From IT Support to Cybersecurity Powerhouse:

The New Mandate for MSP Growth

Independent Survey Commissioned by WatchGuard

Executive Summary

New global research from WatchGuard signals a defining moment in cybersecurity. A comprehensive global study of IT and cybersecurity leaders across SMB and midmarket organizations reveals a market at a critical inflection point. As cyber threats grow more sophisticated, persistent, and resource-intensive, internal teams are being pushed beyond their limits, driving a decisive shift toward managed service providers (MSPs) for the expertise, scale, and strategic partnership required to keep pace.

This shift is redefining the role of MSPs. Organizations are no longer looking for basic IT support; they expect proactive, outcome-driven security partners that deliver measurable protection, innovation, and operational relief. At the same time, rising expectations are raising the bar for performance, responsiveness, and value.

Contents

SMB and Midmarket IT Teams Are Outmatched by Growing Cybersecurity Demands

Despite 55% of organizations reporting that their IT teams are adequately staffed, the reality is more complex. Cybersecurity demands are expanding across both scope and time. Two-thirds (67%) of organizations require additional support to manage growing compliance requirements, while more than half (54%) cite the need for continuous, 24/7 monitoring and support – an expectation that most internal teams are not structured to meet alone.

This combination is shifting cybersecurity from a manageable function to a continuous operational challenge that exceeds internal capacity.

That pressure is reinforced by the volume and frequency of real-world incidents. Organizations report consistent exposure to multiple types of threats:

- **Malware or virus infections: 33%**
- **Phishing and business email compromise: 32%**
- **Data breaches or unauthorized access: 29%**

These are not isolated events. Almost 75% experienced at least one cybersecurity incident in the past year, placing sustained pressure on teams to respond, recover, and prevent future attacks.

As a result, organizations are increasingly turning to external support. Nearly half (48%) already rely on external providers to supplement internal teams, while others outsource most or all security functions, reflecting a growing dependence on external expertise to close capability gaps.

Key takeaway: Internal teams are capable, but outmatched by the scale, speed, and continuity of modern cybersecurity demands.

Cybersecurity Incidents Experienced by Organizations (Last 12 Months)

