Why Switch to BlackBerry UEM

Comparing Solutions for Resilience and Data Sovereignty

Mobility sits at the heart of employee activity across government and enterprise operations. Deployments today demand a delicate balance between preserving data integrity, providing a seamless user experience, and ensuring absolute privacy.

Governments and organizations worldwide now face an unprecedented convergence of threats to their mobile infrastructure: nation-state adversaries probing endpoint management platforms, regulatory bodies mandating rapid vendor disconnects, and a geopolitical environment demanding complete data sovereignty. The choice of a Unified Endpoint Management (UEM) platform is no longer merely a procurement decision; it is a national security decision.

Since 2023, the consequences of selecting the wrong UEM platform have become starkly visible. Ivanti suffered 12 critical Common Vulnerabilities and Exposures (CVEs) on its UEM platform alone during this period. In 2024, the CISA Emergency Directive ED 24-01 triggered mandatory disconnection orders for all Federal Civilian Executive Branch (FCEB) agencies in the United States (CISA, 2024). These are not isolated incidents; they represent systemic failures of platforms built primarily for commercial enterprise convenience rather than sovereign resilience. Intune and Omnissa (formerly VMware Workspace ONE) have also experienced multiple CVEs.[1]

This white paper evaluates BlackBerry UEM, Ivanti, Microsoft Intune, and Omnissa against the sovereignty, security, certification, and resilience requirements that matter most to government, enterprise, and critical infrastructure organizations.

The UEM Crisis: Why Commercial Platforms Fail Sovereign Security Requirements

Modern endpoint management platforms sit at the heart of government digital infrastructure. They control device enrollment, policy enforcement, application distribution, and, critically, cryptographic key management. A vulnerability in a UEM platform is not merely an IT problem; it is a potential vector for full network compromise, data exfiltration, and mission failure.

Yet the market is dominated by platforms designed for commercial enterprise agility, not sovereign security. The result is a growing and dangerous misalignment between what governments need and what most UEM vendors deliver.

Five Critical Challenges Facing Government UEM Decision-Makers

1. Sovereignty gaps

Most commercial UEM platforms are cloud-centric, routing device telemetry, policies, and credentials through vendor-controlled infrastructure. For governments requiring data residency, air-gapped operations, or classified network support, this represents an unacceptable risk, yet many platforms cannot guarantee it.

2. Certification deficits

NIAP Common Criteria, BSI, NATO NIAPC, and FIPS 140-2/3 certifications are not marketing achievements; they are evidence of independently verified security architecture. These certifications

require rigorous third-party testing by government security authorities. Most competitors hold limited or no coverage across these frameworks, leaving procurement teams unable to demonstrate compliance with security mandates.

3. **Vulnerability exposure**

Commercial UEM platforms optimized for feature velocity over security rigor create systemic risk at national scale. When a UEM platform is compromised, every endpoint it manages becomes vulnerable.

4. **Post-quantum readiness**

Cryptographically relevant quantum computers are approaching operational viability within defense planning horizons. UEM platforms not already aligned to NIST post-quantum standards (FIPS 203-205) leave governments exposed to harvest-now-decrypt-later attacks today. Adversaries are already collecting encrypted data for future decryption.

5. **Integration complexity**

Government environments increasingly operate across Microsoft 365, classified networks, legacy infrastructure, and mobile-first field operations. UEM platforms must integrate seamlessly across these ecosystems without introducing new attack surfaces or operational friction.

Competitive Landscape

Ivanti: Security and Operational Risk Considerations

Ivanti's UEM platform accumulated **12 critical CVEs** between 2023 and 2026 (NIST NVD, 2026)1, triggering CISA Emergency Directive ED 24-01—a mandatory disconnection order across all FCEB agencies (CISA, 2024) 2. This was not a precautionary measure; it was a response to active nation-state exploitation.

