The BYOD Opportunity

What MSPs need to close the last unmanaged gap

Author: Jessica Davis, Principal Analyst, Omdia

April 2026

In partnership with:

AURA Business

This Omdia White Paper was commissioned by Aura.

Contents

This Omdia White Paper was commissioned by Aura.

Executive Summary

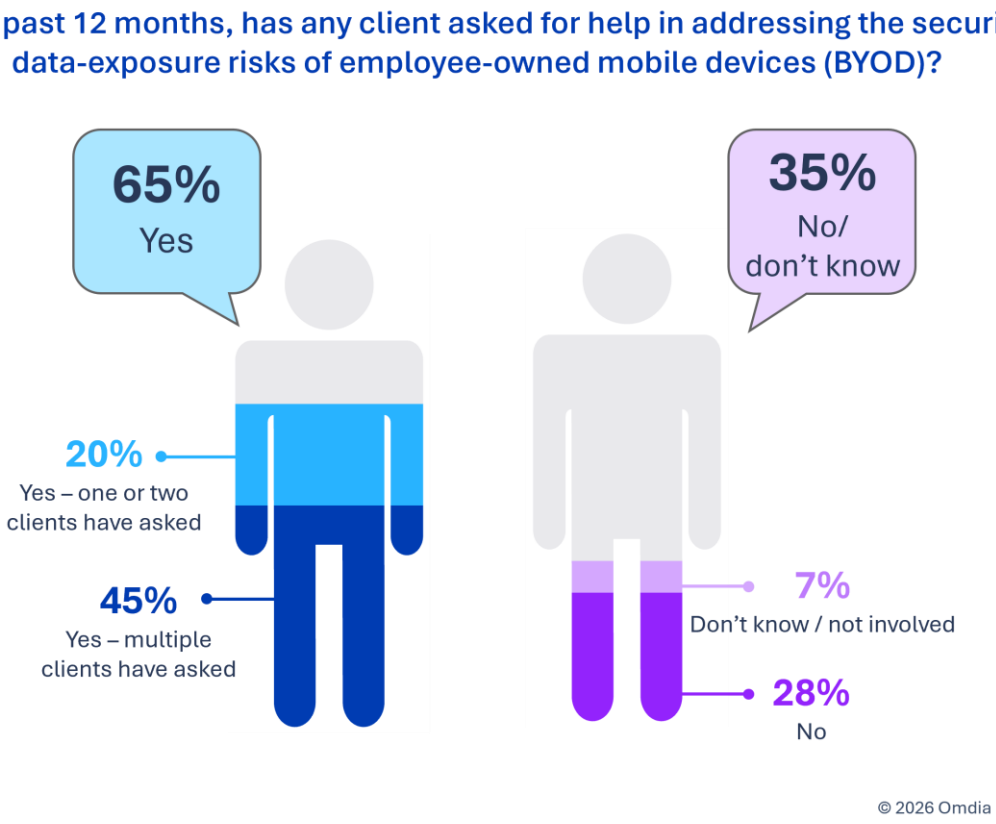
Employee-owned devices represent the last significant category of unmanaged risk for managed service providers (MSPs). In a survey of 319 US-based MSPs conducted by Omdia in early 2026, 65% reported client requests for bring your own device (BYOD) security help, and 55% had experienced at least one BYOD-related security incident in the past 24 months. The most common incidents are identity-based—credential theft and email compromise—rather than physical device loss. Despite clear demand and demonstrated risk, most MSPs have not formalized a BYOD offering, citing operational complexity and liability concerns as the primary barriers. This report examines the market conditions, the evolving solution landscape, and the delivery model MSPs prefer for closing this unmanaged gap.

This Omdia White Paper was commissioned by Aura.

The demand signal for BYOD

MSP clients are looking for help with BYOD security. In a survey of 319 US-based MSPs conducted by Omdia in early 2026, 65% reported that at least one client had asked for help addressing the security or data-exposure risks of employee-owned devices in the past 12 months. Nearly half—45%—said multiple clients had raised the issue.

