citrix

White Paper

Why a successful BYOD policy begins with endpoint management

When people can use their own devices for work, great things happen. Employees become more mobile, productive, and engaged, able to work their own way without traditional constraints. For the organization, a BYOD program can mean lower cost and less work for IT, as well as greater flexibility to empower people wherever and whenever work needs to get done. But it's crucial to do it right so that the freedom that comes with personal devices won't also expose corporate data to security risks.

Citrix Endpoint Management gives your employees the freedom they enjoy while protecting your business. Complete mobile app and device management capabilities keep corporate data safe wherever and however it's accessed and used. Features like better-than-native productivity apps, single sign-on, and third-party integrations help people get more done no matter what device they're using.

Freedom, flexibility, and cost savings – why everyone loves BYOD

As BYOD grows more prevalent as a mainstream strategy, its benefits have become well established. To begin with, employees often prefer to use their own devices for work. Having chosen, customized, and become familiar with their own laptops, tablets, and smartphones, they feel more comfortable and engaged in these environments. Being allowed to bring this part of themselves into their work life, rather than trading it for corporate-issue tools, adds a welcome touch of humanity to their day.

More substantively, BYOD helps people become more flexible and productive. They can flow more seamlessly into work from their personal life without having to switch gears on a different platform, including after hours, on the road, or at other times when a corporate device might have been left at the office. And no one likes having to carry around two laptops or phones to be ready for anything. In the often unpredictable world of digital business, the ability to hit the ground running quickly and work fast can be critical.

And there's a clear link between engagement and productivity. In a study by the Economist Intelligence Unit, a majority of companies (64%) reporting higher employee engagement and productivity than their peers believe that low productivity has a negative impact on employee engagement. A plurality (43%) believe low productivity and low engagement are mutually reinforcing. Another study found that companies with higher employee engagement see 2.5x greater revenue growth.

For IT departments with busy digital transformation agendas, the opportunity to shift focus from buying, provisioning and maintaining commodity endpoints can be a breath of fresh air. Both capital and operating costs around user devices can be greatly reduced, including the associated ongoing administrative and support desk burdens. Instead, users can be given a stipend to help address their own device needs — as they're already accustomed to doing for personal usage.

Getting the benefits of BYOD without increasing risk

One of the primary requirements for successful BYOD is security. To realize the benefits of BYOD without exposing the organization's data and network to harm, IT needs an effective way to address risks across three categories.

- **Compromised devices** – It's all too easy to leave a device behind in a cab or hotel room, or worse, have it stolen. At that point, the organization can be at the mercy of whatever passcodes or other protective measures its owner might — or might not — have taken. When the device has been used for work, that can leave sensitive corporate data exposed to theft and misuse, and leave the business exposed to regulatory fines, blackmail, loss of IP, and much more
- **Hacking** – Every IT department knows how hard it can be to maintain security best practices even on corporate-issued endpoints. Imagine how much more vulnerability can be introduced by the wider variety of activities people engage in on their own time, from visiting nonsecure websites, to running ill-advised apps, to jailbreaking phones. For hackers, that can leave the door wide open for stealing corporate data and gaining access to the corporate network
- **Data leakage** – Even when employees think they're being careful, having corporate and personal apps on the same devices can allow data to leak between the two via the clipboard, open-in settings, and other device-wide functionality. That introduces huge vulnerabilities in terms of regulatory compliance as well as data protection

Beyond security, it's also important to make sure people can work easily anywhere with a great experience on their personal devices. To be creative, purposeful, and productive, people need to be able to focus on their role, not on technical details like logins, networks, and security settings.

And keep in mind that BYOD is about more than just iOS and Android phones and tablets. While mobility is a key benefit of BYOD, what matters is the mobility of the employees themselves — whatever devices they use. That can also include Chromebooks, Windows 10 laptops, MacOS laptops, tvOS devices, and IoT devices. By the same token, people need to be able to access the full scope of tools they'd use on corporate devices, including enterprise apps, virtual apps and desktops, and SaaS.

A successful BYOD program addresses risks across three categories.