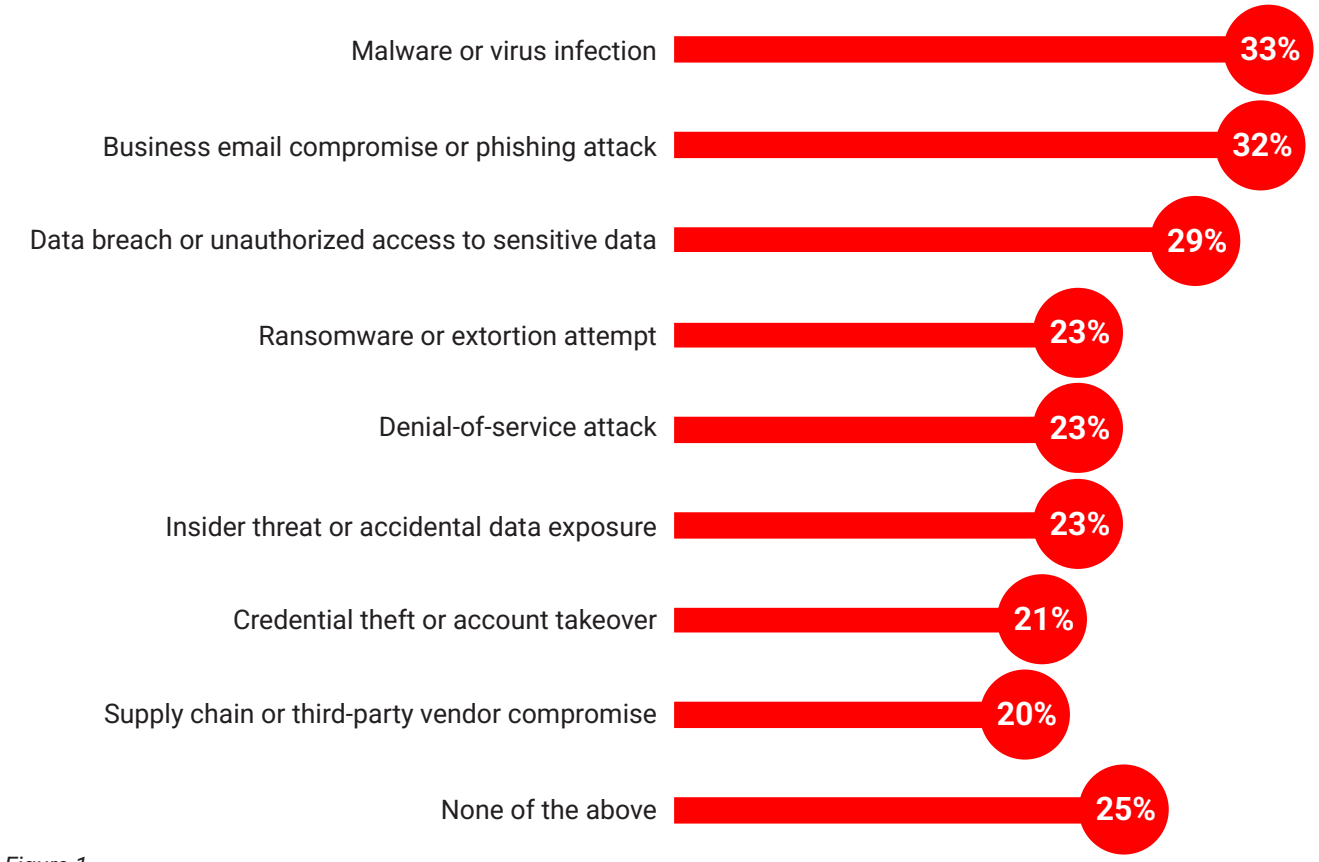

Figure 1

Demand Is Shifting Toward Outcome-Driven Security Partnerships

As internal strain increases, expectations for external partners are evolving in parallel. Organizations are no longer evaluating providers solely on the services they deliver, but on the outcomes they enable.

Current adoption patterns still reflect foundational security priorities. The most widely used services include:

- **Network security and firewall protection: 65%**
- **Managed threat detection and response: 57%**
- **Risk assessments and vulnerability management: 55%**

However, demand is shifting beyond these core capabilities toward more advanced and integrated solutions. Organizations increasingly prioritize and would like additional support from their providers in the following areas:

- **AI-driven threat detection and response: 44%**
- **Managed detection and response: 36%**
- **Risk assessments and vulnerability management: 35%**
- **Identity and access security: 35%**

At the same time, expectations are rising for how services are delivered. Customers are placing greater emphasis on:

- **Faster incident response: 38%**
- **Employee cybersecurity training: 37%**
- **Improved communication and transparency: 31%**

This shift is also reflected in how organizations perceive their providers. Nearly half already view their MSP as either a strategic advisor (24%) or a proactive partner (23%), indicating a move toward deeper, outcome-based relationships, while also highlighting that a significant portion of the market has yet to fully transition.

Key takeaway: Customer expectations are shifting from service delivery to measurable security outcomes, requiring MSPs to expand capabilities while improving speed, transparency, and overall experience.

Areas Where Customers Want More Provider Support

Option	Rank	Response %
AI-driven response capabilities	1	44%
Managed threat detection and response	2	36%
Risk assessments and vulnerability management	3	35%
Identity and access security	4	35%
Network security and firewall protection	5	33%
Backup and ransomware recovery	6	32%
Incident response and breach management	7	30%
Security operations center services	8	30%
Endpoint security	9	27%
Zero-trust architecture	10	26%
None of the above	11	5%

Figure 2

AI Is Raising Both Risk and Customer Expectations

AI is becoming a central force in cybersecurity, expanding the range of threats organizations must address while increasing expectations for faster, more adaptive defense.

- **91% of organizations report at least some concern about AI-driven cyberattacks**
- **44% want AI-driven response capabilities from their provider**
- **44% are willing to pay more for AI-driven threat detection and automated response**

Taken together, these signals suggest that AI is no longer an emerging consideration. It is already influencing how organizations assess cybersecurity risk, where they expect providers to innovate, and which capabilities they are willing to fund.