Figure 1



Source: Omdia

The demand is not confined to MSPs serving large enterprises. It's even more common among those serving mid-market clients with 100 or more employees; 70% state they have received the request. Even among MSPs focused on small businesses with fewer than 10 employees, 42% have heard BYOD-related requests from customers.

The nature of these requests is practical and action-oriented. Half of MSPs report that clients want help implementing technical controls, while 46% were asked for best-practice recommendations, and 40% were asked to define or review BYOD policies. These are not abstract inquiries. They are

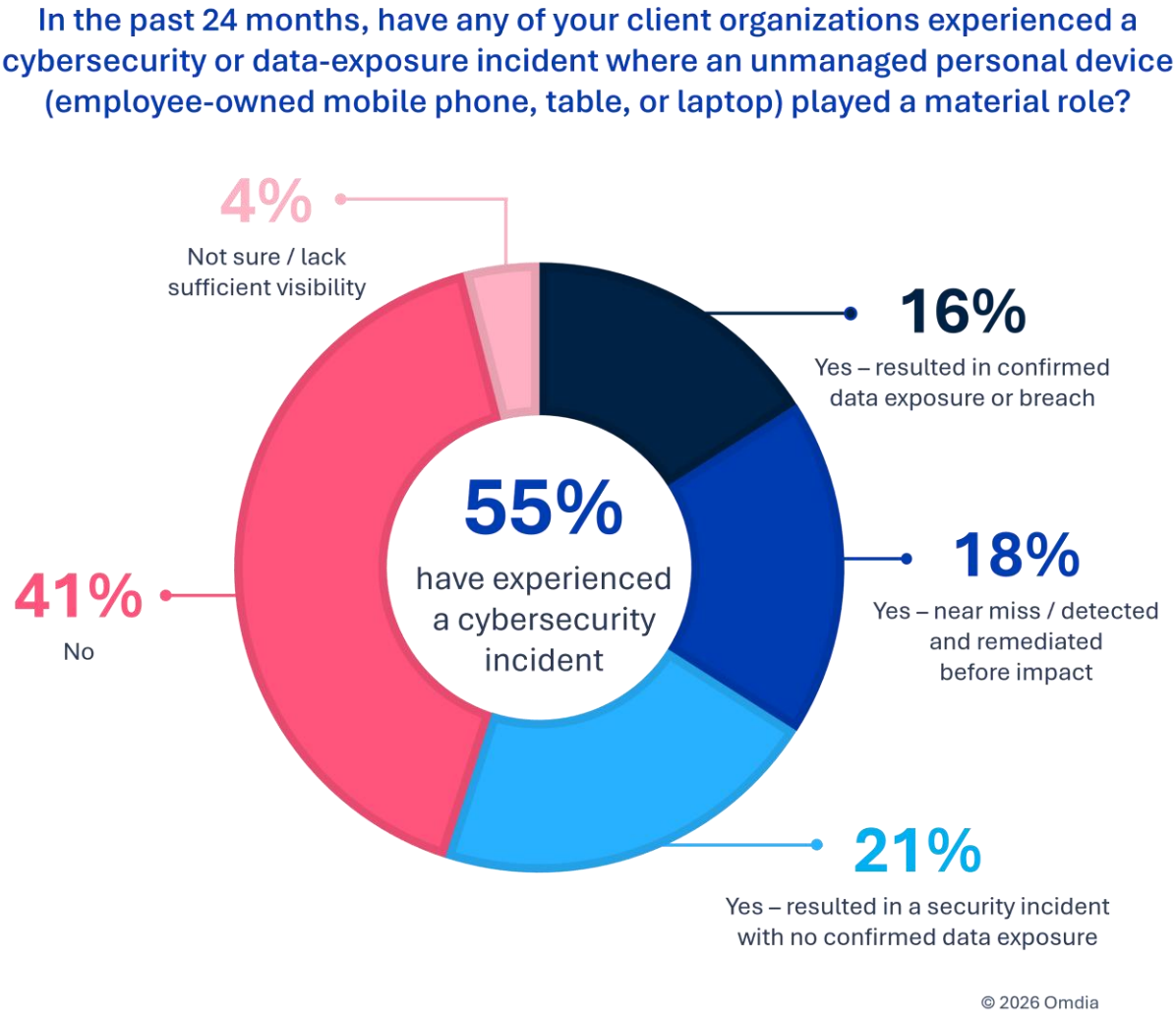
structured, repeatable engagements—the kind that map directly to MSP recurring service models. Indeed, offering these services to end customers can yield an additional revenue stream.