Compromised devices

Hacking

Data leakage

Supporting your BYOD policy with Citrix Endpoint Management

Citrix Endpoint Management makes BYOD simple and secure by providing a modern approach for managing all kinds of devices, whoever owns then, through a single platform. Employees get a seamless, intuitive, and productive work experience on the endpoints of their choice, while IT gets the ability to ensure security on BYOD devices without having to interfere with the employee's own content.

Securing BYOD devices, files, and data

The diversity of devices in the consumer world can create dizzying complexity for IT. Citrix Endpoint Management lets IT manage mobile apps and devices across all platforms from a single console, including settings for security and compliance

While traditional client management tools focused on Mobile Device Management (MDM), which meant taking control of the entire device, Citrix now helps organizations evolve to a more flexible approach based on Unified Endpoint Management (UEM) and Mobile Application Management (MAM). This makes it possible to avoid a key sticking point for BYOD security: the need for employees to grant full access to their personal devices — including the ability for IT to wipe the entire device remotely.

With MAM, IT can be given access only to specific managed applications rather than the entire device. In this way, IT can ensure that the device is safe for work before launching its corporate apps, and apply corporate security settings as needed while these apps are used, without interfering with any of its personal apps or content. Real-time compliance checks verify the device's location, network connection, and allow IT to selectively turn off individual services like USB ports, copy-paste mapping, and so on by policy depending on the risks they might pose in the current context. Devices found to be out of compliance on operating system version, jailbreak status, and other factors can be denied access entirely. If a device is lost or compromised, IT can remotely wipe its corporate apps and data without touching its personal content.

Providing secure mobile productivity apps

The native apps that come with mobile devices are designed for personal use, not enterprise requirements. Citrix mobile productivity apps are optimized for business use, including both convenient integrated workflows and built-in data protection.

- **Better-than-native email** – Work email can push native mobile apps to the limits with the contacts, calendars, and files it often includes. It's also risky to allow business and personal emails to share the same inbox and data environment. Citrix Secure Mail provides a separate app that's strictly for business, built to make it simple to work with contacts, calendars, and files while still providing a convenient consumer look and feel. Features like tabbed navigation, a prioritized inbox, calendar event export, and invite response improve productivity with beyond-native convenience

- **Third-party integrations** – Native email is a narrowly focused tool — not a work environment. Citrix Secure Mail lets people broaden their experience with easy ways to access and share content, track Salesforce workflows, move conversations into Slack, and join GoToMeeting, Skype, and WebEx virtual meetings

- **Secure web browsing** – The role of mobile browsers as the front end for many web, cloud, and mobile apps make them an inviting attack vector for hackers to enter the corporate environment. Citrix Secure Web lets IT apply secure policies before allowing access to the corporate intranet and work-related sites without putting restrictions on personal browsing

Allowing simple, secure access to enterprise apps

BYOD goes beyond mobile devices — and employee productivity goes beyond mobile apps. Citrix Endpoint Management provides convenient single sign-on access to all of an employee's apps on any device they use. App container and microVPN technology on mobile devices is complemented with easy onboarding for BYOD devices for secure productivity on any platform.

- App containers let IT apply more than 70 policies to manage and secure each app and the data it processes without imposing device-wide controls or interfering with personal content
- App-specific microVPNs for Citrix Secure Mail and Citrix Secure Web let IT allow mobile access to the corporate network without allowing entry for threats that might be hiding elsewhere on the device. On-demand activation helps lower data transfer costs while allowing better performance and longer mobile battery life
- The container that holds Citrix Secure Mail and Citrix Secure web can interact with Microsoft Office 365 apps, allowing people to cut, copy, paste, and interact across any of these apps without the danger of leaks or infection via personal apps. Microsoft Managed Browser and Microsoft Edge can also be secured with the Citrix microVPN

Conclusion

The best BYOD programs combine freedom, productivity, and a great experience for the user with security and data protection for IT. With Citrix Endpoint Management, IT can protect corporate data and networks while empowering employees and respecting their privacy.

To learn more, visit www.citrix.com/uem

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States