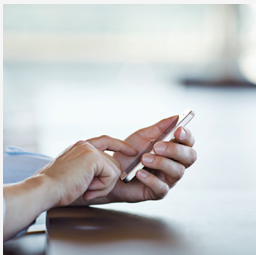# 10 Reasons To Bring All Your Endpoints Under One Roof

Secure, Control, and Consolidate on a Single Platform

iOS

macOS

Executive Summary

The market for Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) has evolved. These management strategies were designed chiefly for smartphones and tablets when the BYOD movement was in its preliminary stages. Just when organizations were becoming proficient at traditional endpoint management, a new disruptor arrived – the Internet of Things (IoT) – bringing a raft of new connected devices.

MDM and EMM are not equipped to manage the emerging Enterprise of Things (EoT), made up of all the IoT devices in today's workplace. New use cases and the increasing fragmentation of endpoints present new security and logistical challenges that demand a different management approach.

BlackBerry

Traditional Endpoints and EoT Endpoints

It's no longer enough for organizations to focus exclusively on securing smartphones, tablets and laptops. There is massive growth in the number of connected devices: Gartner forecasts that more than 20 billion connected things will be in use worldwide by 2020, and millions of new things get connected every day. [1]

A survey of 200 enterprise IT decision-makers from 10 countries in multiple industries by 451 Research found the most common endpoints under management are still laptops and PCs, smartphones/tablets and cameras/surveillance technology.[2] Yet respondents also listed a growing and diverse number of IoT devices used to optimize operations and customer service.

Data breaches in EoT endpoints can result in major direct financial losses and indirect losses through reputational damage. Ensuring the safety and data security of EoT endpoints is a top challenge and priority for IT decisions-makers today, according to the 451 Research report. [3]

Current Landscape of Endpoint Management

Several factors have combined to result in a patchwork approach to endpoint management at many organizations:

- The persistence of legacy investments in security and management systems that support only one class of endpoints

- A separation between management responsibility for enterprise mobility endpoints (with IT managers) and EoT endpoints (with operational technology or line-of-business managers), resulting in two silos

- Multiple user groups, ownership models (BYOD, BYOC, Corporate Owned Personally Enabled - COPE, Corporate Owned Business Only - COBO), deployment models (container, OS embedded, native), and operating systems and device types, resulting in several management platforms (sometimes from different vendors)

According to the 451 Research survey, 100% of respondents reported that their organizations have deployed at least one type of solution to secure endpoint data, with 90% reporting use of eight or more solutions.[4] The most widely used solutions are anti-malware, VPN, Data Loss Prevention software, and EMM, MDM or other management tools. Taken together, the survey data reveals that most organizations have not deployed a single solution capable of addressing the multiple risks around endpoint data.

BlackBerry

The Pitfalls Of Deploying Multiple Endpoint Management Strategies

A patchwork approach to endpoint management can produce deep complexity and multiple challenges for organizations. Using traditional PC management tools and remote access technology (such as VPN) can be more expensive and often requires more IT support. For mobile endpoints, using multiple EMM/MDM platforms can result in:

Higher IT costs
- From multiple vendors and contracts, multiple infrastructures, and increased staff and training requirements

Increased security risks
- Point solutions potentially create gaps and expand cyberattack surface
- Inconsistent policies, groups and users may increase risk

Poor user experience
- Complex provisioning process
- Multiple admin consoles for IT to use
- Inconsistent user experiences on different platforms
- No universal sign-on
- Multiple help desks

Inefficient compliance processes
- Multiple approaches for each regulation increases chance of errors
- Difficult to have unified view of compliance status

BlackBerry

The Next Stage In Endpoint Management: Unified Endpoint Management

Given these many potential drawbacks, many organizations are recognizing the need to take the next step in endpoint management. The 451 Research survey found the concept of unifying all endpoint security and management within a single system holds strong appeal among decision-makers, with 78% saying they would be interested if there were solutions available. [5]

Beyond the obvious benefits of lower costs and ease of use, any consolidated endpoint management strategy must preserve optimal productivity and security to add value to an organization. Business leaders want to support employee productivity with wider adoption of computing solutions, flexible deployment and a wide variety of user support models – all within budget constraints. For IT leaders, the priority is to ensure every device is secure, including new endpoints like smart glasses and future intelligent devices in the enterprise.