The demand signal is clear among MSP customers, and it is broad-based and already generating client conversations across the MSP market.

The risk reality

Why are customers so concerned? The BYOD conversation is not speculative. More than half of MSPs surveyed have already experienced what BYOD governance is designed to prevent.

Figure 2



Source: Omdia

Of those surveyed, 55% of MSPs reported at least one BYOD-related security incident in the past 24 months—an incident where an unmanaged personal device played a material role. Meanwhile, 21% experienced a security incident with no confirmed data exposure, 18% caught a near miss that was detected and remediated before impact, and 16% reported a confirmed data breach.

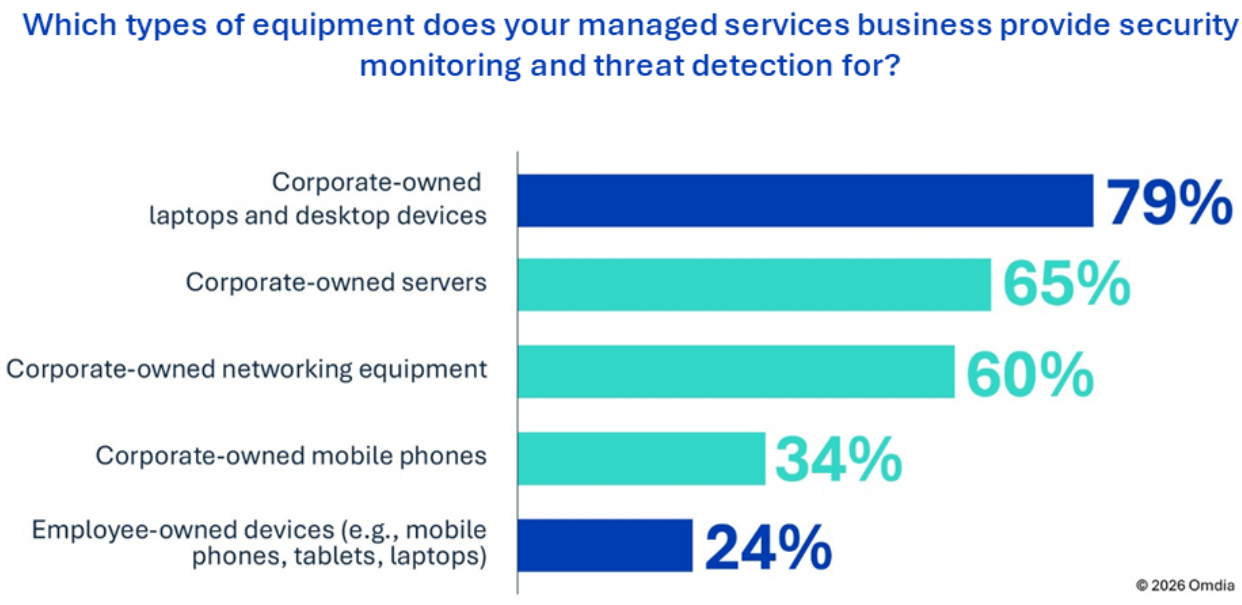
Those who hadn't been touched by a BYOD incident were in the minority.

The BYOD risk scales with visibility. MSPs with more than $10 million in annual recurring revenue reported a 61% security incident rate, compared to 52% for smaller MSPs. This likely reflects a detection gap rather than a difference in actual exposure—MSPs with more monitoring infrastructure see more incidents. This means that the 55% overall figure may understate the true prevalence, particularly among MSPs with limited visibility into personal device activity.

Yet, MSPs manage the risk of employee-owned devices at a much lower rate than they manage the risk of any other customer device.

