Hypori
One Device, Zero Worries™

The Virtual Mobile Infrastructure Report:

Trends in Secure Mobile Access & BYOD

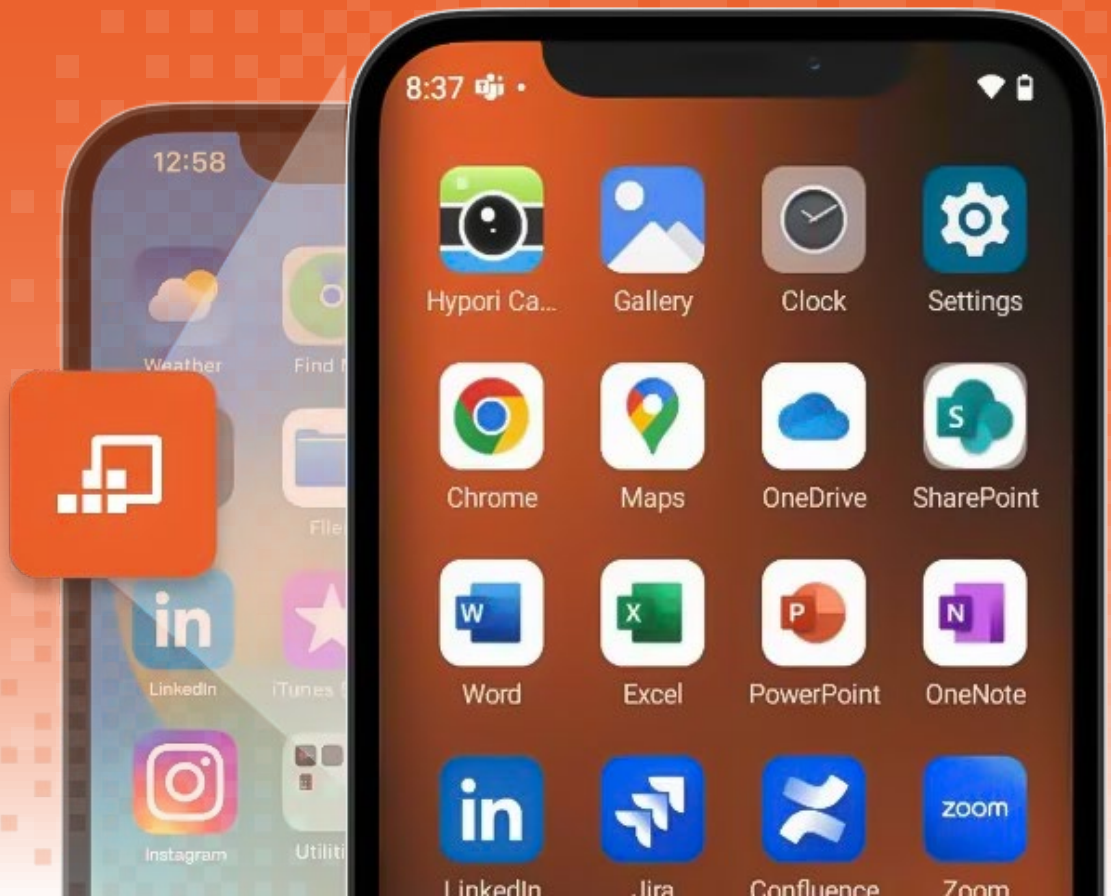


Table of Contents

Executive Summary

The mobile enterprise is at a pivotal crossroads. As organizations increasingly embrace hybrid working, cloud services, and BYOD models, combined with the need to meet mounting security regulations and mitigate risks, all within strict budgetary controls, the traditional tools of mobile security—rooted in endpoint device control—are no longer fit for purpose.

What was once acceptable under Mobile Device Management (MDM) and Mobile Application Management (MAM) is now a source of friction: for users, a source of privacy concern; for businesses, a barrier to productivity and agility.

At the same time, the issue of employee privacy is moving rapidly up the agenda. Enterprises consistently acknowledge that privacy violations are among their most significant risks, yet many deprioritize the issue when it comes to actual security strategies. This disconnect highlights a growing tension: businesses recognize the reputational and compliance stakes around mishandling personal data, but continue to rely on tools that blur the line between corporate oversight and personal device intrusion. For employees, this erodes trust and fuels resistance.

For organizations, it undermines adoption and leaves a blind spot in their overall risk posture.

