BlackBerry UEM and Microsoft Intune

Better Together: Achieving the Best Security & Productivity Outcomes

Summary

Enterprises need top-tier device governance and sovereign-grade data protection. Many of these same enterprises have a productivity strategy built around Microsoft® Office. For these organizations, BlackBerry® UEM and Microsoft® Intune work together to deliver a complete and uniquely complementary solution.

Together, they expand Microsoft's modern device, application, and identity management ecosystem. BlackBerry adds a secure container, certified encryption for data in transit, and a productivity suite designed for compliance and control.

Unlike other Unified Endpoint Management (UEM) solutions, this partnership enables organizations to achieve FIPS-validated and NIAP-accredited control of data across devices, applications, and networks. This provides a crucial advantage in regulated and security-focused environments.

An Enterprise Conundrum

Microsoft is widely recognized for its leadership in productivity solutions. A core strength of Intune lies in its ability to seamlessly manage the Microsoft® 365 suite of applications on mobile devices. Combined with Microsoft® Azure™ Active Directory® (now Microsoft® Entra ID), Intune extends access to content and resources behind the firewall, ensuring users remain productive while maintaining a consistent identity and access experience.

Many organizations believe that Intune provides a comprehensive and cost-effective Unified Endpoint Management (UEM) solution, often assuming it is *included* or *free* in their existing Microsoft licensing bundles. However, the total cost of ownership (TCO) can be higher than expected once all necessary security and management capabilities are factored in. For example, organizations often need to purchase or integrate additional tools to achieve compliance, threat detection, or data loss prevention, adding both cost and complexity.

It is also commonly believed that Microsoft can handle all operational and security requirements for an organization, which might lead organizations to adopt a single-vendor lock-in mentality. Customers often think Microsoft can serve as their OS provider, productivity suite, cloud host, UEM platform, and security solution—in an all-in-one package. To fill the missing security and management gaps, organizations must deploy add-ons, such as:

- VPN clients for secure end-to-end connectivity.
- Mobile security tools for threat detection or data encryption.
- Solutions for secure email, messaging, and collaboration outside Microsoft 365.
- MDM/UEM tools for managing non-Windows or mixed device fleets.

This *bundled security* forms a fragmented technology stack that introduces potential vulnerabilities, administrative burden, and inconsistent protection across devices, in addition to higher TCO and admin costs.

What Intune Offers

Intune offers native integration with Microsoft® Office 365® productivity apps. It also provides conditional access and identity offerings, making Intune is an obvious choice for Microsoft customers who are invested in its ecosystem.

While Intune's customer base spans many industries and geographies, the solution is less attractive to government and regulated customers due to stringent regulatory compliance and data security requirements. For example, the lack of FIPS 140-2 compliance for Intune and Tunnel (its VPN connectivity add-on) makes it infeasible for organizations, particularly as the transition to FIPS 140-3 and post-quantum cryptography (PQC) looms.

Organizations often underestimate the licensing and subscription costs of Intune, which can significantly contribute to the total cost of ownership (TCO). Intune is licensed with different pricing tiers and feature sets. While the base licensing fees may appear reasonable, the true TCO can quickly escalate when factoring in the need for additional licenses to cover all add-on services, devices and users within an organization. The Intune pricing model can be complex, with the potential for unexpected cost increases due to changes in licensing requirements or the addition of new features. Organizations may need to purchase higher-tier licenses or add-ons to access critical functionality, further increasing TCO.

Better Together

Using BlackBerry UEM alongside Intune bridges the common security and management gaps in Intune deployments. This *better-together* approach not only enhances security but also helps manage—and even reduce—the total cost of ownership (TCO). By strengthening Intune for security-focused users, organizations can save on add-ons and opt for a lower-tier base package, maximizing cost efficiency.

Pairing BlackBerry UEM with Intune helps keep TCO down while ensuring customers meet compliance needs. This is especially crucial as communication threats grow, including the emerging risks posed by quantum computing.

The key to resolving this security challenge is to look beyond the productivity and OS layers and instead focus on security as the foundation, not an afterthought. For example, attackers can compromise data in Personal Information Management (PIM) apps if protection relies solely on the mobile OS. A truly secure architecture, like that provided by BlackBerry UEM, enforces encryption, isolation, and compliance controls at the container level, safeguarding data at rest and in transit across all apps and devices.

With a secure foundation in place, organizations gain peace of mind across the entire productivity stack, reducing the need for multiple add-on products, improving compliance readiness, and maintaining flexibility to choose best-in-class solutions rather than being constrained by a single vendor ecosystem.

Here are six reasons BlackBerry UEM, paired with Microsoft Intune, is the best approach for security-focused organizations.

1. Securing Productivity Without Compromise

Modern workforces need seamless access to Microsoft 365, Microsoft Teams®, and other business apps on mobile devices. BlackBerry UEM goes beyond policy enforcement and app distribution to provide:

- Persistent protection of data at rest and in transit**.**
- Effective containment of data leakage when a device or session is compromised.
- Certified cryptographic assurance demanded by regulated industries.

The effectiveness of security baselines applied through Intune depends on the security of the underlying Host OS. If the Host OS is compromised or has unpatched vulnerabilities, it could undermine the security policies enforced through Intune and expose work data. Other MDM/MAM solutions fail to help Intune mitigate this risk.

Better Together:

BlackBerry UEM addresses these gaps by providing a foundational security layer that integrates directly with Intune's conditional access and identity controls, without impacting productivity.

2. Securing Data at Rest and in Transit

BlackBerry UEM employs FIPS 140-2-validated encryption (migrating to FIPS 140-3) to protect both device-stored data and live communications:

Security Dimension	Microsoft Intune	With BlackBerry UEM
Data at Rest	OS-level encryption and app sandboxing	BlackBerry® Dynamics™ container isolates all business data; encrypts with independent keys and prevents data exfiltration or unauthorized copy/paste.
Data in Transit	Standard TLS/HTTPS between device and Microsoft cloud	BlackBerry provides end-to-end encryption with Elliptic curve cryptography, certificate-based authentication, and inspection-resistant tunneling for Office apps and third-party services.
	No plan for FIPS 140-2 or FIPS 140-3	FIPS 140-2 accredited with a path to achieving FIPS 140-3 with quantum readiness achieved through adopting NIST PQC algorithms.
Compromised Devices	Conditional access can block future logins	BlackBerry UEM policy instantly wipes or blocks container access; no residual corporate data remains on device storage.

Better Together:

This layered approach ensures zero leakage even if the underlying OS or app environment is compromised. Users of Intune get true cryptographic separation between work and personal environments, ensuring personal data privacy and protecting work data, while also opening the possibility of true BYOD deployments. The future of data in transit remains secure, with a clear path toward FIPS 140-3 compliance and becoming 'Quantum-Ready'.

3. Conditional Access and Real-Time Policy Enforcement

When integrated with Entra ID (Azure AD), BlackBerry UEM adds device posture and compliance data directly into Intune's Conditional Access engine.

This enables:

- Real-time enforcement based on device health, certificate validity, and container integrity.
- Adaptive access decisions for Office 365, Teams, and other SaaS apps.
- Granular per-app VPN routing through BlackBerry® Access for secure cloud connectivity.

Better Together:

A combined architecture allows only trusted, compliant, and encrypted endpoints to reach sensitive corporate or government resources. Conditional access is more effective.

4. Secure Productivity With MS Office Apps

For organizations using Microsoft 365, BlackBerry® Bridge delivers a seamless, secure experience:

- Users can open, edit, and save Office documents within the BlackBerry Dynamics container using native Microsoft Office mobile apps.
- Corporate data stays protected inside the encrypted workspace, even when users collaborate in Microsoft® Outlook® or Teams.
- BlackBerry Bridge stays aligned with Microsoft Intune and BlackBerry UEM policies, ensuring that both systems honor the same DLP, encryption, and conditional-access rules.

Better Together:

This joint capability eliminates the trade-off between usability and compliance, enabling secure productivity at scale.

5. Enterprise App Ecosystem

As a security platform, BlackBerry provides the BlackBerry® Dynamics™ SDK for adding existing Enterprise productivity apps in a secure environment. This enables the growth of a healthy ISV ecosystem and the extension of secure use-case compatibility. The BlackBerry Dynamics SDK contains a large library of pre-integrated enterprise applications, from secure browsers, file editors, and CRM tools to industry-specific applications.

- All BlackBerry Dynamics enabled apps inherit the same security posture: encrypted data storage, controlled data sharing, and certificate-based authentication.
- Developers can easily wrap or integrate third-party apps into the container, expanding the reach of Intune without compromising control.
- The current ISV ecosystem boasts 127+ secure enterprise apps across 100+ ISV partners.

Better Together:

Intune provides users with secure access to a broader range of enterprise apps, enabling a richer, more secure application ecosystem – far more than other UEM vendors.

6. Enhancing User Experience – Outlook

BlackBerry® Work is purpose-built for secure enterprise mobility, designed from the ground up with FIPS-validated encryption, containerization, and a consistent user experience across all devices. Unlike Microsoft® Outlook® Mobile, which evolved from a consumer-grade app and relies heavily on the underlying mobile OS for data protection, BlackBerry Work operates independently within the secure BlackBerry Dynamics container. This separation of work and personal data not only enforces strict compliance and policy controls but also ensures the secured workspace keeps sensitive

corporate information inside at all times. Its design enables users to access email, calendar, and contacts with confidence, knowing that data is protected both at rest and in transit.

Better Together:

BlackBerry Work enhances the Microsoft productivity experience by providing a hardened layer of security without sacrificing usability. The result is a unified user experience that delivers both enterprise-grade protection and frictionless productivity. Users get secure access to Microsoft content while BlackBerry maintains compliance and control.

BlackBerry UEM and Microsoft Intune: Better Together

In a hybrid workforce, device management alone or app management alone is not enough. BlackBerry UEM enables organizations with sovereign-grade data protection, certified cryptography, and full control of the Microsoft Intune environment, transforming it into a truly secure productivity platform. Together, BlackBerry UEM and Microsoft Intune deliver unmatched risk reduction and operational assurance.

Talk to an expert

Contact us today to learn more about BlackBerry UEM or visit blackberry.com/securecomms

ABOUT BLACKBERRY

BlackBerry (NYSE: BB; TSX: BB) provides enterprises and governments the intelligent software and services that power the world around us. Based in Waterloo, Ontario, the company's high-performance foundational software enables major automakers and industrial giants alike to unlock transformative applications, drive new revenue streams and launch innovative business models, all without sacrificing safety, security, and reliability. With a deep heritage in Secure Communications, BlackBerry delivers operational resiliency with a comprehensive, highly secure, and extensively certified portfolio for mobile fortification, mission-critical communications, and critical events management.

BB25 | 250206