78% of decision-makers are interested in unifying all endpoint security and management within a single system

In the 451 Research survey, 63% of respondents said security concerns are an obstacle to successfully achieving digital transformation goals.[6] Viewing traditional and mobile endpoints and IoT endpoints as two separate categories requiring separate security and management can also hinder progress towards these goals. Unified Endpoint Management (UEM) can bring your organization to the next stage of digital transformation, offering one platform with multiple competitive benefits.

BlackBerry

BlackBerry Unified Endpoint Management (UEM)

BlackBerry® UEM delivers complete, unified endpoint management and policy control for the diverse and growing fleet of devices and apps in today's organizations. With a single management platform and trusted end-to-end security, BlackBerry UEM is designed to help increase the productivity of the mobile workforce and realize the operational benefits of the EoT. It enables organizations to secure and manage devices, apps, data and policies— all without sacrificing functionality or flexibility.

Top 10 reasons to choose BlackBerry UEM:

1. It secures your data – everywhere it goes.

Whether your security needs are basic or complex, BlackBerry UEM offers the essential security and control that must be in place before you give employees access to key business productivity tools and network resources. With BlackBerry UEM, users are BlackBerry® Secure™. It supports any mobile security strategy from a single platform, including:

- Native management leveraging OS MDM controls

- BlackBerry® Work for secure Personal Information Management (PIM)

- BlackBerry® Dynamics™ App Development Platform for securing and enabling third-party apps as well as custom apps

- Un-managed device scenarios, or app-centric approaches

- Native container solutions such as Android™ Enterprise and Samsung KNOX™ Workspace

- Native protection capabilities for iOS® and Windows® 10 BlackBerry® Workspaces file-level data protection

BlackBerry UEM provides seamless access to resources behind the firewall for iOS, Android Enterprise and Samsung KNOX Workspaces, while BlackBerry Dynamics provides the same access for Windows 10 and macOS – without any additional network configuration changes or VPN requirements. In addition, BlackBerry UEM does not require the use of any inbound network ports, leveraging outbound ports only.

BlackBerry

BlackBerry: #1 in mobile security software

- Tied for first place in IDC EMM global market share report; the outright market share leader in Western Europe[7]

- A leader in the 2017 Magic Quadrant for EMM for the second year in a row[8]

- Ranks highest in all six use cases of Gartner's 2017 Critical Capabilities for High-Security Mobility Management for the second year in a row[9]

2. It delivers unified, multi-OS endpoint management across all ownership models.

BlackBerry UEM provides a single, integrated view of the users, devices, apps and policies in your environment. You get comprehensive support for devices operating on a wide range of platforms (including iOS, Android™, Android Enterprise, Samsung KNOX, Windows, macOS, BlackBerry, watchOS and Android Wear), all managed from one console. BlackBerry UEM is designed for BYOD, BYOC, COPE and COBO ownership models. Most organizations require varying levels of security and management for a mix of personal and corporate devices, including individual users with multiple devices. These requirements include leading security and user experience for unmanaged personal devices, advanced security and controls for corporate-owned devices, and unique requirements for specialized use cases such as kiosks.

Secure and manage your apps from a single platform with BlackBerry Dynamics

BlackBerry Dynamics, managed by BlackBerry UEM, allows organizations to deploy and manage secure custom and third-party business apps from the same console. It provides full multi-OS containerization for advanced mobile workflows.

3. It's built to secure and manage the growing number of endpoints in the Enterprise of Things, as well as new classes of devices.

As connected devices become more pervasive in the enterprise, BlackBerry UEM enables you to secure current and future EoT endpoints with a unified platform. Wearable devices are increasingly common,[10] for example, and BlackBerry UEM allows IT to apply a consistent platform and management approach across all these devices.

