Evaluating Endpoint Management:

Why legacy solutions don't address modern concerns

Introduction

Today’s workforce is mobile, distributed and demands more flexibility than ever.

Whether your organization is remote, hybrid or fully back in the office, the use of mobile devices is inseparable from business operations. Smartphones, tablets and other mobile endpoints are integral tools across industries, streamlining workflows, enabling real-time data access and powering productivity from virtually anywhere.

As mobile adoption accelerates, the question isn’t whether these devices belong in the enterprise – it’s whether organizations are equipped to manage and secure them effectively beyond their original intent.

Evolving into essential business tools across sectors like healthcare, finance, construction and transportation, this evolution comes with complexity: IT faces rising pressure to manage a fragmented device landscape, enforce compliance across mixed ownership models and support productivity without compromising security or user privacy – all while aligning mobile technology and IT processes with business goals and outcomes.

This e-Book explores the critical shift in enterprise mobility management and security to explain why legacy tools or the “one-size-fits-all” approach no longer meets the needs of today’s modern enterprises. It highlights the importance of scalable, integrated solutions that support modern workflows, empower end-users and give IT the control and visibility they need to keep mobile fleets in lockstep with strategic priorities.

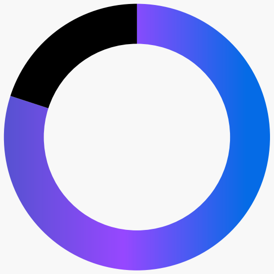
If your current tools weren’t built for mobile-first, hybrid work environments, this guide will help you assess whether they can still deliver value – or if it’s time to rethink your approach.

Work without borders

Regardless of whether your organization is fully remote or follows a return to office mandate -- regardless of where you physically are -- the ubiquity of mobile devices in our personal lives cannot be denied. It is so strong in fact that it crossed the threshold into professional use cases, becoming the go-to device of choice in many industries with its blend of capabilities, performance, portability and efficiency, blurring the line between personal and professional usage.

How critical is mobile to business continuity?

According to the **Verizon 2024 Mobile Security Index**,



“80% of respondents agree mobile devices are critical to the smooth running of their organizations.”

With mobile being such a critical tool for continuing business operations and the delivery of products and/or services from your industry to its customers, it is imperative for organizations to ensure that mobile endpoints are not just managed and secured, but closely aligned to business objectives to ensure that mobile remains compliant, fully supporting the evolving needs of the organization, its users and the safeguarded from an ever-changing threat landscape.

Evolution of roles and how tasks are performed

In recent years, many industries have looked to mobile devices to drive businesses and enable growth in novel ways, made possible only by mobile adoption. Examples of some of these industries, roles and ways in which they've benefited from increases in efficiency from implementing mobile devices are:

Aviation

Mobile devices streamline aircraft maintenance, flight operations and passenger service by **enabling real-time data access and communication** – from the flight gate to the cockpit. By switching from conventional flight bags to electronic flight bags, airline pilots reduce bulk from maps, flight manuals and handbooks weighing about 40 lbs. to a single iPad that stores it all with a 5 lbs. footprint, improving operational efficiency and compliance.

Construction

Tablets and smartphones improve collaboration, **reduces delays and strengthens project oversight** through digital documentation and access to project management tools on-site and off. iPads enable workers access to blueprints while enabling supervisors to process paperwork and sign documents on-the-fly – all while allowing teams to stay in constant communication with stakeholders and supply partners.

Financial services

Smartphones enhance client service, increase productivity and support compliance through multiple encrypted communications platforms. Financial professionals, such as analysts gain secure access to client data, simultaneously allowing them to monitor market activity at any time. Similarly, brokers are empowered to execute transactions from anywhere – securely and right from managed iPhones – allowing them to **tailor support that best suits client needs**.

Hospitality

Smartphones and tablets help hotels **elevate guest experiences while streamlining workflows across departments** using connected mobile systems to help staff deliver faster, more personalized services. iPads in kiosk mode provide guests with a self-check-in option that helps them begin to enjoy their stay sooner. Additionally, managed iPads in guest rooms facilitate simplified room management while dedicated apps provide detailed information and concierge support at a touch.

