How to Enable and Secure in the Next Stage of BYOD: Reap the Benefits of Bring Your Own Laptop

Executive Brief

Summary

There is a new development in the ‘Bring Your Own Device’ (BYOD) movement in today’s workplace. While employees continue to use their smartphones and other mobile devices, a growing number are also using their own desktops, laptops, tablets and Windows® Surface Pros. ‘Bring Your Own Laptop’ (BYOL) has multiple potential advantages for organizations, including greater productivity, flexibility and significant cost savings.

The trend towards increasing use of personal and non-corporate managed computers is part of broader changes in the enterprise technology landscape, with increased heterogeneity of endpoints, applications, ownership models and users. Unfortunately, this diversification is happening in the shadow of intensifying cybersecurity threats targeting sensitive corporate data.[1]

When employees, partners and contractors use their own computers remotely or on site, enterprises have much to gain – as long as they can safeguard critical data while providing cost-effective, seamless access to business content and tools.

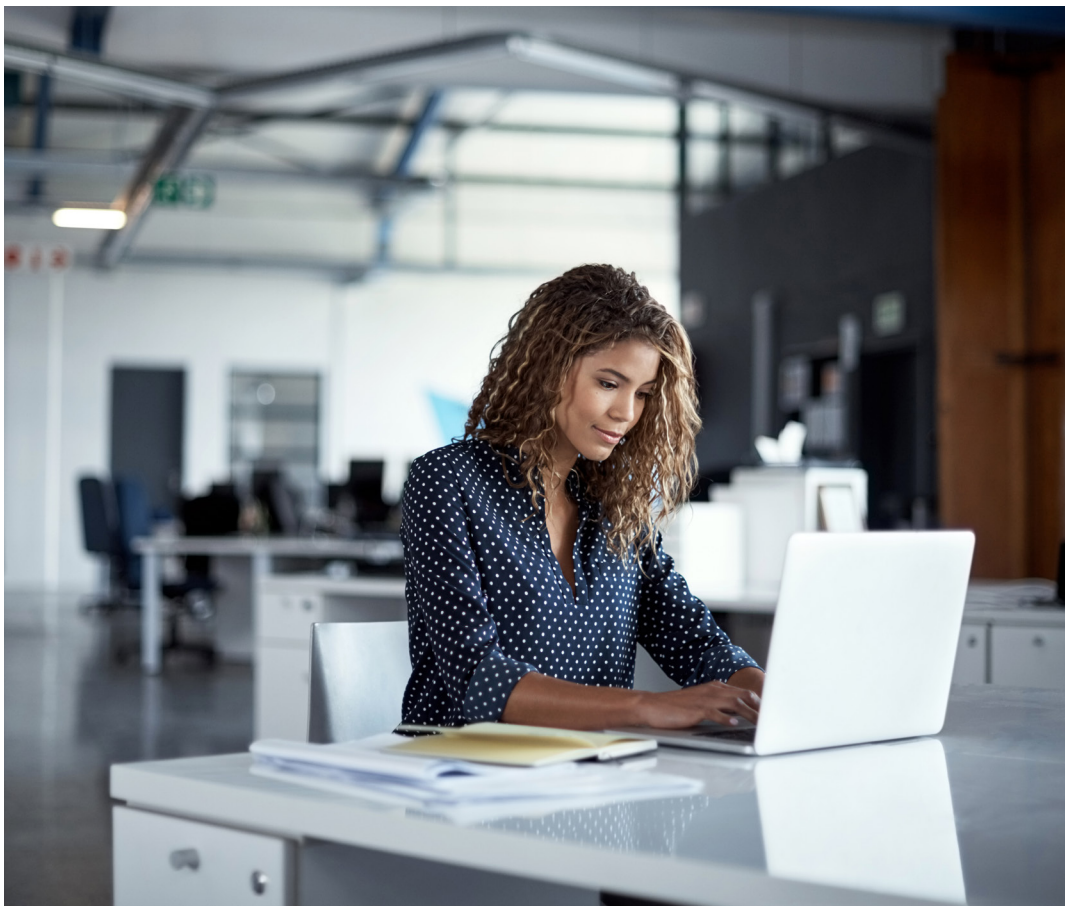


Table of Contents

Top 5 forces driving change in the enterprise technology ecosystem 4

From BYOD to BYOL 5

Migration to Windows® 10 5

Savings, productivity and morale: The upside of BYOL 6

Security and privacy risks: The downside of BYOL 7

5 ways to reap the benefits of BYOL – and keep corporate data safe 8

BlackBerry® Offerings for Desktop: A solution for the new era of devices 9

Top 5 forces driving change in the enterprise technology ecosystem

The days when IT departments' primary job was to manage employee desktops are long gone. But so are the more recent days when it was enough to secure business data on employees' smartphones and other mobile devices. Current trends all point to the need for new management principles for a new era of devices, which includes:

1. More endpoints