There is a 55-percentage-point gap between corporate laptop monitoring (79% of MSPs) and employee-owned device monitoring (24%). Corporate mobile phones sit at 34%. MSPs have progressively extended security coverage from servers to networks to corporate endpoints, but personal devices—the devices that are most likely to access corporate email, files, and credentials outside the managed perimeter today—remain largely unmonitored.

Figure 3



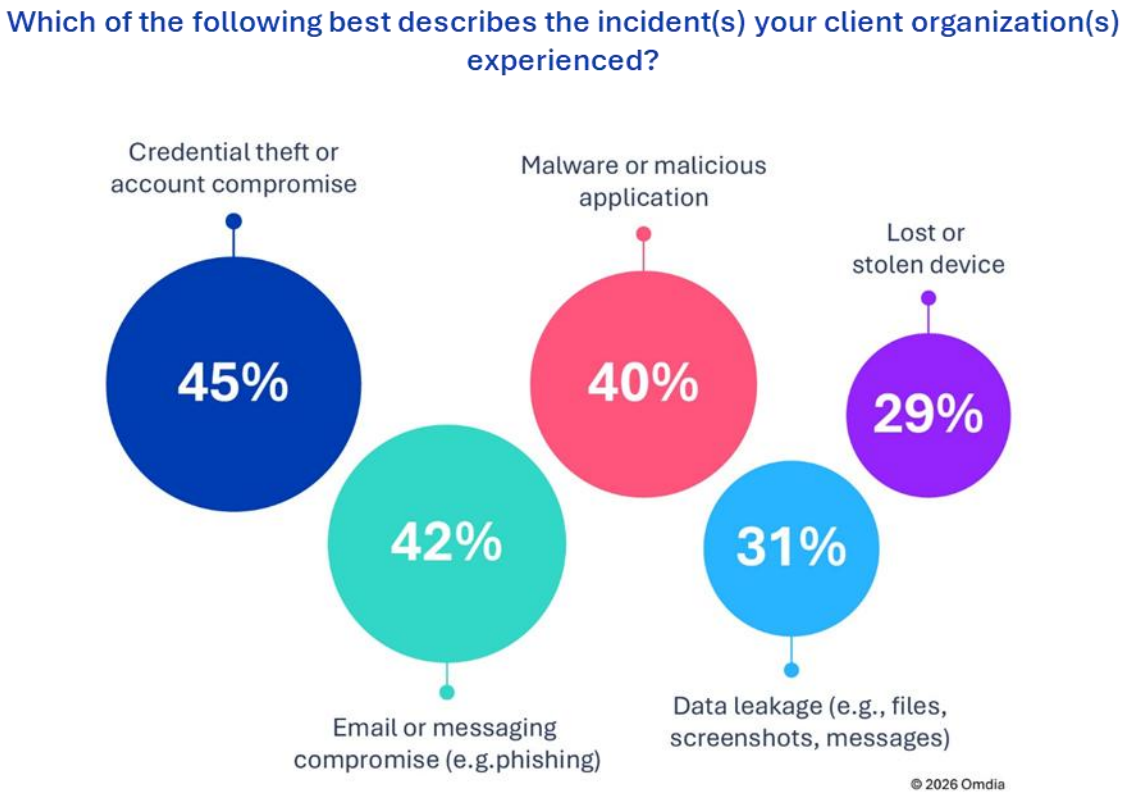
Source: Omdia

That gap is not a planning oversight. MSPs in the past have avoided managing devices not owned by the customer company for a few important reasons. That said, the threat landscape and cybersecurity protections have evolved.

The threat has moved to the identity layer

The profile of BYOD incidents challenges a longstanding assumption. For years, the primary mobile security concern was physical—a lost phone, a stolen laptop. The survey data tells a different story.

Figure 4



Source: Omdia

Among the 177 MSPs who reported BYOD-related incidents, credential theft or account compromise was the most common type, cited by 45%. Email or messaging compromise—primarily phishing—was second at 42%. Malware ranked third at 40%, while data leakage, including files, screenshots, and messages, was reported by 31% of respondents. Lost or stolen devices ranked last at 29%.