Retail

Mobile devices benefit retailers and guests with faster transactions, improved customer engagement and **more agile operations across physical and digital storefronts**. In switching from traditional Point of Sale (PoS) systems to mobile systems, sales associates may easily manage inventory while assisting customers on the floor without leaving their side. Furthermore, all the information they need is at a glance, including the ability to update customer data and process payments with mobile checkout options – all from their iPhone or iPad.

Enterprise challenges

The traditional approach of using a single management solution to oversee a uniform fleet of devices no longer reflects the reality of today's growing mobile-first enterprises. With employees leveraging a broad mix of mobile device types, varying ownership models and operating systems, IT faces increasing pressure to maintain business alignment, ensure compliance and boost productivity across highly fragmented environments. All this while the threat landscape evolves and endpoint diversity grows, organizations must evaluate whether their current management solution still meets (or can adapt to) the progressively complex demands while still delivering value to your business.

One size does not fit all

Historically, IT has led with the belief that managing one device type, running one OS, across the enterprise is feasible using one management solution. Whether tasked with managing 100, 1000, of tens of thousands of devices – there was a certain logic to this belief that helped IT keep homogenous endpoints managed and secured.

Stop to review the variety of device types that fall under the umbrella of mobile devices alone:

- Smartphones
- Tablets
- Laptops
- Wearables
- Internet of Things (IoT)
- E-readers
- Handheld Gaming Consoles
- Digital Cameras

Consider the multitude of these device types, taking into account the **average number of devices owned** per capita worldwide (3.6) and compare them to historical enterprises. You'll find it shares little in common with the modern computing landscape – and by extension, the modern threat landscape.

"85% of respondents say risks from mobile device threats have increased in the past year."

– Verizon 2024 Mobile Security Index

It begs the question: Does your management and security solution still align with business objectives, enforce compliance requirements and support productivity needs?

Maintaining compliance across varying ownership models

Before attempting to answer the question posted in the prior section, we would be remiss if we didn't consider the impact that varying ownership models has on mobile device usage in the enterprise.

Specifically, this section speaks to **maintaining security parity across the enterprise** when mobile devices used for work are a mix of company- and personally owned devices. Adding complexity is having to support:

- varying device types (Laptops, smartphones, tablets, wearables)
- manufactured by different vendors (Apple, Microsoft, Samsung, etc.)
- multiple operating system platforms (Apple, Android, ChromeOS and Windows)
- differing software versions (apps and OS)
- distributed workforces (return to office, remote work and hybrid environments)

Make no mistake, modern enterprises are a veritable melting pot of devices, ownership models and operating environments that impact needs and requirements in countless ways. This solely leaves IT to the challenge of ensuring that endpoints – regardless of ownership status – allow end-users access to business resources to remain productive. That employee productivity using mobile devices is protected comprehensively across the enterprise. And finally, that the crucial business tools (mobile devices) are used in a manner that align with business objectives and support business operations in a way that drives growth and scalability in lockstep with organizational needs.

"87% of critical infrastructure respondents believe a security breach involving mobile and IoT devices would have a substantial impact on their business."

– Verizon 2024 Mobile Security Index

Solving for X

Legacy tools were not developed to keep up with today's mobile-first, hybrid work environments. IT teams need integrated solutions that scale, secure and streamline management. Modern management solutions help organizations achieve desired business outcomes by simplifying zero-touch deployment, automate patching and enforce compliance baselines across platforms. Meanwhile, deep integration with identity providers enables Zero Trust architecture and secure access from any network connection. Behavioral threat detection and real-time endpoint monitoring improve incident response. Combining support for CIS benchmarks empowers IT to continuously audit and prove compliance while maintaining productivity and performance across all device types, ownership models and work environments.

