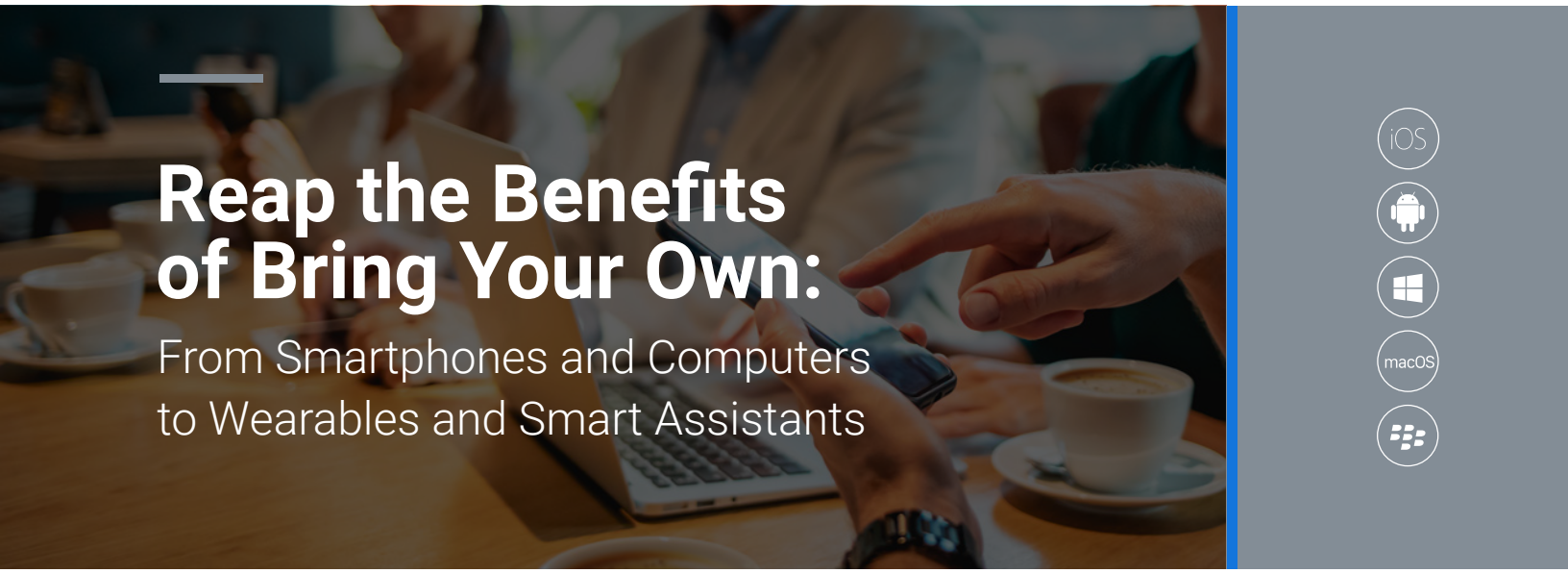
BlackBerry

Whitepaper



Reap the Benefits of Bring Your Own:

From Smartphones and Computers to Wearables and Smart Assistants

Summary

There are new developments in the 'Bring Your Own' (BYO) movement in today's workplace.

While employees continue to use their smartphones, a growing number are also using their own laptops, tablets, wearables and smart assistants. This trend has multiple potential advantages for organizations, including greater productivity, flexibility and significant cost savings.

The increasing use of personal and non-corporate managed devices 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] A recent survey of 200 CEOs of leading companies identified cybersecurity as a top global challenge threatening business growth.[2]

When employees, partners and contractors use their own mobile devices, computers, wearables and smart assistants remotely or on site, enterprises have much to gain – but only if 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

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' mobile devices and laptops. 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 using all types of devices and tools – including the latest Windows® 10 and macOS® devices, popular wearables such as the Apple Watch and Samsung Galaxy Watch, and smart assistants such as Alexa and Siri. By 2022, Gartner forecasts that up to 70% of enterprise software interactions will occur on mobile devices.[3] Unfortunately, mobile endpoints are more than twice as likely than servers to be successfully compromised.[4]

2. New application types

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. Global revenue for the enterprise app software market is steadily rising and is expected to reach $305 billion by 2022 – an indication of the ongoing proliferation of apps in the workplace.[5] According to Entrepreneur magazine, a typical company used an average of 52 apps in 2016 and 112 in 2019.[6]

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), then to BYOL (including desktops, laptops, tablets and Windows® Surface Pros), and now to BYO wearables and smart assistants.