Virtual Mobile Infrastructure (VMI) offers a way forward—removing the device from the risk equation entirely and delivering secure, seamless access to enterprise environments from any device, anywhere. It aligns with Zero Trust principles, reduces operational overhead, and respects user privacy—solving the dual challenge of securing corporate data while empowering users.

The future of secure mobility lies not in controlling the endpoint but in enabling the remote workforce. The organizations that act now—replacing rigid legacy systems with adaptable, cloud-native infrastructure—will lead in resilience, innovation, and employee trust.

The time to reimagine enterprise mobility is not coming. It's here.

01.
Introduction: The New Reality of Mobile Security

In recent years, the BYOD (Bring Your Own Device) market has increased exponentially. In 2024, the global market for BYOD and Enterprise Mobility was estimated at US$129.2 billion and is projected to reach US$331.6 billion by 2030, growing at a CAGR of 17.0% from 2024 to 2030, according to Research and Markets' Global Strategic Business Report[1].

With BYOD adoption rising and mobile devices becoming a primary work interface, the risk landscape has shifted.

52%

increase in cyberattacks on mobile devices in 2023, totaling 34 million incidents globally[2].

Moreover, approximately 48 % of organizations have suffered data breaches linked to unsecured or unmanaged personal devices in the past year.

Not only do BYOD policies create a larger attack surface and increase the risk of data exposure, adding a layer of complexity to the management of corporate cybersecurity, there are increasing concerns around user privacy and work enablement / productivity that stem from legacy mobile security models.

In June 2025, Hypori commissioned independent research, conducted by Sapio Research, to ascertain the state of the secure mobile landscape.

We surveyed 1,000 security, risk, mobility, and BYOD decision makers, in organizations with more than 1,000 employees across a range of industries globally, seeking to understand how confident business leaders are in their current mobile security posture.

Where do leaders see their greatest vulnerabilities? How are today's corporate security controls and BYOD policies impacting user satisfaction, productivity and privacy concerns? And what does the future of secure mobility look like?

This "VMI Report: Trends in Secure Mobile Access & BYOD" presents VMI as a transformative solution. One that enables organizations to rethink their BYOD policies: addressing security concerns, increasing compliance and removing an entire attack vector; mitigating the cost and operational overhead of legacy mobile security models — all while respecting user privacy.

1. https://www.researchandmarkets.com/reports/4804695/byod-and-enterprise-mobility-global-strategic
2. https://cds.thalesgroup.com/en/hot-topics/mobile-security-what-are-threats-targeting-business-devices

02.
Understanding VMI: A Better Alternative to MDM and MAM

What is VMI?

Virtual Mobile Infrastructure (VMI) delivers a virtualized mobile environment from the cloud, where corporate applications and data reside entirely off the end-user's device. Unlike Mobile Device Management (MDM) or Mobile Application Management (MAM), VMI offers secure access via a thin-client app without requiring deep access to, or control over, the user's device.

Virtual Mobile Infrastructure (VMI) refers to the digital and network systems that enable seamless, secure, and efficient mobility services without the need to rely solely on physical infrastructure. It can be thought of as a virtual device running in the cloud that can be accessed by a thin client app on mobile endpoints.

Comparison: VMI vs. MDM vs. MAM

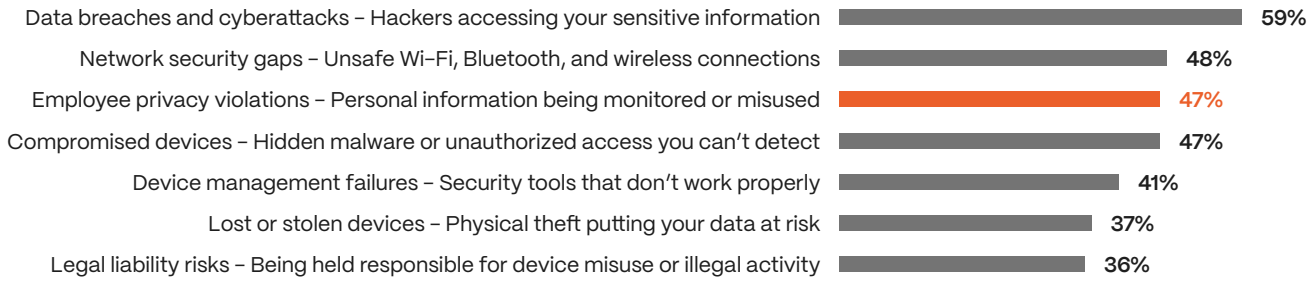
Feature	VMI	MDM	MAM
Data Storage	Off-device on secure servers	On actual device	App-wrapped data on device
Privacy	No corporate access to personal data, applications or browsing	Corporate access to personal data, apps and device settings	Privacy concerns for device monitoring
Security	Pixel-streamed, zero data-at-rest, ideal for Zero Trust	Depends on endpoint—if rooted or infected, compromised	Still vulnerable due to OS-level leaks, configuration drift
Platform Support	Device-agnostic (iOS, Android, etc.) with single hosted Android instance	Often OS-specific; requires enrolment per device	App-level control but still relies on device OS
Compliance & Management	Centralized updates, audit logs, ideal for regulated workloads (CMMC, HIPAA, FedRAMP)	Device-level policies, remote wipe	App-centric policies; complex to maintain