Align technical processes to business objectives

IT, like any other facet of business, is critical to organizational success. To achieve its mission, IT processes must exceed traditional device management strategies tested by supporting mobile devices, distributed work environments and evolving security threats.

To remain competitive, it is essential that IT align with core business objectives, directly contributing to:

1. strategic growth
2. operational efficiency
3. long-term resilience

in addition to empowering the business by enhancing agility, supporting productivity and mitigating risk without sacrificing user experience.

Aligning a management solution that supports mobile diversity alongside your business strategy enables measurable outcomes across key industries, with evolving use cases, such as:

Manufacturing

iPads enable production workers to access real-time supply chain data and digitize workflows. An IDC survey discovered that 85% of organizations that **invested in digital transformation (DX) technologies** found a correlation between "an improved employee experience and higher employee engagement translate to a better customer experience, higher customer satisfaction, and higher revenues for their organization."

Healthcare

iPads and iPhones empower care providers with instant, secure access to electronic personal health information (PHI) and telemedicine tools. According to the National Institutes of Health (NIH), of the ten studies researched for the article titled, **Smartphone and Mobile App Use Among Physicians in Clinical Practice**, *"70% reported the use of mobile apps"* to improve patient outcomes and streamline care delivery based on access to evidence-based medicine to support clinical decision-making.

Government

iPhones enable secure remote access to agency resources while supporting field data collection. With just a hair over 90% of mobile devices reported lost or stolen resulting in a "confirmed data disclosure", according to **Verizon 2024 Data Breach Investigations Report**, scalable, comprehensive security adapts to growing fleets and evolving policies while maintaining consistent, holistic protection.

Optimize mobile device fleet support

Modern mobile device strategies are necessary for IT teams to scale support, enforce compliance and maintain user privacy across personal and company-owned devices. Cross-platform security ensures security parity is achieved and compliance remains enforced, while streamlined reconfiguration of shared devices reduce risk and promote uptime – allowing deskless workers to be more productive. This approach improves operational efficiency and ensures consistent protections, enabling IT leaders to align mobile fleet management with evolving business and workforce needs.

Scalable support for ownership models

Modern enterprises face scalability challenges when supporting a hybrid fleet of personally and company-owned devices. Purpose-built solutions, like **support for varying enrollment models**, are essential for IT teams to:

- reduce complexity
- extend security holistically
- segment business and personal data
- enforce compliance
- balance user privacy

A key function for maintaining security while upholding privacy is to **protect business data while encrypting network connections** to/from company resources while routing non-business traffic directly to the internet on personal devices. This approach ensures a consistent device security posture and policy enforcement at scale, across varied ownership models.

Cross-platform endpoint security parity

In addition to the challenge IT faces with varying ownership models, modern enterprises frequently operate in heterogeneous, or mixed environments made up of differing operating systems, like iOS/iPadOS, Windows and Android are all in use by stakeholders. Multiplying the complexity by the number of devices easily ratchets up the difficulty of minimizing risk due to all the variables introduced.

With a blend of defense in depth strategies and the right controls, like:

- advanced telemetry
- behavioral threat detection
- unified access policies

and cross-platform support means mobile endpoints are secured consistently – on-device and in-network – **regardless of their platform**. This cross-platform support allows IT teams to reduce fragmentation while **maintaining strong security standards across the mobile fleet**.

Shared Devices and Deskless Workers

Reducing downtime between user sessions is essential in industries where shared devices and multi-user environments are common. Whether it's:

- quickly setting up an iPhone to support customers during a busy shopping season
- deploying iPhones to flight crews to streamline food and beverage purchases aboard aircrafts
- reconfiguring an iPad on the fly from kiosk mode to best support nursing care

When seconds matter most, simplifying device reconfiguration by **empowering users to quickly switch roles** or **wipe and supervise devices without IT intervention** can be a life-saving task. Purpose-built solutions ensure that shared devices remain secure and ready for the next user, while reducing support requests and improving overall operational efficiency.