The most prevalent BYOD risks are identity-based, not device-based. Attackers are compromising credentials and email accounts on personal devices that touch corporate systems—not physically taking hardware. This has implications for how MSPs evaluate BYOD governance solutions.

Approaches anchored primarily to device management address an important layer, but not the most commonly reported threat vectors.

Recent incidents in the broader threat landscape reinforce this pattern. Credential-based attacks that leverage native management tools—so-called living-off-the-land techniques—have demonstrated that a compromised identity can turn a device management platform itself into an attack vector. MSPs are familiar with this pattern from their own ecosystem, where remote management tools have been similarly exploited.

The incident data points toward BYOD governance strategies that address the identity layer alongside device management—not as a replacement, but as a necessary complement.

Demand, risk, and opportunity converge

The combination of client demand, incident prevalence, and the shift toward identity-based threats points to a commercial opportunity for MSPs—if they can find a delivery model that fits.

The demand is there: 65% of MSPs are fielding client requests. The risk is also there: more than half of MSPs have seen incidents, and the threat vectors are well-defined. The competitive context favors investment in security-adjacent services. While standard IT services face increasing pricing pressure, cybersecurity services remain a source of differentiation and margin protection for MSPs.

Yet adoption of BYOD management remains low. Only 24% of MSPs monitor employee-owned devices. Only 22% of those managing mobile devices manage both corporate and BYOD. The market conditions support a BYOD governance offering, but most MSPs have not built one.

The gap between opportunity and adoption is not explained by a lack of awareness. MSPs know their clients want this. They have seen the incidents. What they have not found is a delivery model that meets their conditions.

This Omdia White Paper was commissioned by Aura.

What kind of solution fits?

The barriers MSPs cite are well-established: operational complexity, legal liability, and the risk that a BYOD incident spreads into the broader client environment. These concerns are rational, and they have historically been difficult to address. A solution that requires per-device configuration, manual enrollment, and client-by-client policy scoping does add operational burden. A solution that gives the MSP ownership of a personal device does create liability exposure.

Figure 5

Source: Omdia

However, the solution landscape is evolving. MSPs themselves are describing what the next generation of BYOD governance looks like—and it does not resemble the models that created these barriers in the first place.

In open-ended responses, MSPs called for automated, self-service enrollment workflows. They asked for hyper-automated onboarding and selective wipe processes that can scale to thousands of users. They described a shift from device-centric to identity-centric security models—protecting the credential and the session rather than controlling the hardware. Additionally, they

emphasized that BYOD governance must operate alongside the existing security stack, not complicate it.

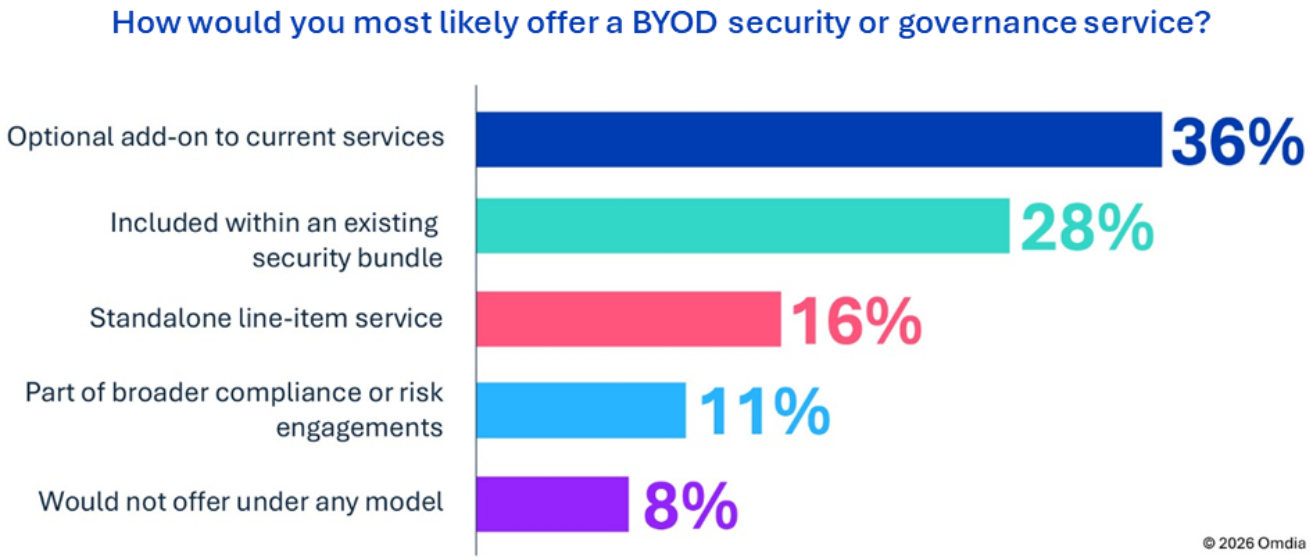
> "The ecosystem must shift from reactive device management to an identity-centric, automated, and privacy-first architecture."
>
> — US-based MSP