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 can also mean increasing use of personal and non-corporate managed mobile devices, laptops, wearables and smart assistants.

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 first blurred these distinctions. Today, wearables (including smart watches, glasses and clothing) and chatbots are expanding this frontier.

From BYOD to BYOL to BYOE

BYOD is firmly entrenched in the workplace: an IDC MarketScape report found 90% of enterprises support BYOD.[7] 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, tablets, wearables and smart assistants.

According to Gartner, by 2023 almost one-third of IT organizations will extend BYOD policies to include "Bring Your Own Enhancement" (BYOE) policies that address technologies that enhance – and track – performance and productivity.[8] Advances in wearable technology have driven the trend towards "augmented workers" in a wide range of industries, and Gartner predicts other physical augmentations will soon help people do their jobs better, faster and even more safely.[9] As these technologies evolve and increase in the workplace, however, organizations will need to balance their security risks with their benefits.

Migration to Windows 10

In January 2020, Microsoft ended its support of Windows® 7.[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. Investment in new PC hardware is rebounding after a time of decline, according to both Gartner and IDC.[11]

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 BYO

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

For workers, BYO 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.[12]

Security and privacy risks: The downside of BYO

C-level executives

12x

times more likely to be targeted

A growing number of employees want and/or expect to use their personal mobile devices, laptops, wearables and smart assistants 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 technology.

A recent report from Verizon® found that 33% of global data breaches included social attacks, and C-level executives were 12 times more likely to be targeted.[13] These numbers prove that cybercriminals are still exploiting human error within organizations. Industry analyst Aberdeen estimates that the annual business impact from mobile phishing attacks reaches more than $200 million, with a median cost of about $500,000.[14]

The BYO 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 mobile devices, computers, wearables and smart assistants with deficient security

Internal: corporate data leakage by employees and third parties via simple errors, well-intentioned workarounds, 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.

Affected organizations also face potentially massive fines if they don't meet the requirements of the General Data Protection Regulation (GDPR) for protecting customers' personal data. 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. Other jurisdictions have begun enacting similar laws, such as the California Consumer Privacy Act of 2018.

The traditional methods used to secure corporate data on personal mobile devices and 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 BYO – 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 mobile devices, computers, wearables and smart assistants could outweigh any benefits. The new era of enterprise technology demands new security solutions. While many solutions may promise full business productivity on employee technology, organizations should keep the following requirements in mind as they consider their options.

Can the solution...

1. Enable a zero trust approach while delivering a zero touch experience, and even allow users to work offline?

A zero trust security model protects against cyberthreats by trusting nothing and no one by default. But employees must still be able to access what they need to work, anytime and anywhere — without having to jump through hoops.

2. Ensure cost-effective, end-to-end encryption?

Organizations need reliable security. Although VPN and VDI can secure a network connection, the costs associated with licensing, hardware, software, infrastructure and help desk support add up quickly. These legacy technologies also fail to effectively safeguard against the growing threat of malware and other cyberthreats.

3. Support 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 whatever technology they choose.

BlackBerry

Smarter security from BlackBerry: A solution for the new era of BYO

The next generation of security threats sparked the next generation of smarter security from the leader in mobile security. Always adapting, AI-enabled BlackBerry® software is human nature-proof, protecting employee smartphones, laptops, tablets, wearables and smart assistants at the device, app and content levels.

Most employees don't intentionally adopt poor security habits. However, organizations must mitigate the effects of human nature — and accommodate the high expectations of today's digitally savvy users — while ensuring security and privacy.

BlackBerry® offerings for desktop on Windows® 10 and macOS® allow enterprises to benefit from BYOL, 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.

And now, with BlackBerry Intelligent Security, enterprises can embrace the next generation of BYO and all its advantages. Going beyond the rigid BYO security policies that organizations have traditionally used, it delivers security that changes based on where, when and how employees are working. So enterprises get cost-effective protection from escalating security threats, and employees get the freedom to be productive wherever, whenever on their preferred mobile device, wearable or smart assistant.

Ten Key Benefits

1. 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.

2. Provides an extra layer of AI-driven security for BYO mobile devices AND BYO desktop

CylancePROTECT — a leading-edge, AI-based malware solution — delivers native Mobile Threat Detection in BlackBerry UEM. It works at the device and application level to prevent, detect and remediate threats without disrupting usability and productivity.