03.
The Mobile Threat Landscape and Market Growth

Risk Perception

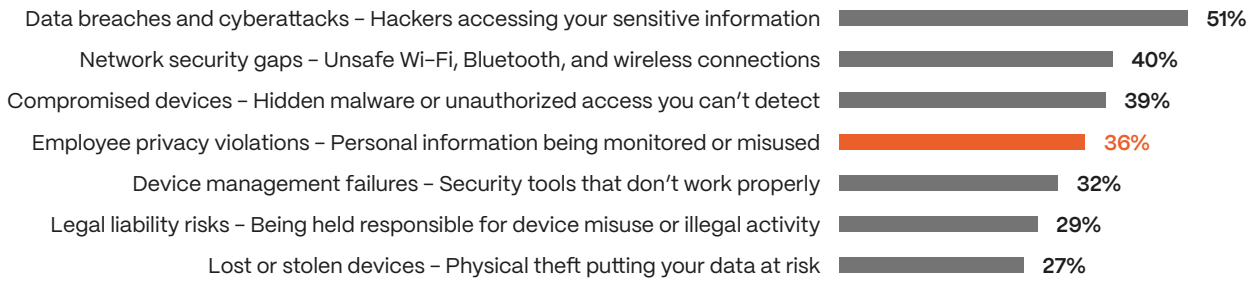
The current mobile threat landscape is defined by escalating risks, with **47% of surveyed organizations citing employee privacy violations as one of their top concerns, alongside data breaches and cyberattacks (59%), network security gaps (48%) and compromised devices (47%). However, only 36% are actively prioritizing privacy violations in their mitigation strategies.**

BIGGEST MOBILE SECURITY RISKS



In your opinion, what are the biggest mobile risks facing your organization currently? Select all that apply

RISKS BEING PRIORITIZIED FOR MITIGATION



And of these risks, which are you currently prioritising in terms of risk mitigation in your organization? Select top three

This divergence is reinforced by the growing operational conflicts organizations face in managing concerns around compliance, privacy and data protection (48%) and balancing security with the user experience (46%) – particularly in BYOD contexts, where MDM solutions often conflict with end-user trust and productivity. Indeed, 69% of organizations report that current security controls negatively impact user satisfaction or productivity.

This conflict between recognition and action highlights a fundamental weakness in current secure mobility strategies. Organizations are clearly aware of the risks to employee privacy, yet continue to deprioritize them in favor of more traditional threat categories. The result is a widening trust gap: employees increasingly view enterprise security controls as invasive, while businesses inadvertently undermine adoption and compliance. Unless privacy is elevated to the same level of importance as data protection and network defense, enterprises risk both alienating their workforce and exposing themselves to avoidable reputational and regulatory consequences.

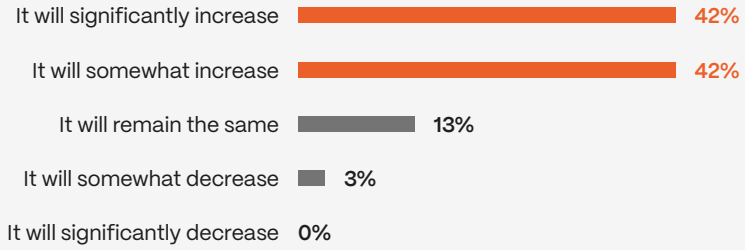
Maturity and Security Confidence

According to the survey data, only 39% of organizations consider their mobile security posture to be "very mature," signaling a market with significant room for growth. Notably, maturity levels vary by geography and sector—North America (49%) and the defense industry (54%) lead, while Europe (25%) and government organizations (19%) lag behind.