These are not aspirational descriptions. Solutions with these characteristics exist today. The question for MSPs is no longer whether the technology can meet their conditions, but whether they are evaluating BYOD governance against its current capabilities or against the limitations of earlier approaches that shaped their initial reluctance.

The commercial opportunity for MSPs

92% of MSPs said they could see a path to offering BYOD services under some model. The question is packaging. The top choice is to offer such services as an optional add-on to existing services (36%).

Figure 6



Source: Omdia

What does this mean for MSPs?

Employee-owned devices represent the last significant category of unmanaged risk in the modern IT estate.

These devices regularly access corporate email, files, and credentials, but they sit outside the managed perimeter. MSPs have progressively extended security monitoring from servers to networks to corporate endpoints. Personal devices are where that progression stalls.

The survey data shows this is where demand, incidents, and commercial opportunity converge. Clients are asking for help. Incidents are already occurring, and the most common types are identity-based. MSPs have clear conditions for adoption, and the solution landscape is evolving to meet them. The preferred delivery model—an optional add-on to existing services—fits how MSPs already build their service stack.

BYOD service plans sit squarely in a service category that is not being squeezed by commoditization. It is a security-adjacent service with demonstrated client demand and a defined threat profile.

MSPs who close this gap first will not just reduce risk for their clients. They will build a competitive position in the part of the market that still rewards specialization.

Conclusions

The threat landscape does not wait for MSPs to build the perfect service offering. Credential-based attacks are accelerating, personal devices that access corporate systems are multiplying, and the living-off-the-land pattern—where attackers weaponize the management tools organizations already trust—has moved from theoretical concern to operational reality.

MSPs are well-positioned to respond. They already have the client relationships, the security foundations, and the commercial infrastructure. 76% treat security as core to their practice, and 92% can envision a BYOD delivery model. Furthermore, their clients are already asking.

The survey data suggest that the conditions that created MSP reluctance are shifting. MSPs themselves are describing the next generation of BYOD governance in terms that differ meaningfully from the approaches that shaped their initial caution—automated, identity-centric, and designed to operate alongside the existing stack rather than complicate it.

MSPs who formalize a BYOD offering can close the biggest remaining unmanaged gap in their security practice. Cybersecurity specialization still commands a margin of protection that other stack components do not. In a market where standard IT services face increasing pricing pressure, that distinction matters.

Appendix

Methodology

Omdia conducted a survey of 319 US-based MSPs in 1Q26. All respondents derived more than 50% of their revenue from managed services. The sample captures a range of MSP sizes: 38% reported annual recurring revenue above $10 million, with the remainder below that threshold. Sixty percent of respondents were at the director level or above. The client profile skews mid-market: 59% of respondents serve clients with 100 or more employees, though MSPs serving smaller clients are also well represented in the sample.

Further reading

Omdia Cybersecurity Partner 500 (February 2026)

MSP Trends and Predictions 2026 (January 2026)

Cybersecurity Decision Maker Survey 2025: Identity, Authentication, Access (September 2025)

Signal versus noise: how channel partners are navigating MDR services (May 2025)

Jessica Davis, Principal Analyst, MSPs
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B Materials information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer