succeed in an increasingly mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.