Key Ivanti limitations for government customers:

- **Sovereign deployment constraints:** Ivanti's cloud-centric architecture limits fully sovereign on-premises deployment options needed for high-assurance government environments.
- **Certification gaps:** Ivanti lacks BSI certification and does not have NATO NIAPC recognition, reducing its suitability for NATO-aligned procurement requirements.
- **FIPS cryptography coverage: I**vanti offers limited FIPS 140-2/3 validated cryptographic coverage compared to platforms built for regulated government use.
- **Post-quantum posture:** Ivanti has no publicly confirmed roadmap aligned to NIST post-quantum standards (FIPS 203–205) for the UEM layer.
- **Security architecture:** Ivanti relies primarily on OS-level controls rather than application-level cryptographic isolation, increasing exposure if the OS is compromised.
- **Air-gapped/dark-site support:** Ivanti does not provide verified support for fully air-gapped or dark-site operations required in classified environments.
- **Multi-tenant model fit:** Ivanti's cloud-only multi-tenant management model is poorly suited for hybrid and dark-site government operations.
- **Support experience risk:** Reported customer support satisfaction (NPS 28) is materially below typical enterprise benchmarks, increasing operational risk during incidents and migrations.
- **Microsoft ecosystem integration:** Ivanti provides only basic Microsoft 365 and Intune integration, limiting co-management and migration-friendly architectures.

For any government agency or critical infrastructure operator that has been operating Ivanti, the federal disconnect order and chronic vulnerability record represent a clear and urgent signal to migrate to a platform built on sovereign security principles.

Microsoft Intune: Cloud Strengths and Sovereignty Constraints

Microsoft Intune has significant enterprise adoption through its deep integration with the Microsoft 365 ecosystem. For commercial enterprises operating entirely within the Microsoft cloud, Intune offers genuine value. However, for government and critical infrastructure customers, Intune falls short of the sovereign deployment capabilities BlackBerry UEM is built to deliver.

Key Intune considerations for government customers:

- **Cloud dependency:** Intune is a cloud native service tightly integrated with Microsoft Entra ID and the Microsoft cloud, but it does not support fully air-gapped or dark site deployments required for classified or extremely sensitive government environments.
- **Sovereignty limitations:** Data residency, tenant isolation, and the absence of foreign-controlled infrastructure are non-negotiable for many governments. Intune's architecture does not provide the complete infrastructure sovereignty that on-premises or hybrid dark site deployment models offer.
- **Certification scope:** While Intune benefits from Microsoft's broader FedRAMP and compliance certifications, it lacks NIAP UEM-specific, BSI, and NATO NIAPC certification at BlackBerry UEM's level.
- **Post-quantum posture:** Microsoft has begun post-quantum research across its platform, but Intune's UEM layer lacks publicly confirmed FIPS 203–205 post-quantum certification.
- **Security architecture:** Intune enforces policies at the OS and MDM profile level, but it does not provide application-level cryptographic isolation independent of the operating system. This matters in environments where OS compromise must not expose secure communications.
- **Competitive context:** Where BlackBerry UEM complements Intune: BlackBerry UEM is a Microsoft Intune Partner and supports Entra CA integration and BRIDGE for secure Microsoft Office document editing. This allows BlackBerry UEM to work alongside Intune, strengthening Microsoft environments with sovereign-grade security rather than replacing existing investments.

For organizations standardized on Microsoft, BlackBerry UEM partners with Intune and integrates with Entra CA to provide a migration-friendly path to sovereign endpoint management without giving up existing Microsoft productivity investments.

Omnissa (VMware Workspace ONE): Deployment and Certification Considerations

Omnissa, now operating Workspace ONE after Broadcom's acquisition and divestiture, retains broad device management capabilities. However, ownership disruption and a commercial-first architecture leave significant gaps for government customers.

Key Omnissa considerations for government customers:

- **Deployment model:** Omnissa Workspace ONE supports on-premises deployment through Unified Access Gateway and on-prem components, but its strategy is increasingly cloud-focused. As a result, support for fully air-gapped, dark site, or classified environments is more limited than the purpose-built sovereign deployment capabilities of BlackBerry UEM.
- **Certification posture:** Workspace ONE holds some government-relevant certifications, including FedRAMP authorization for its cloud offering, but lacks NIAP Common Criteria UEM Server and

Android Client certifications, BSI certification with NATO recognition, or NIAPC approval at NATO Restricted classification, certifications held by BlackBerry UEM.

- **Security architecture:** Workspace ONE applies security at the MDM profile and OS configuration layers but does not cryptographically isolate applications from the operating system.
- Post-quantum readiness: No independently verified NIST FIPS 203-205 aligned post-quantum roadmap has been published for the Workspace ONE UEM layer.
- **Organizational continuity risk:** Broadcom's acquisition and the later Omnissa divestiture raised uncertainty around Workspace ONE's roadmap, licensing stability, and long-term vendor commitments for government customers on multi-year procurement cycles, this uncertainty adds risk to Workspace ONE, risk that BlackBerry UEM does not carry as a dedicated secure communications vendor.
- **FIPS cryptography:** Limited FIPS 140-2/3 validated cryptographic coverage compared to the comprehensive implementation of BlackBerry UEM.

These challenges demand a UEM platform purpose-built for sovereign operations from the ground up. BlackBerry UEM is that platform.

BlackBerry® UEM: Assessment Against Sovereign Deployment Requirements

BlackBerry® UEM stands apart. With zero CVEs over a five-year period from 2021 to 2026, NIAP/Common Criteria certification, BSI certification with NATO recognition, NIAPC approval at NATO Restricted classification, and a post-quantum cryptography roadmap aligned to NIST FIPS 203-205, BlackBerry UEM is a purpose-built endpoint management solution in high-security environments for organizations where failure is not an option.

Figure 1: Securing Communications for all required Outcomes

The BlackBerry UEM Suite delivers comprehensive security and streamlined enterprise endpoint management, designed to meet the needs of a dynamic and hybrid workforce, particularly within the most demanding enterprise, government, and critical infrastructure environments.

What distinguishes BlackBerry UEM is not a single feature; it is the totality of a platform purpose-engineered for sovereign operation from the ground up. BlackBerry UEM is built on a foundation of security, ensuring security follows all communications, while saving on additional security add-ons.

Deployment Model Comparison

BlackBerry UEM is the only UEM platform that supports the complete spectrum of sovereign deployment models:

- **On-Premises**: Full deployment within customer-controlled infrastructure, with no dependency on BlackBerry or any third-party cloud service. Policies, credentials, device data, and telemetry never leave the organization's physical perimeter.
- **Cloud:** For organizations requiring cloud delivery, BlackBerry UEM cloud deployments maintain rigorous data residency and sovereignty controls.
- **Hybrid:** Mixed on-premises and cloud deployment, allowing organizations to maintain classified or sensitive workloads on-premises while leveraging cloud efficiency for lower-classification endpoints.
- **Dark Site:** Fully air-gapped deployment for classified networks, SCIF environments, and operational theater deployments where internet connectivity is unavailable or prohibited. No other major UEM platform supports dark site deployment at this level of maturity and certification.
- **Bright Site:** Controlled internet-connected deployment for sensitive but unclassified operations requiring external connectivity management.

This deployment flexibility eliminates the fundamental sovereignty risk inherent in cloud-dependent platforms. Organizations can deploy BlackBerry UEM entirely within their own jurisdiction, on their own hardware, under their own security controls, with no foreign-controlled systems in the data path.

Security Architecture: App-Level Cryptographic Isolation

While competitors enforce security at the OS and MDM profile level, BlackBerry UEM implements application-level cryptographic isolation independent of the operating system**.** This architectural distinction is fundamental.

In a threat environment where OS-level compromise is a realistic adversary objective, security controls that depend entirely on OS integrity are insufficient; see Figure 2.

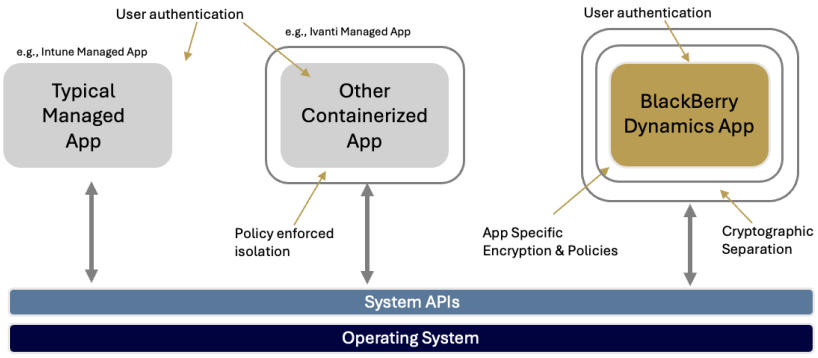

Figure 2: Securing Data at Rest with Cryptographic Isolation

The BlackBerry UEM solution's app-level isolation means:

- Cryptographic keys are managed at the application layer, not exposed to OS-level processes.
- A compromised operating system cannot trivially access encrypted enterprise data or communications.
- Secure container separation is maintained even when OS vulnerabilities have been exploited.

This architecture ensures that even if an adversary achieves OS-level access through zero-day exploits, enterprise data protected within the BlackBerry secure container remains cryptographically isolated and inaccessible.

Comprehensive Comparison: How The Solutions Compare

This comparison evaluates UEM platforms against the deployment, certification, security, and operational resilience requirements most relevant to government, critical infrastructure, and other high-security environments.

Metric	BlackBerry UEM	Ivanti UEM/Neurons	Microsoft Intune	Omnissa (Workspace ONE)
Critical CVEs (UEM Platform, 2023–2026)	0	12	2	3
CISA Emergency Directives	None	ED 24-01	None	None
Federal Disconnect Mandates	None	Yes — all FCEB agencies	None	None
Sovereign Deployment	On-Prem, Cloud, Hybrid, Dark Site, Bright Site	Cloud-centric, limited on-prem	Cloud-native	SaaS based On-prem; no verified dark site
FIPS 140-2/3 Validated Crypto	Yes — Full	Limited	Partial	Limited
Post-Quantum Roadmap Assured	Yes (NIST FIPS 203-205 aligned)	No	Unconfirmed at UEM layer	No
Customer Support NPS	85 (Top Tier)	28[4]	N/A (Microsoft enterprise support)	N/A
Security Architecture	App-level crypto isolation — independent of OS	Relies on OS-level controls	OS/MDM profile-level controls	OS/MDM profile-level controls
Multi-Tenant Management	Unified Cloud + On-Prem MTM	Cloud-only MTM	Azure-only MTM	Cloud-primary MTM
MS 365 and Intune Integration	Entra CA, Intune Partner, BRIDGE for secure MS Office doc editing	Basic integration	Native (Microsoft ecosystem)	Moderate integration
Air-Gapped / Dark Site Support	Yes, fully verified (BSI)	No	No	No
Vendor Stability	Dedicated secure comms vendor	Recent security incidents	Major enterprise vendor	Post-acquisition transition (Broadcom → Omnissa)
Built-in Secure Connectivity	Yes	No	No	No

Abbreviations: CVE = Common Vulnerabilities and Exposures; FCEB = Federal Civilian Executive Branch; MTM = Multi-Tenant Management; Entra CA = Microsoft Entra Certificate Authority.

The Certification Portfolio That Matters

BlackBerry UEM holds the most comprehensive government certification portfolio among these UEM platforms[5,6,7,8]:

Certification	BlackBerry UEM	Ivanti UEM/Neurons	Microsoft Intune	Omnissa Workspace ONE
NIAP/Common Criteria	✓ Full Coverage	Limited	Limited	Limited
FIPS 140-2/3 Validated Cryptography	✓ Yes	Limited	At Server	Limited
BSI Certified (Germany) + NATO Recognition	✓ Yes	✗ No	✗ No	✗
NIAPC (NATO Restricted)	✓ Yes	✗ No	✗ No	✗
Post-Quantum Roadmap (NIST FIPS 203-205)	✓ Yes	✗ No	Unconfirmed (UEM layer)	✗

These Certifications represent independently verified security architecture validated by the most rigorous government testing authorities across NATO allied nations. They are not self-attestations; they are third-party confirmations that BlackBerry UEM meets the security standards required for government and critical infrastructure operations.