Unlock new workflows to drive productivity

Streamlining mobile device management boosts IT efficiency and user productivity across the enterprise. Seamless integration with identity and security tools supports faster provisioning, compliance reporting and access control. Automating deployment reduces setup time and manual errors, while self-service capabilities empower users to access essential apps and resources on demand. Ultimately, unlocked workflows capitalize on efficiency to simultaneously minimize downtime while permitting IT teams to focus their skills on developing processes drive value toward business objectives.

Seamless integration with existing tools

"Silver bullet" solutions don't exist.

That's why **integration is a key part to successfully managing and securing mobile devices** because it:

- extends services holistically
- adds comprehensive security layers
- allows businesses to build upon existing tools
- customizes workflows to meet compliance needs

For example, **integrating with identity providers** like Microsoft Entra ID and Okta centralizes access control, enforces conditional access policies and adds phishing-resistant MFA to authentication workflows. Mitigating risk of unauthorized access to protected resources is just one of countless examples where integration with security platforms allows IT to:

- streamline device onboarding
- enable faster provisioning
- simplify compliance reporting
- reduce friction across the technology stack
- align with business workflows

Automate device deployment and provisioning

Depending on organizational needs, manually onboarding mobile devices can take upwards of 30 minutes per device, resulting in delayed productivity and increased IT overhead.

But **automating mobile device deployment with Zero-Touch** and Apple Business Manager (ABM) shave provisioning times down significantly by streamlining deployment, effectively reducing downtime. This approach **boosts efficiency for IT** while providing organizations the following benefits:

- eliminates manual setup and reduces the risk of introducing human error
- accelerates onboarding, including app installations and configurations
- ensures every device meets security and compliance standards – from day one
- users have the resources they need and are ready to work upon activation

Provide users access to resources they need – when they need it

A **good response time** for an IT request typically falls within the range of 24 hours, or one business day. However, when a stakeholder requests an app or configuration that's necessary before they can complete a task, every minute delay equates to loss of productivity, potentially impacting the organization's operations and ultimately, its bottom line.

Self Service empowers stakeholders by granting them access to:

- a curated catalog of approved apps
- business resources and services
- secure configurations and settings

– all without submitting support tickets!

Users can securely access the resources they need to remain productive while IT retains control over what's available, reducing help desk volume while empowering stakeholders to act with confidence.

Implement a comprehensive security strategy

Enterprises must evolve and scale their security practices to efficiently meet modern threats across diverse mobile environments. Automating patch management minimizes vulnerabilities by ensuring devices and apps remain up to date while reducing IT overhead. Advanced threat detection requires real-time analytics, deep integration and layered defenses to identify and mitigate risks. A Zero Trust strategy, built on device health and user identity, ensures secure access to resources regardless of location, platform or ownership model.

Automate patch management

Human error is the single most preventable threat to an enterprise's cybersecurity plan. Outdated software, which falls under this purview, leaves mobile devices vulnerable and undermines organizational compliance aims. The good news is that by **automating patch management for both operating systems and apps**, this type of threat can be mitigated in the following ways:

- real-time monitoring and alerts
- proactive review of unified logs
- leveraging **Smart Groups**
- enforcing dynamic policies
- **App Installers** workflows
- minimum app version pinning

By leveraging automation, IT reduces manual effort while ensuring devices remain consistently updated and meet internal and regulatory requirements, all while minimizing user disruption and downtime.

Threat detection and prevention

Cyberattacks peaked in 2020, then declined – until **mobile attacks surged 147%** from Q1 to Q4 in 2023, according to Kaspersky. Mobile threats have grown more sophisticated, often bypassing the capabilities of traditional malware tools. Effective mobile security must prevent known threats and use on-device and in-network behavioral analytics to detect advanced risks in real time. Deep integration across management, identity and security provides IT teams with:

- deeper visibility into mobile device activity
- real-time assessment of risk postures
- faster incident response times across multiple platforms, ownership types and work environments
- seamless integration with third-party SIEMs
- comprehensive, layered controls without compromising device performance

Zero Trust Network Access (ZTNA)

Work environments and device usage have evolved, so should enterprises still rely on legacy tools designed for a different era to manage and secure today's mobile fleet?

Simply put: no.

Shifts to cloud computing, hybrid work environments and mobile devices make controlling access based on user identity and device health imperative to maintaining compliance. Today's perimeter-less enterprises achieve this by:

- **replacing legacy VPNs with encrypted microtunnels** to isolate network traffic
- implementing conditional access policies that only grant access to sanctioned users and verified devices
- seamless integrating identity alongside their management and security stack
- developing a **Zero Trust strategy** that holistically secures corporate resources – no matter where employees work, on which device or who owns it

Standardize and enforce compliance holistically

Effective compliance starts by implementing security baselines built on industry standards, ensuring all mobile devices meet enforceable policies from day one. Active monitoring of endpoint health delivers real-time visibility and AI-driven risk detection, helping IT maintain compliance and respond to threats swiftly. Finally, verifying compliance through benchmarks like CIS allows organizations to audit, remediate and report on adherence.

Strengthen security postures by implementing baselines

Technical controls and policies are essential for compliance and enforcement, but where does one start on the path to compliance and the requirements of a specific industry? It begins with baselines, built upon industry-accepted standards and frameworks.

Establishing configuration baselines ensures that each endpoint – whether corporate- or personally owned – adheres to **enforceable security requirements upon enrolling mobile devices within MDM**. It's a foundational step and critical to developing and implementing a defense-in-depth security strategy. One that helps IT:

- **establish compliance through structured configuration profile** deployment to targeted Smart Groups
- automate consistent provisioning, reducing configuration drift at scale
- align mobile device processes with data security to support business continuity
- **customize security strategies to meet unique organizational needs and industry regulations**

Actively monitor endpoint health

The next key step after implementing baselines is actively monitoring mobile device fleets where continuous visibility into health statuses is essential for sustained compliance, including fast incident response when non-compliant endpoints are detected. Thanks to the tight integration between management, identity and security, the silos between IT teams are broken down, **leveraging AI to improve organizational security postures** in addition to enabling:

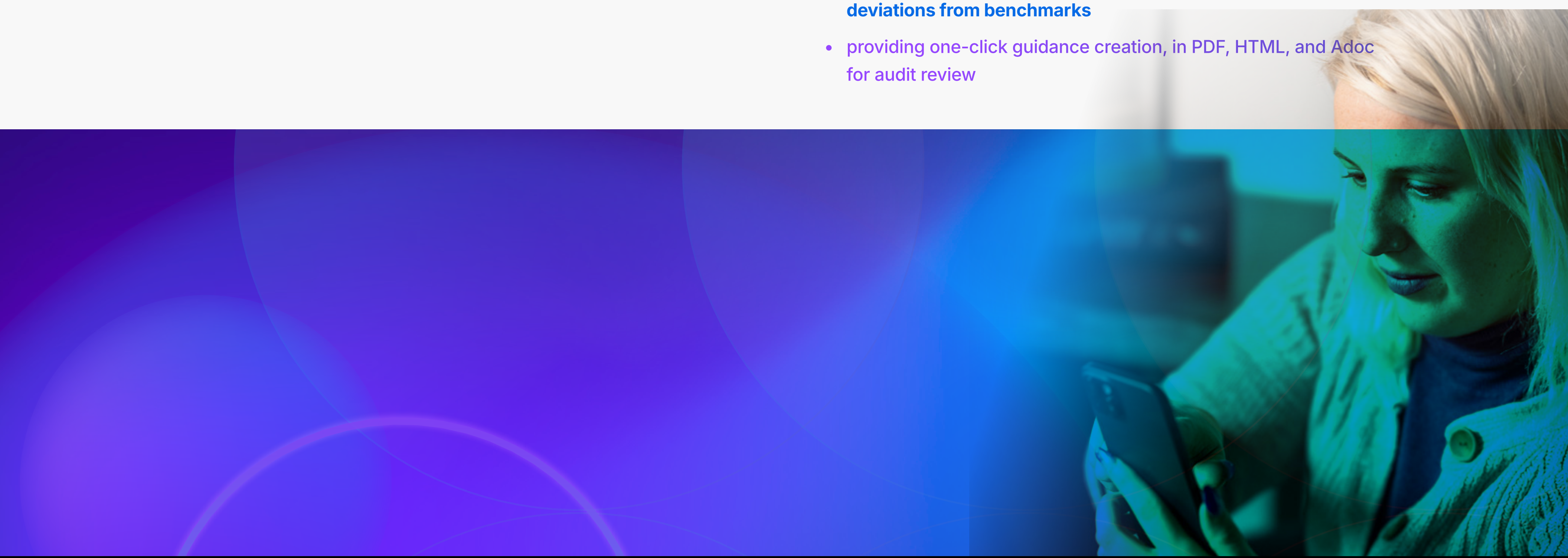
- use of **real-time telemetry and insights into endpoint behavior**
- machine learning (ML)-powered risk detection and even faster remediation
- **proactive mobile endpoint threat hunting**, analysis and response of sophisticated threats

Verify and enforce compliance with benchmarks

The third key step closes the loop on the mobile device compliance lifecycle by bridging the gap between enforcement, review and improvement, by provides a means for organizations to continuously audit compliance. Moreover, it facilitates **showing proof of compliance as mandated in regulated industries**.

Modern management solutions empower organizations by not only standardizing and monitoring compliance, but provide the native tooling necessary to verify compliance against industry-accepted benchmarks, like CIS Level 1 and 2 – supporting internal governance and regulatory readiness by:

- **allowing IT the flexibility to customize benchmarks** to meet unique company needs
- automating baseline measurement to **automatically remediate deviations from benchmarks**
- providing one-click guidance creation, in PDF, HTML, and Adoc for audit review



Convenience vs Security: By the numbers

Opting for convenient or low-cost tooling often sacrifices security, leading to greater long-term risk and operational disruption. Inconsistent protections across device types weaken the overall security posture and create gaps attackers can exploit. Cyber incidents not only impact security but also degrade device performance, hinder productivity and disrupt business continuity. To avoid these pitfalls, IT leaders must prioritize solutions that secure all endpoints – regardless of ownership or operating system – ensuring efficacy, resilience, efficiency and sustained organizational health.

Why saving money on "easy" ends up costing orgs more than "safe"

Cost is a driving factor for organizations choosing solutions to manage and secure mobile device fleets. While keeping existing legacy solutions or opting for a "one-size-fits-all" type may reduce initial setup times and/or front-end costs, the compromise often being comprehensive mobile security in exchange for the convenience and price points these tools offer.

Unfortunately, gaps in security can lead to costly breaches. With **the global average cost of a data breach at $4.44 million** – and the US average at $10.22 million – according to IBM's Cost of a Data Breach 2025 Report.

Conversely, a cost analysis conducted from IBM's report found a cost savings of $1.9 million from "security teams using AI and automation" – to extensively shorten breach times by 80 days while also lowering the average breach cost – compared to organizations that chose solutions with basic support for management, identity or security.

TL;DR Businesses investing in cybersecurity is intrinsically tied to business operations, public reputation and regulatory compliance – all of which contribute to the organization's bottom line in different ways.

Lack of parity weakens the organizational security posture

When mobile device security is platformdependent instead of platform-agnostic support of the security capability itself, organizations are left with security disparity.

Simply stated: some mobile devices lack the protections others have.

A recent article in **Infosecurity Magazine** discussed how 41% of respondents cited stolen devices containing sensitive data as the leading cause of data loss – surpassing weak and stolen credentials (36%) and ransomware attacks (32%). This scenario stems from inconsistent controls across supported platforms, leading to a false sense of protection against exploitable security gaps that undermine overall resilience.