4. It enables the mobile workforce with the Microsoft apps they need.

BlackBerry UEM manages and applies security to Microsoft® Office 365® apps on iOS and Android devices, giving users access to native Microsoft Office productivity experiences. From BlackBerry UEM, administrators can apply Microsoft® Intune app protection policies to Microsoft Office 365 apps. BlackBerry Workspaces, managed by BlackBerry UEM, can apply digital rights management to all Office documents. These capabilities allow users to mobilize content and content repositories like Microsoft® SharePoint and Microsoft® OneDrive™.

5. It helps organizations reduce risks and meet regulatory compliance requirements.

By providing comprehensive security, visibility and control, BlackBerry UEM helps organizations in even the most highly regulated industries meet their compliance requirements (for example by allowing efficient auditing of all device communications).

6. It protects your business by protecting employee privacy.

BlackBerry UEM makes it simple to safeguard employee privacy using containerization, helping your organization avoid legal complications by establishing a clear separation between employees' private content and sensitive business data. BlackBerry UEM can even provision a work phone line to your employees' personal devices, without disrupting or impacting employee privacy.

7. It delivers a consistent user experience.

Unlike patchwork endpoint management strategies, BlackBerry UEM makes it easy and intuitive for users to securely access the information they need, using the devices and apps they prefer. It is a management platform for all intelligent endpoints in the enterprise, including users, devices, apps and content.

8. It reduces your Total Cost of Ownership (TCO).

BlackBerry UEM offers low TCO by:

- Reducing hardware costs with the choice of a single-server footprint or cloud deployment

- Eliminating VPN licenses

- Lowering training costs by making it easy to use for both IT and end users

- Decreasing IT resource burden with its self-serve user portal and single-console interface

9. It's flexible, extensible and ready to evolve with your organization.

BlackBerry UEM is a highly scalable solution, creating a solid foundation for your future mobile and EoT initiatives. A single BlackBerry UEM server can support 25,000 users, easily supporting even the largest organizations. It is available as a cloud-based or on-premises deployment and can be migrated to the cloud if your business needs change in the future.

10. It enables easy snap-in with homegrown IT management platforms.

BlackBerry® UEM Integration SDK allows you to take advantage of all the features and benefits of BlackBerry UEM while integrating with capabilities from your organization's internal systems. BlackBerry® UEM Integration SDK allows you to add new capabilities to BlackBerry UEM as well as incorporate UEM capabilities into your existing systems and processes.

Conclusion

Consolidating your management and security strategy for both traditional and EoT endpoints can enhance security and create cost efficiencies – without sacrificing productivity. BlackBerry UEM unifies your mobile strategy by bringing all your intelligent endpoints onto a single management platform.

BlackBerry UEM is constantly evolving to meet new business requirements. Not only does it manage today's endpoints, apps, content, data and security, it also prepares your organization for future challenges and opportunities. With BlackBerry UEM, you can be ready for the Enterprise of Things.

Sources

1. https://www.gartner.com/newsroom/id/3165317

2. https://global.blackberry.com/en/register-to-download?downloadurl=/content/dam/blackberry-com/asset/enterprise/pdf/wp-451-research-securing-eot.pdf

3. https://global.blackberry.com/en/register-to-download?downloadurl=/content/dam/blackberry-com/asset/enterprise/pdf/wp-451-research-securing-eot.pdf

4. https://global.blackberry.com/en/register-to-download?downloadurl=/content/dam/blackberry-com/asset/enterprise/pdf/wp-451-research-securing-eot.pdf

5. https://global.blackberry.com/en/register-to-download?downloadurl=/content/dam/blackberry-com/asset/enterprise/pdf/wp-451-research-securing-eot.pdf

6. https://global.blackberry.com/en/register-to-download?downloadurl=/content/dam/blackberry-com/asset/enterprise/pdf/wp-451-research-securing-eot.pdf

7. https://www.idc.com/getdoc.jsp?containerId=US42890217

8. https://us.blackberry.com/enterprise/forms/gartner-emm-mq

9. https://us.blackberry.com/enterprise/forms/gartner-critical-capabilities

10. https://www.statista.com/statistics/487291/global-connected-wearable-devices/

BlackBerry