Microsoft Ecosystem Integration: Enhancing, Not Replacing

For organizations deeply invested in Microsoft infrastructure, BlackBerry UEM provides a uniquely compelling proposition: sovereign-grade endpoint management that enhances rather than displaces existing Microsoft investments.

- **Microsoft Entra CA Integration:** BlackBerry UEM integrates natively with Microsoft Entra Certificate Authority (formerly Azure AD CA) for certificate-based authentication, extending Zero Trust principles across the endpoint management layer.
- **Microsoft Intune Partnership:** BlackBerry UEM is a certified Microsoft Intune Partner, enabling co-management scenarios where the BlackBerry UEM solution's sovereign security capabilities layer on top of Intune's Microsoft 365 integration.
- **BRIDGE for Secure Microsoft Office Document Editing:** BlackBerry UEM solution's BRIDGE technology enables secure editing of Microsoft Office documents within the BlackBerry encrypted container, preventing data leakage while maintaining full Microsoft Office productivity.

This positions BlackBerry UEM not as a Microsoft alternative but as the sovereign security layer that governments require on top of their Microsoft infrastructure.

Moving to BlackBerry – Why Now is the Right Time to Migrate

Uncertain times require reliability, particularly when facing modern threats to mobile users, anywhere and anytime. Coupled with the urgency of post-quantum readiness and sovereign data requirements, the need for BlackBerry UEM has never been clearer.

BlackBerry supports customers moving to BlackBerry UEM with:

- Competitive license pricing and migration incentives for current Ivanti, Omnissa, and Intune customers.
- Comprehensive policy migration tooling and migration-targeted professional services engagements.
- Coexistence and co-management with Intune, strengthening Intune while offering a path to full migration if required.
- On-premises, cloud, hybrid, and dark site deployment options meeting any sovereignty requirement.
- Full breadth of user deployment options, including BYOD and COPE.
- Sovereign deployment models and a certification portfolio that provide immediate risk mitigation.
- Post-quantum readiness and crypto-agility to stay ready.

Ready for a Better, Secure UEM Experience?

Do not compromise on security or productivity. Switch to BlackBerry UEM and experience a consistent, secure, and efficient endpoint management solution purpose-built for government, critical infrastructure, and enterprise organizations in today's hybrid work environment.

Contact our team to learn more about how BlackBerry UEM can transform your organization's endpoint management strategy.

References

1. NIST National Vulnerability Database (2026). CVE Search Results: Ivanti, Microsoft, Omnissa UEM Platforms. Retrieved from https://nvd.nist.gov/vuln/search
2. Cybersecurity and Infrastructure Security Agency (2024). Emergency Directive 24-01: Ivanti UEM Disconnection Mandate. CISA Known Exploited Vulnerabilities Catalog. Retrieved from https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. The Register (2024, February 15). Broadcom moves to reassure VMware customers amid uncertainty. Retrieved from https://www.theregister.com/2024/02/15/broadcom_moves_to_reassure_vmware/
4. NIAP Common Criteria Evaluation and Validation Scheme (2026). Product Compliant List. Retrieved from https://www.niap-ccevs.org/
5. NIST Cryptographic Module Validation Program (2026). FIPS 140-2/140-3 Validated Modules. Retrieved from https://csrc.nist.gov/projects/cryptographic-module-validation-program
6. Bundesamt für Sicherheit in der Informationstechnik [BSI Germany] (2026). Certified Products and Protection Profiles. Retrieved from https://www.bsi.bund.de/EN/Home/home_node.html
7. NATO Communications and Information Agency (2026). NATO NIAPC Evaluated Products. Retrieved from https://www.ia.nato.int/NIAPC
8. National Institute of Standards and Technology (2024). Post-Quantum Cryptography Standardization: FIPS 203, 204, 205. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

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.

For more information, visit BlackBerry.com and follow @BlackBerry.

BB26 | 260301