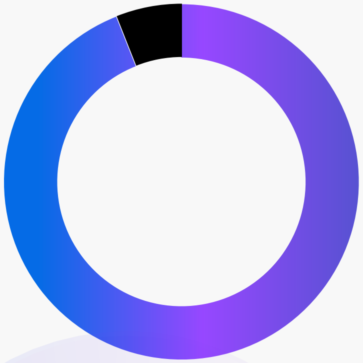
TL;DR Enterprise security must apply to all endpoints that accessing the organizational infrastructure by virtue of each device representing (and potentially introducing) risk to the enterprise – regardless of the device type, OS platform or who owns it. Risk is risk.

Impact on device performance and employee productivity

Cyber incidents don't just have financial implications (as discussed earlier). They impact device and organizational security postures sure, but they also degrade performance and affect user productivity – all of which have a recursive effect on business operations.

Encompassing breaches across multiple types of environments (mix of public and private clouds, and on-premises), IBM found that the Mean Time to Identify (MTTI) a data breach measured 207 days. The Mean Time to Contain (MTTC) required an extra 70 days, bringing the average total time to identify and contain a data breach across various environments to 276 days, bridging financial and opportunity costs from impacted performance of affected devices and enterprise systems.

While the prior segment both directly and indirectly impacts employees, fallout from certain threats and attacks can have greater direct impacts on user productivity. Take for example a ransomware attack. In an article about the results of prolonged network and business downtime, **Help Net Security** noted that



"94% of those who suffered a ransom event experienced a period of significant downtime and delays in productivity. This included 40% of victims who stated they experienced a period of total work stoppage and complete loss of productivity."

TL;DR: Cyberattacks have effects that extend beyond immediate costs, including lost business opportunities, reduced productivity, eroded public trust and declining market value – consequences that often reverberate well after a breach is contained.

Key Takeaways

1.

Mobile is mission-critical:

Mobile devices are essential tools across industries, enabling real-time communication, flexible workflows and business continuity in remote, hybrid and on-site environments.

2.

Legacy tools fall short:

Traditional and one-size-fits-all management solutions cannot maintain security parity amidst the complexity of modern mobile fleets, varying ownership models and cross-platform OS's.

3.

Security must be comprehensive:

Modern enterprises require cross-platform, identity-integrated security strategies that include real-time threat detection, conditional access policies and automated patch management.

4.

Compliance is nonnegotiable:

Effective mobile management supports audit-ready compliance by deploying secure baselines, monitoring endpoint health and verifying adherence with industry benchmarks.

5.

Scalability and automation are key:

Purpose-built solutions streamline deployment, simplify provisioning and reduce manual overhead, enabling IT to scale support holistically across distributed teams.

6.

User experiences matter:

Empowering employees with self-service tools and consistent access to business resources enhances productivity without sacrificing privacy or security while reducing IT workloads.

7.

Business alignment drives value:

Aligning mobile device management with strategic objectives improves operational efficiency, supports growth and positions IT as a driver of innovation.

Conclusion

The growing reliance on mobile devices to drive productivity enables work -- at the desk or away from it. Delivering business outcomes is no longer a trend – it is a defining characteristic of the modern enterprise.

Expanding complexity from device types, ownership models and support for multiple operating systems have left legacy management tools unable to meet some of the most fundamental security, compliance and user experience requirements of modern enterprises.

IT is no longer being asked to simply manage devices.

They are being called upon to align technology and management processes with business strategy in support of business objectives. To protect critical assets while supporting a workforce that expects seamless access from anywhere, on the device of their choice and running the operating system, they feel most productive with.

1. **The stakes are higher.**

2. **The risks are greater.**

3. **And the margin for error is shrinking.**

Modern endpoint management solutions are designed to meet these evolving demands. From zero-touch deployment and advanced threat detection to cross-platform support and Zero Trust security. Purpose-built tools enable IT teams to scale, secure and optimize business operations running on mobile without compromising security, efficiency or productivity.

The question remains:

Does your current management solution still meet the evolving needs of your enterprise, IT and employees? If the answer is uncertain, now is the time to reevaluate your approach...the success of your business depends on it.

Try Jamf