Confidence in mobile security is on an upward trend. A robust 75% of organizations report increased confidence in mobile security solutions over the past three years, with the defense (88%) and technology (90%) sectors leading this sentiment.

Investment Plans

Investment data reinforces this optimism.



85%

of respondents anticipate increased investment in secure mobility over the next year, with 42% predicting a significant increase.

How do you think investment in secure mobility will change over the next year? Select one

The defense sector, again, stands out with a projected 90% of organizations predicting greater secure mobility spending. BYOD programs are also set for expansion, with 63% of organizations planning to increase investment—averaging a 4.9% budget growth globally and peaking at 7.6% in the defense sector.

Conclusion

The mobile threat landscape is intensifying, yet so is organizational readiness to invest, particularly given ongoing concerns with current mobile security postures. VMI stands at the intersection of these trends—offering a secure, cost-effective alternative to legacy mobile security models, particularly as BYOD and remote work become institutional norms.

04.
VMI vs. MDM / MAM: Security Limitations and Gaps

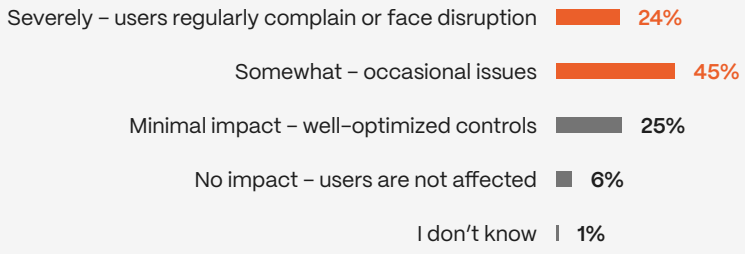
MDM and MAM solutions have to date served as the default for enterprise mobile security as part of a broader ecosystem that controls the device or application.

However, as this research highlights, these traditional approaches are revealing critical shortcomings – not least because, as part of a highly complex infrastructure, MDM and MAM are rife with potential configuration issues, privacy violations and increased attack surface.

Unsurprisingly, a significant 77% of organizations currently using MDM therefore report major limitations with their existing solutions. The most cited issues include persistent security gaps (43%) and limited control over BYOD environments (39%).

These are particularly concerning given the widespread and increasing adoption of BYOD policies—63% of organizations expect to increase BYOD investment over the next year, with average budget increases of nearly 5%.

MDM's core limitation lies in its reliance on controlling and managing the physical device. This approach creates friction with employees, especially when personal devices are involved. Indeed, respondents also cite lack of user privacy and poor user experience as limitations with MDM.



69%

of organizations report that their current security controls (MDM and MAM included) negatively impact end-user satisfaction and productivity.

To what extent have security controls impacted end-user productivity or satisfaction in your organization? Select one

VMI offers a fundamentally different model: rather than managing the device, it virtualizes the workspace entirely. Sensitive data never resides on the endpoint. Instead, the user interacts with a virtual instance hosted in the cloud.

This eliminates the risk of data leakage through device compromise or loss and bypasses the need to access or monitor the user's personal device. It directly addresses the privacy concern that 47% of organizations identify as a major security risk—yet which only 36% actively prioritize in their mitigation strategies.

Zero Trust & VMI

Critically, VMI also aligns closely with Zero Trust principles.

86%

of respondents believe VMI supports Zero Trust architecture.

Only 37% of organizations consider themselves experts in Zero Trust, and 92% still face challenges in implementation. MDM and MAM often struggle in this area due to their dependence on legacy security models that trust the endpoint. VMI, by not trusting or relying on the endpoint at all, inherently supports a Zero Trust stance.

From an operational perspective, VMI also offers faster deployment and less overhead. Organizations cite cost (35%) and complexity (30%) as barriers to traditional MDM solutions—but VMI's cloud-native approach means there's no need to manage physical devices or push updates across a fragmented mobile fleet.

Conclusion

While MDM and MAM still have market share, they are failing to address key enterprise needs—particularly around BYOD privacy, user experience, and data containment. VMI not only addresses these, but positions organizations for future-readiness with its alignment to Zero Trust, cloud-based delivery, and superior security architecture. As mobile threats grow and user expectations evolve, the shift from device control to data-centric access will be central.

05.
Privacy and User Experience

As mobile usage becomes increasingly central to enterprise operations, organizations are facing a difficult balancing act: securing sensitive corporate data while maintaining employee privacy and productivity.

Data from this 2025 research paints a clear picture—current mobile security strategies are falling short on both fronts. The emerging consensus is that legacy tools are creating friction, undermining both user experience and return on investment.