Modern workers want to work anytime, anywhere on all types of devices – including the latest Windows® 10 and macOS® devices. By 2020, IDC expects mobile workers will account for nearly three-quarters (72.3%) of the total U.S. workforce.[2] And by 2022, Gartner forecasts that up to 70% of enterprise software interactions will occur on mobile devices.[2]

2. New application types

According to Gartner, using mobile apps results in a 60% productivity increase. But in the current app-centric economy, no single app can accomplish a workflow. As a result, new app types (especially HTML5 apps) continue to gain traction.[3]

3. New ownership models

As new endpoints enter the workplace, ownership models have evolved from traditional enterprise-owned and managed devices to BYOD (focused on mobile devices) to BYOL (including desktops, laptops, tablets and Windows® Surface Pros).

4. New user populations

In today's collaboration culture, enterprise workflows not only span the organization, but can extend outside the organization to partners, contractors and short-term employees. More users could also mean more personal and non-corporate managed devices are used.

5. New types of endpoints

Traditionally, there have been three distinct personal device categories in enterprise: laptops, smartphones and tablets. The growing use of hybrid tablet/laptops, 2-in-1s and phablets have blurred these distinctions.

From BYOD to BYOL

BYOD is firmly entrenched in the workplace: an IDC MarketScape report found 90% of enterprises support BYOD.[4] But now employees are using more than just their smartphones to get work done, opting to also use personal and non-corporate managed desktops and laptops.

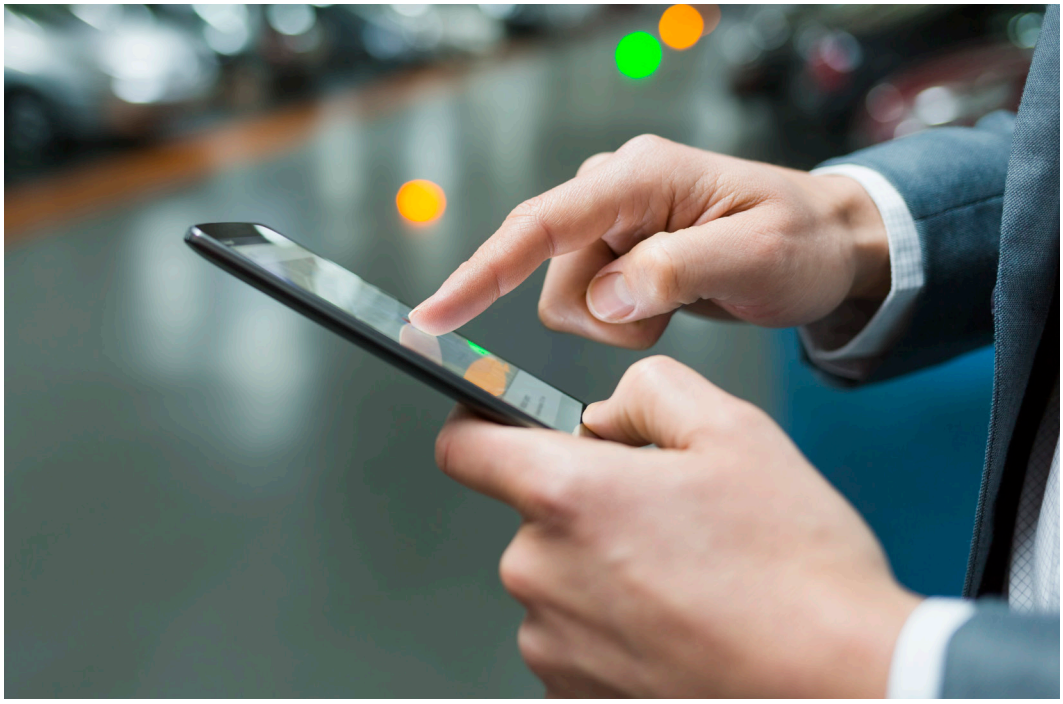
According to a report in the Harvard Business Review online, BYOL nearly doubled at high-performing companies (from 44% to 80%) in recent years. Most of this increase, however, has come from unofficial use, which means a growing number of employees are using their own computers without IT/corporate approval.[5] When employees connect to cloud services on non-corporate devices outside the view of IT, it significantly increases the risk of a data breach.

Migration to Windows® 10

The adoption of Windows® 10 is growing fast, both inside and outside the enterprise, and it is becoming available on more and more devices – including new phablets and other hybrids. The March 2017 Gartner User Survey Analysis found:[6]

- 85% of organizations will have started Windows® 10 deployments by the end of 2017
- Migration to Windows® 10 will be significantly faster than prior OS adoption

With the growing popularity of Windows® 10 showing no signs of abating, enterprises must ensure efficient measures are in place to manage and secure it. Before Windows® 10, managing Windows® could be complicated, expensive and restrictive, while provisioning Windows® could be time-intensive. Windows® 10 aims to enable a modern, simplified approach to management, security and provisioning when combined with Unified Endpoint Management (UEM).



Savings, productivity and morale: The upside of BYOL

When employees use their own computers for some or all of their work, there can be direct cost savings on hardware, software, provisioning and help desk for organizations. This is especially evident when it comes to onboarding and offboarding contract and short-term employees.

For workers, BYOL helps enhance work-life balance by supporting greater mobile productivity. A study quoted in Forbes found almost half of workers polled feel they are more efficient and productive when they can choose their own devices.[7] With BYOL, there are few, if any, obstacles to employees using the latest Windows® 10 devices.

Security and privacy risks: The downside of BYOL

A growing number of employees want and/or expect to use their personal computers for work – which often involves accessing sensitive business resources. But with wide-ranging levels of security training and awareness, employees can be careless with their computers. A recent Data Breach Investigations Report from Verizon® found phishing and malicious email attachments are still the main cause of data breaches.[8]

The BYOL movement increases the risk of both external and internal data breaches.

- **External:** corporate data theft by external bad actors from personal and non-corporate managed laptops with deficient security

- **Internal:** corporate data leakage by employees and third parties via simple errors, susceptibility to phishing scams and/or weak third-party security

Whether the data breach originates internally or externally, the potential repercussions can be equally serious. Losing control of sensitive data can impact the bottom line directly via financial losses, or indirectly via brand/reputational damage.

When the General Data Protection Regulation (GDPR) comes into effect in May 2018, affected organizations will also face potentially massive fines if they don't meet the requirements for protecting customers' personal data.[9] While this regulation is focused on European organizations, it applies to any company that uses, stores, or processes personal information about an EU citizen, and it will likely become a benchmark for organizations globally.

The traditional methods used to secure corporate data on personal and non-corporate managed computers – Virtual Private Network (VPN) and Virtual Desktop Infrastructure (VDI) – can be expensive, complex and may deliver a poor user experience.

5 ways to reap the benefits of BYOL – and keep corporate data safe

If organizations do not take steps to secure business data in a cost-effective way, the potential risk and expense attached to the increased use of personal and non-corporate managed computers could outweigh any benefits. The new era of devices demands new solutions to secure them. While many solutions may promise full business productivity on employee desktops, laptops, tablets and Windows® Surface Pros, organizations should keep the following requirements in mind as they consider their options.

Can the solution...

1. Provide flexible but secure access to corporate servers from personal or non-corporate computers, and even allow users to work offline?
Employees must be able to access what they need to work, anytime and anywhere, securely – but without having to jump through hoops to start working.

2. Ensure cost-effective, end-to-end encryption?
Organizations need reliable security. Although VPN and VDI are able to secure a network connection, the costs associated with licensing, hardware, software, infrastructure and help desk support can add up quickly.

3. Enable easy onboarding and offboarding?
Provisioning and deprovisioning users should be quick and easy, allowing IT to quickly scale up in the case of acquisitions, new projects or seasonal demand. They should also be able to confidently deprovision devices, knowing business data and access capabilities have been removed.

4. Extend access to key business apps and data to partners, without giving them full access to enterprise systems?
Organizations should have the ability to only allow access to corporate resources that are relevant to specific business engagements. It should be possible to define access by users, groups and even specific files – what users can do with those files, and how long they have access to those files.

5. Deliver a superior user experience?
Any solution should support employee productivity with a consistent, intuitive interface that doesn't impede workflows, on any Windows® 10 device.

BlackBerry® Offerings for Desktop: A solution for the new era of devices

BlackBerry® offerings for desktop on Windows® 10 and macOS® allow enterprises to broadly embrace BYOL and all its benefits, with full confidence in the security of business data. The modern, simple approach provided by **BlackBerry® Access**, **BlackBerry® Work** and **BlackBerry® Workspaces** enables optimal productivity on non-corporate managed and personal computers. Together, these offerings deliver the security enterprises need with the freedom for employees to choose their preferred device.

Key Benefits

- **Enables secure remote connectivity to business resources from any computer**

BlackBerry® Access allows secure access to corporate servers, content and HTML5 applications, including third-party extensions such as Salesforce®. It gives employees the tools they need to work remotely on any personal or non-corporate managed Windows® 10 or macOS® device, including desktops, laptops, tablets and Windows® Surface Pros.

- **Reduces costs and maintence complexity**

BlackBerry® Access removes the need to provision and maintain corporate laptops and software, along with VPN or VDI licenses (and their time consuming sign-in procedures). Instead, it offers smooth single sign-on to intranet and business applications.

- **Delivers rich policy and access controls**

BlackBerry® Access offers simple connectivity management via whitelists (for fine-tuned access control) or flexible routing. It enables system administrators to set different browser and access policies for different user groups, creating a seamless experience for end users and easy management for IT.

- **Provides turnkey onboarding and offboarding**

BlackBerry® Access helps extend productivity to both traditional and non-traditional employees—including contractors, remote workers and partners. It creates a secure environment for corporate data, separate from all personal apps, that can be wiped clean for offboarding, lost devices or potential data breaches.

- **Ensures cost-effective end-to-end security**

BlackBerry® Access enables seamless connections for remote users to sensitive data sources. Data Path Controls securely route traffic through the firewall, while keeping intranet and any Software as a Service (SaaS) data secure and containerized.

- **Supports uninterrupted workflows – even offline**

BlackBerry® Access delivers online and offline access to BlackBerry® Work on laptops – a secure, multi-OS, all-in-one mobile productivity app designed for collaboration in business users. BlackBerry® Work combines email, calendar, contacts, presence, document access, document editing and more. It provides the same set of capabilities as corporate-owned/managed computers for full business productivity on personal and non-corporate managed computers.

- **Enables enterprise-grade file sharing**

With BlackBerry® Workspaces, users can securely share files both inside and outside the organization. It embeds Digital Rights Management (DRM) protection directly into files, allowing customized controls on what users can do with files (save, edit, copy or print). BlackBerry® Workspaces makes accessing and controlling files easier than ever on personal and non-corporate managed computers.