And CylancePROTECT for BlackBerry Desktop delivers next-generation antivirus and malware protection to critical desktop tools, enabling convenient and secure access to enterprise resources on personal or non-corporate managed Windows 10® and macOS® devices and continuous protection against cyberattacks.

3. Bridges the gap between zero trust and zero touch

BlackBerry Zero Trust Architecture leverages AI to provide continuous, contextual authentication across the full spectrum of devices, networks, apps and users while still delivering the zero-touch experience that employees want and need: instant access to corporate resources with minimal hassle.

4. Allows real-time risk scoring on any device

BlackBerry Intelligent Security dynamically adapts the security requirements of protected employee devices and apps to individual users' real-world experience based on factors such as geographic location, network trust, and time and usage anomalies. Based on these scores, users may be granted access, receive an authentication challenge or generate a security alert.

5. Reduces costs and maintenance complexity

BlackBerry® Access removes the need to provision and maintain corporate mobile devices, computers and software, wearables and smart assistants, 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.

6. 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.

7. 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.

8. Supports uninterrupted workflows – even offline

BlackBerry® Access delivers online and offline access to BlackBerry® Digital Workplace — a multi-OS, browser-based all-in-one mobile productivity app with continuous malware and virus protection from CylancePROTECT. BlackBerry® Digital Workplace combines email, calendar, contacts and a secure, inbuilt document editor: the same set of capabilities as corporate-owned/managed computers for full business productivity on smartphones, laptops, wearables and smart assistants.

9. 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 mobile devices, laptops, tablets, wearables and smart assistants.

10. 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 provide enhanced collaboration and security.

In the 2019 Gartner Critical Capabilities for Unified Endpoint Management Tools report, BlackBerry UEM achieved the highest scores for two primary use cases (Nontraditional Device Management and Highly Secure and Regulated Industries), and the second highest score in a third use case (Unmanaged Devices/BYO). Find out more.

There is no turning back for the BYO revolution. There are now more mobile devices in the world than people.[15]

Worldwide spending on wearables alone will total $52 million in 2020, an increase of 27% from 2019.[16] The US smart assistant market is anticipated to grow at an average annual rate of over 20% to reach $9 billion in revenue by 2023.[17] Most importantly, employees' preference for using their own devices is deeply entrenched.

Today the BYO movement has reached a new level of complexity – introducing a new level of potential threats to organizations – but it still offers opportunities to save money on hardware, software, provisioning and help desk costs. BlackBerry's smart, cost-effective, AI-powered platform safeguards critical data on all BYO while improving productivity. Whether it's smartphones, laptops, tablets, wearables or smart assistants, employees get the power of choice and organizations get end-to-end security. Learn more

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points — from cars to smartphones — making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ. For more information, visit BlackBerry.com

1 https://research.checkpoint.com/2019/cyber-attack-trends-2019-mid-year-report/
2 https://www.prnewswire.com/news-releases/investors-and-boards-support-ceo-action-on-global-challenges-ey-survey-finds-300880595.html
3 https://www.computerworld.com/resources/152625/how-to-manage-mobile-app-madness
4 https://www.blackberry.com/us/en/forms/enterprise/wp-bis-zero-trust-enterprise-mobility
5 https://www.statista.com/statistics/247554/global-enterprise-application-software-revenue/
6 https://www.entrepreneur.com/article/327778
7 https://www.idc.com/getdoc.jsp?containerId=US42890217
8 https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2020-and-beyond/
9 https://www.gartner.com/en/newsroom/press-releases/2019-22-10-gartner-unveils-top-predictions-for-it-organizations-and-users-in-2020-and-beyond
10 https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows-7-to-windows-10-upgrade-automated
11 https://www.computerweekly.com/microscope/news/252466647/Windows-migration-helping-drive-growth-in-the-PC-market
12 https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/#2c6c84d81f30
13 https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf
14 https://www.blackberry.com/us/en/forms/enterprise/wp-bis-zero-trust-enterprise-mobility
15 https://www.bankmycell.com/blog/how-many-phones-are-in-the-world
16 https://www.gartner.com/en/newsroom/press-releases/2019-10-30-gartner-says-global-end-user-spending-on-wearable-dev
17 https://www.prnewswire.com/news-releases/smart-speaker-market-in-us---industry-outlook-and-forecast-2018-2023-siri-apple-alexa-amazon-google-assistant-google-and-cortana-microsoft-influencing-the-market-300771871.html