The Cost of Security: Privacy and Productivity Under Pressure

One of the most significant data points from this study is that 69% of organizations report that their current mobile security controls have negatively impacted end-user productivity or satisfaction, with 24% stating that the impact has been severe. This effect is consistent across regions:

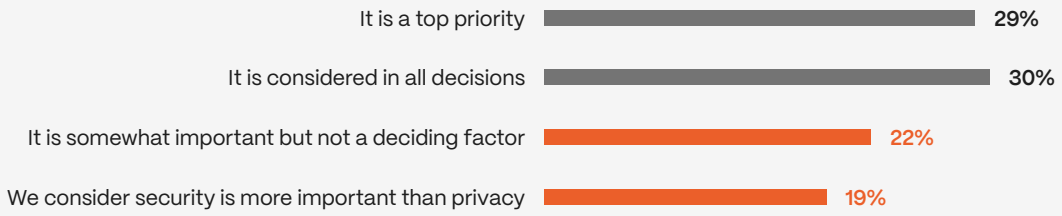
73% in APAC

72% in North America

67% in LATAM

62% in Europe

These figures underscore a systemic issue: current secure mobility solutions are too invasive or too restrictive to enable seamless, productive work—especially in BYOD contexts. **Despite this, only 29% of organizations say employee privacy is the top priority in their mobile security strategy.**



41% admit it is not a deciding factor at all.

How important is employee privacy when it comes to your mobile security strategy? Select one

Paradoxically, 47% of respondents identify employee privacy violations as one of the biggest risks in mobile security—yet this ranks fourth in terms of risk mitigation priority (36%). This disconnect between perceived risk and action taken suggests that organizations are aware of the issue but struggle to resolve it within current frameworks.

BYOD and the Illusion of Control

BYOD has been heralded as a flexible solution for today's working practices, but its implementation through MDM/MAM comes at a cost.

39%

of organizations cite limited control over BYOD as a main limitation of their current MDM setup.

43%

point to persistent security gaps in MDM/MAM solutions, showing that even with strict control, vulnerabilities remain.

77%

of organizations with an MDM solution acknowledge major limitations.

Moreover, employee resistance is a growing challenge, with change management cited by over a quarter of organizations as a barrier to secure and efficient mobile access and MDM / MAM anecdotally described as "some stuff my company makes me put on my phone." This sentiment highlights a fundamental adoption problem—users are unhappy compromising personal privacy for work-related access.

The Opportunity: A Shift Toward Privacy-First Secure Mobility

This is an opportunity for change. Enterprises want to secure data and reduce risk, but not at the cost of reduced productivity or workforce disenfranchisement. User experience, particularly privacy and ease of use, is directly linked to adoption, and by extension, the effectiveness of an organization's security strategy. As user expectations grow and data risks increase, organizations must pivot toward solutions – such as VMI – that align with both operational goals and employee experience.

Traditional Mobile Security Solutions Trade-Offs

75%
Confidence increase in new mobile security solutions

63%
BYOD budget increase expectation

47%
Privacy violations as a current risk

This visual shows the tension between perceived risk, investment growth, and the real-world limitations of current strategies—setting the stage for a conversation about the need for modern, user-centric solutions like VMI.

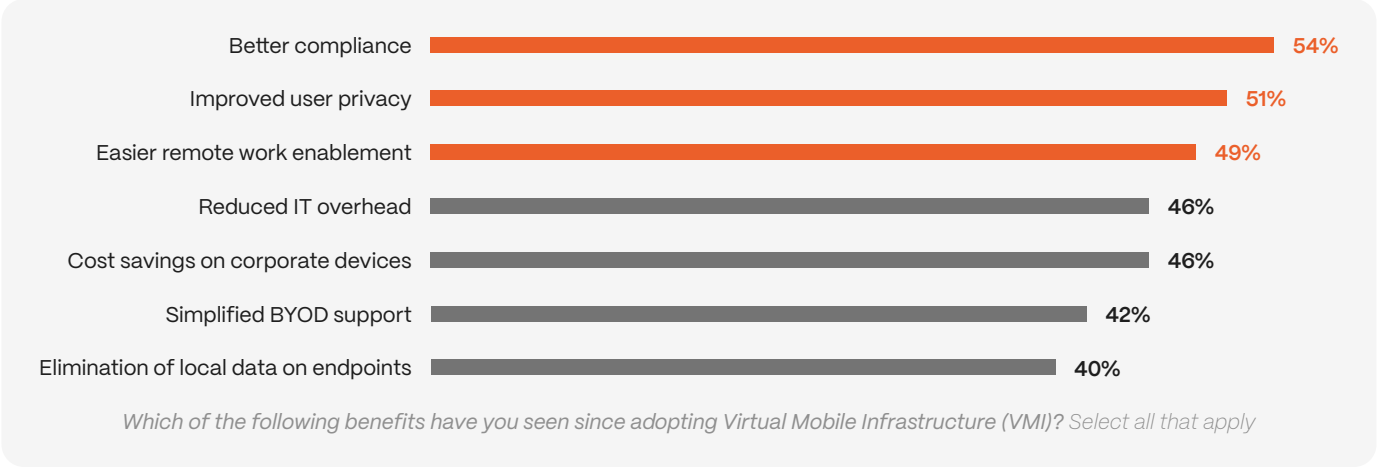
06.
VMI Sentiment: Confidence and Misconceptions