- **Integrates with Microsoft® Office 365®**

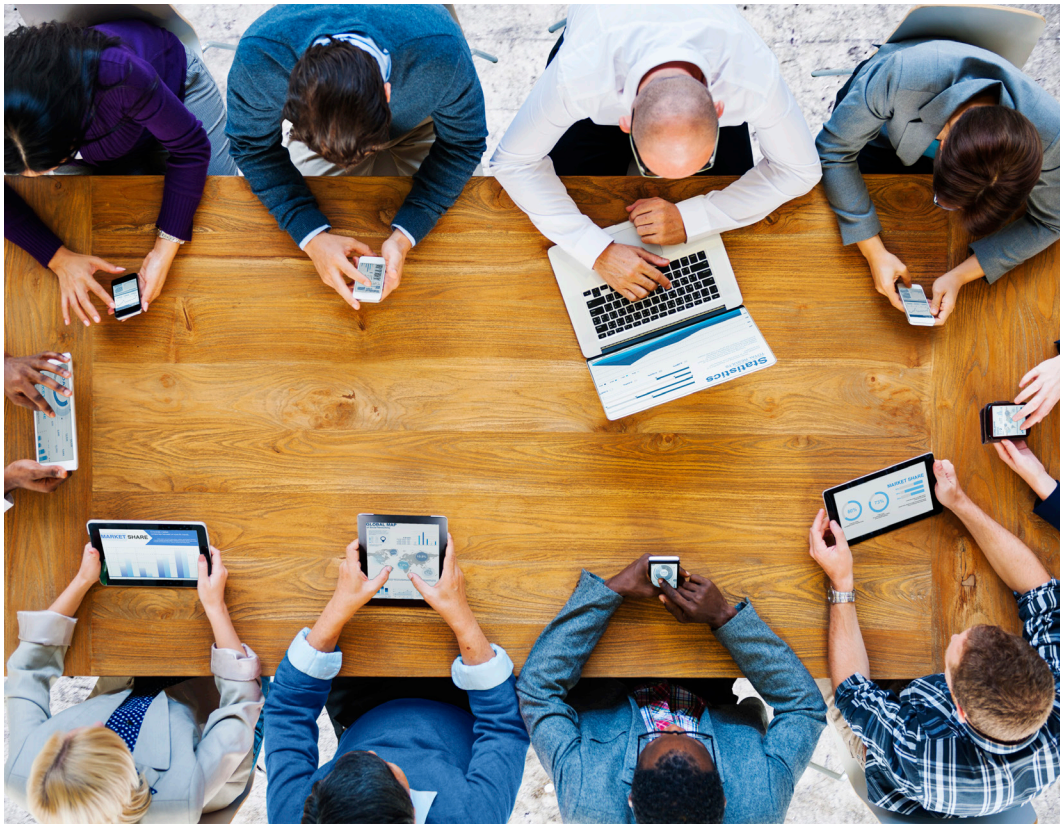
BlackBerry® Access, BlackBerry® Work and BlackBerry® Workspaces integrate with Microsoft® Office on premises, Microsoft® Office 365®, SharePoint and OneDrive to contribute to enhanced collaboration and security.

- **Offers simple, flexible deployment options**

Organizations can opt to deploy BlackBerry® offerings for desktop on Windows® 10 and macOS® either on premises, as a cloud service or in a mixed model. BlackBerry® allows organizations to move to the cloud in steps, with per-user migration from on premises to the cloud, avoiding potentially disruptive full cutovers that may affect access for large groups of users.

With the increasingly widespread use of Windows® 10 and macOS®, the growing popularity of hybrid devices and employees' established preference for using their own devices, BYOD will soon go hand-in-hand with 'Bring Your Own Laptop' (BYOL). This trend can offer an opportunity for enterprises to save money on hardware, software, provisioning and help desk costs, while helping to boost productivity.

BlackBerry® offerings for desktop on Windows® 10 and macOS® allow users to work from personal or non-corporate managed laptops — and even multiple laptops — with full confidence in end-to-end security and the ease of an intuitive user experience. Users get the power of choice, without IT losing control of business data.



Learn more at:
blackberry.com/enterprise/windows-10-macos

1. Identity Theft Resource Center (http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release)
2. Business Wire (http://www.businesswire.com/news/home/20150623005073/en/IDC-Forecasts-U.S.-Mobile-Worker-Population-Surpass)
3. Gartner (https://www.gartner.com/doc/3525665/predicts--mobile-apps-development)
4. IDC MarketScape Report (https://www.idc.com/getdoc.jsp?containerId=US42890217)
5. Harvard Business Review (https://hbr.org/2016/05/tracking-the-trends-in-bringing-our-own-devices-to-work)
6. Gartner Newsroom (https://www.gartner.com/newsroom/id/3690917)
7. Forbes (https://www.forbes.com/sites/centurylink/2013/04/26/byod-employees-bring-their-own-efficiency-to-work/#7e387e92548c)
8. Tripwire (https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/takeaways-from-the-2016-verizon-data-breach-investigations-report/)
9. EU GDPR (https://www.eugdpr.org/)