The overall sentiment towards VMI is overwhelmingly positive among enterprise decision-makers: over 73% of organizations agreed with the advantages of VMI, including its ability to support flexible working, enhance user privacy, and protect sensitive data.

As organizations seek more scalable and privacy-conscious mobile solutions, VMI is emerging as a frontrunner. Indeed, 51% of respondents believe VMI will have the greatest impact on secure mobility over the next three years, placing it above AI-driven endpoint security and Zero Trust architectures.

Adoption Benefits

Among organizations that have already adopted VMI, the benefits are clear. **The top three cited outcomes are: Improved compliance – 54%, Enhanced user privacy – 51%, and Enablement of remote and hybrid work – 49%.** Indeed, 78% of respondents agree that VMI offers a more secure and practical solution for users with more than one phone.



Which of the following benefits have you seen since adopting Virtual Mobile Infrastructure (VMI)? Select all that apply

These benefits are not just theoretical—they directly address the most pressing challenges organizations today cite, including managing mobile cyber threats, protecting sensitive corporate data, and supporting modern working practices – while also delivering significant cost savings by reducing – or removing – the number of enterprise-issued devices. Importantly, these benefits also align with the top drivers pushing businesses toward adoption, suggesting a strong value realization post-implementation.

Adoption Barriers: Perception vs. Reality

While enthusiasm for VMI is high, certain barriers are delaying adoption. The most commonly cited challenges are:

41%
Integration complexity

40%
Privacy concerns

30%
Lack of internal expertise/resources (especially in LATAM at 48%)

Integration complexity tops the list, but this appears to be more a matter of perception than fact. VMI is simple and fast to deploy, often requiring little to no IT intervention, with its touchless setup requiring users only to download an app and enroll.

Additionally, while privacy concerns are mentioned as a barrier, this too likely stems from confusion between VMI and legacy tools like MDM. In reality, VMI stores no data on the device, ensuring complete separation between personal and corporate use—thus offering one of the most privacy-preserving architectures available.

Importantly, return on investment (ROI) is not a significant obstacle. Unlike many security technologies that struggle to demonstrate business value, VMI has a clear cost advantage, especially when compared to issuing secondary devices or deploying complex MDM systems.

Similarly, end-user resistance is notably low. This is a major differentiator from MDM/MAM solutions, which employees often resist due to invasiveness. With VMI, adoption is higher because users are not being monitored or constrained, and organizations are more likely to see full utilization of purchased licenses—critical for long-term ROI.

Conclusion

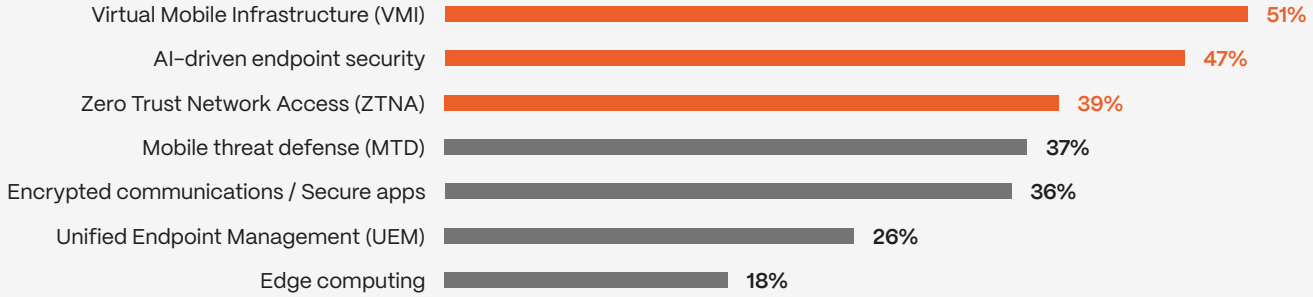
While perceived complexity remains a top barrier to VMI adoption, the reality is that implementation is simple, non-invasive, and well-aligned with modern mobility trends.

The benefits are significant, resistance is minimal, and ROI is evident. Organizations that overcome early misconceptions stand to gain a secure, scalable, and user-friendly mobile access strategy.

07.
The Future of Secure Mobile Infrastructures

The future of secure mobile infrastructure is being defined by a shift away from legacy tools like MDM and MAM toward more scalable, privacy-centric, and cloud-native solutions.

Virtual Mobile Infrastructure (VMI) is at the forefront of this transition. 51% of organizations believe VMI will have the greatest impact on secure mobility in the next three years—more than any other emerging technology.



Which of the following technologies do you believe will have the greatest impact on secure mobility in the next 3 years? Select up to three

This shift is backed by tangible momentum. 85% of organizations plan to increase their investment in secure mobility over the next year, with 42% expecting significant increases. In particular, the defense sector is leading, with a projected 90% increase in secure mobility investment and a 7.6% boost in BYOD-related budgets. This reflects a growing need to enable secure, flexible working while meeting regulatory and data protection requirements—particularly in highly sensitive environments.

VMI's alignment with Zero Trust principles also positions it for future relevance. While only 37% of organizations consider themselves experts in Zero Trust, 86% agree that VMI supports or enables a Zero Trust architecture, making it an accessible on-ramp for organizations struggling with more complex implementations.

Regional nuances are also shaping the future landscape. North America leads in both VMI adoption and expected impact (57%), while Europe lags slightly (45%), partly due to comparatively slower cloud and BYOD adoption, stricter data sovereignty concerns, and stronger cultural work-life separation.

47%
in APAC

57%
in North America

55%
in LATAM

45%
in Europe

Conclusion

In a mobile-first world, where privacy, compliance, and productivity are paramount, the future of secure mobility is clear: VMI offers a path forward that reduces risk, respects users, and prepares enterprises for the evolving digital workplace. Organizations that embrace it early will be better positioned to manage threats, scale securely, and meet rising employee expectations.

08.
Regional Insights

North America

North America leads in maturity, but faces its own pressures. The prevalence of remote and hybrid work has amplified BYOD reliance, increasing demand for scalable and privacy-conscious solutions, while regulatory scrutiny, particularly around data privacy and compliance, is also accelerating the move toward Zero Trust.

49% **of organizations in North America** consider their mobile security posture to be "very mature" — the highest of any region.

90% **of North American respondents believe VMI aligns with Zero Trust principles,** showing strong conceptual adoption.

57% **expect VMI to have the greatest impact** on secure mobility in the next three years — again, the highest globally.

LATAM (Latin America)

LATAM organizations face significant resource and expertise constraints, with infrastructure challenges—such as inconsistent connectivity—adding complexity to cloud-based deployments. Despite these hurdles, investment is accelerating: BYOD budgets in LATAM are projected to grow at a higher rate than the global average, as enterprises seek cost-effective ways to extend secure mobility without issuing secondary devices. Local economic volatility also makes ROI-driven solutions, like VMI, attractive compared to capital-intensive alternatives.

48% **in LATAM report the highest challenge in internal expertise/ resources for implementing VMI** — significantly above the global average (30%).

87% **believe VMI aligns with Zero Trust,** but implementation struggles are more prevalent due to skill and infrastructure gaps.

6.7% **BYOD budgets in LATAM are projected to grow significantly,** with investment increases above the global average (~5.4%).

APAC (Asia-Pacific)

In APAC, a highly mobile, app-driven workforce shows the greatest impact of restrictive MDM/MAM solutions on user expectations. At the same time, APAC shows strong Zero Trust expertise, tied with North America. The challenge here is balancing advanced security ambitions with end-user experience, particularly in markets like Japan, South Korea, and Singapore, where employee pushback against intrusive controls is strong. Rapid digitalization and government-led cybersecurity initiatives are driving adoption of more user-friendly solutions like VMI.

73% **of APAC respondents** say mobile security controls negatively impact user productivity — the highest across all regions.

42% **of APAC organizations rate their understanding of Zero Trust as expert-level,** tied with North America, above EMEA and LATAM.

89% **believe VMI supports a Zero Trust model,** showing strong theoretical alignment with future security strategies.

EMEA (Europe, Middle East, Africa)

EMEA lags in mobile security maturity. Regional complexity stems from stringent data sovereignty regulations, particularly under GDPR, which heighten sensitivity to how and where mobile data is stored. Ironically, however, it is the region where employee privacy ranks low as a deciding factor in mobile security strategies, reflecting a tension between regulatory compliance and internal priorities. Additionally, cloud adoption has been slower in parts of Europe and the Middle East, creating hesitancy toward VMI despite its privacy benefits.

25% **of organizations in EMEA** consider their mobile security posture "very mature" — the lowest of any region.

28% **of EMEA respondents** consider themselves experts in Zero Trust security principles — the lowest expertise level across all regions.

41% **of EMEA respondents say employee privacy is not a deciding factor** in mobile security strategy — reflecting the region's strong work-life separation norms and lower BYOD adoption.

Summary

While the drivers of mobile security investment are global—rising threats, BYOD expansion, and the shift to hybrid work—the barriers are distinctly regional. North America pushes forward under compliance pressure, LATAM wrestles with expertise and resource gaps, APAC grapples with productivity trade-offs, and EMEA navigates regulatory complexity and cloud adoption hesitancy. These local dynamics will continue to shape the speed and scale of secure mobility transformation, and determine where VMI gains traction first.

Why VMI is Better for BYOD

1.
Security-first design:
Corporate data never touches endpoints, reducing risk of leaks or theft

---

2.
Regulatory readiness:
Meets strict compliance standards (CMMC, HIPAA, FedRAMP) while keeping personal devices out-of-scope

---

3.
Privacy-first approach:
No need to enroll or wipe personal devices—employees keep full control

---

4.
Simplified IT footprint:
Apps are managed centrally, updates push once to the hosted environment, not individually per device

---

5.
OS flexibility:
While Hypori runs on an Android VM in a secure cloud environment—users can use the application on any device

Summary

VMI does not allow corporate data to be stored on employee devices, making it an ideal solution for BYOD that balances security, compliance and privacy. It avoids the pitfalls of MDM's invasive access and MAM's fragile app-level security, delivering a cleaner, more robust, and user-friendly approach.

09.
Conclusion: The Call to Action

As the market leader in virtual mobile infrastructure (VMI), the Hypori platform delivers secure mobile access to enterprise apps and data from any mobile device without processing, storing, or transmitting data on the device and without compromising user privacy.

Any organization wanting to modernize their enterprise mobility must rethink mobile access not as a device-centric challenge, but as a data-centric opportunity. Hypori VMI represents this shift – solving the dual challenge of securing corporate data while empowering users.

To request your demo today

Visit: **https://www.hypori.com/request-a-demo**
Or contact us: **info@hypori.com / +1.833.639.3964**

Offices:
1801 Robert Fulton Drive, Suite 340, Reston, VA 20191
11044 Research Blvd, Building B, Suite 530, Austin, TX 78759

Hypori
One Device, Zero Worries™

About Hypori

Hypori is the market leader in virtual mobile infrastructure (VMI), transforming secure virtual access for government, defense, healthcare, finance, and other regulated industries. The Hypori platform delivers secure mobile access to enterprise apps and data from any mobile device without processing, storing, or transmitting data on the device without compromising user privacy. Built on a zero trust architecture and designed to meet the highest security standards, Hypori eliminates the need for traditional mobile device or app management.

Trusted by leading federal agencies, global systems integrators, and enterprises with mission-critical data, Hypori is redefining the edge—one virtual device at a time. One Device. Zero Worries. The company is headquartered in Reston, VA, with a technology hub in Austin, TX.

For more information, visit **hypori.com**.

About Sapio Research

Sapio Research is a full-service B2B and tech market research agency that helps businesses grow thanks to high quality, efficient and honest research solutions.

We deliver valuable insights to support our clients understand their audience, build powerful brands, cut through the noise with great content and thought leadership. We're based in the UK and have access to over 149 million people across 130 countries, working with clients that range from top tech companies to global consultancies, Marketing/PR agencies and household name brands.

Our purpose-driven team of expert market researchers is passionate about providing data confidence for all and performing research that makes a difference. We're here to support our clients every step of the way in all areas of quantitative and qualitative research, so they can save time and thinking space, deliver with confidence, and unlock more value with their research.

For more information, visit **sapioresearch.com**.