Confidence in providers remains strong, but it is not evenly distributed. Overall, 91% of organizations say their cybersecurity provider adequately protects them from emerging threats, including AI-driven attacks. Among those using a dedicated MSP or MSSP, that confidence rises to 94%, compared with 93% for general IT support companies or VARs, 89% for internet or telecom providers, and 83% for consulting or professional services firms.

This suggests that as AI reshapes both the threat landscape and the required response, organizations are increasingly looking to specialized providers to keep pace. Rather than developing every capability internally, many are relying on MSPs to operationalize AI within detection, response, and broader security operations.

Key takeaway: AI is accelerating both cybersecurity risk and customer expectations, making it an immediate driver of provider evaluation, service demand, and willingness to invest.

Perceived Effectiveness of Cybersecurity Providers Against Emerging Threats

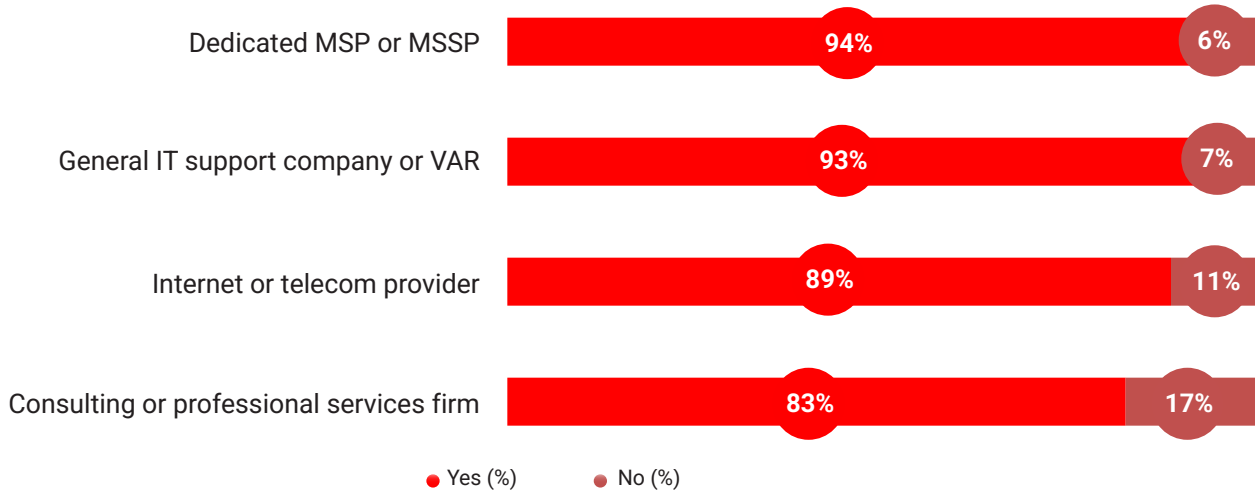

Figure 3

Cybersecurity Spending Is Increasing – With a Clear Focus on Value

Despite broader cost pressures, organizations are continuing to invest in cybersecurity – particularly in areas that deliver clear, measurable outcomes.

Willingness to pay more is concentrated around capabilities that improve responsiveness and strengthen protection:

- **24/7 monitoring and rapid incident response: 47%**
- **AI-driven detection and response: 44%**
- **Proactive threat hunting: 37%**

This aligns with broader spending trends. Three-quarters (75%) of organizations expect their cybersecurity spending to increase over the next two years, indicating sustained prioritization of security investments.

At the same time, perceived value remains high. A majority (78%) say their cybersecurity provider delivers value above cost, suggesting that investments are being evaluated based on outcomes rather than price alone.

MSP clients report the strongest returns, and are more likely to view their providers as strategic partners rather than service vendors—further reinforcing the shift toward outcome-based relationships.

Key takeaway: The market is not price-sensitive; it is value-sensitive.

Key Drivers for Incremental Cybersecurity Spend

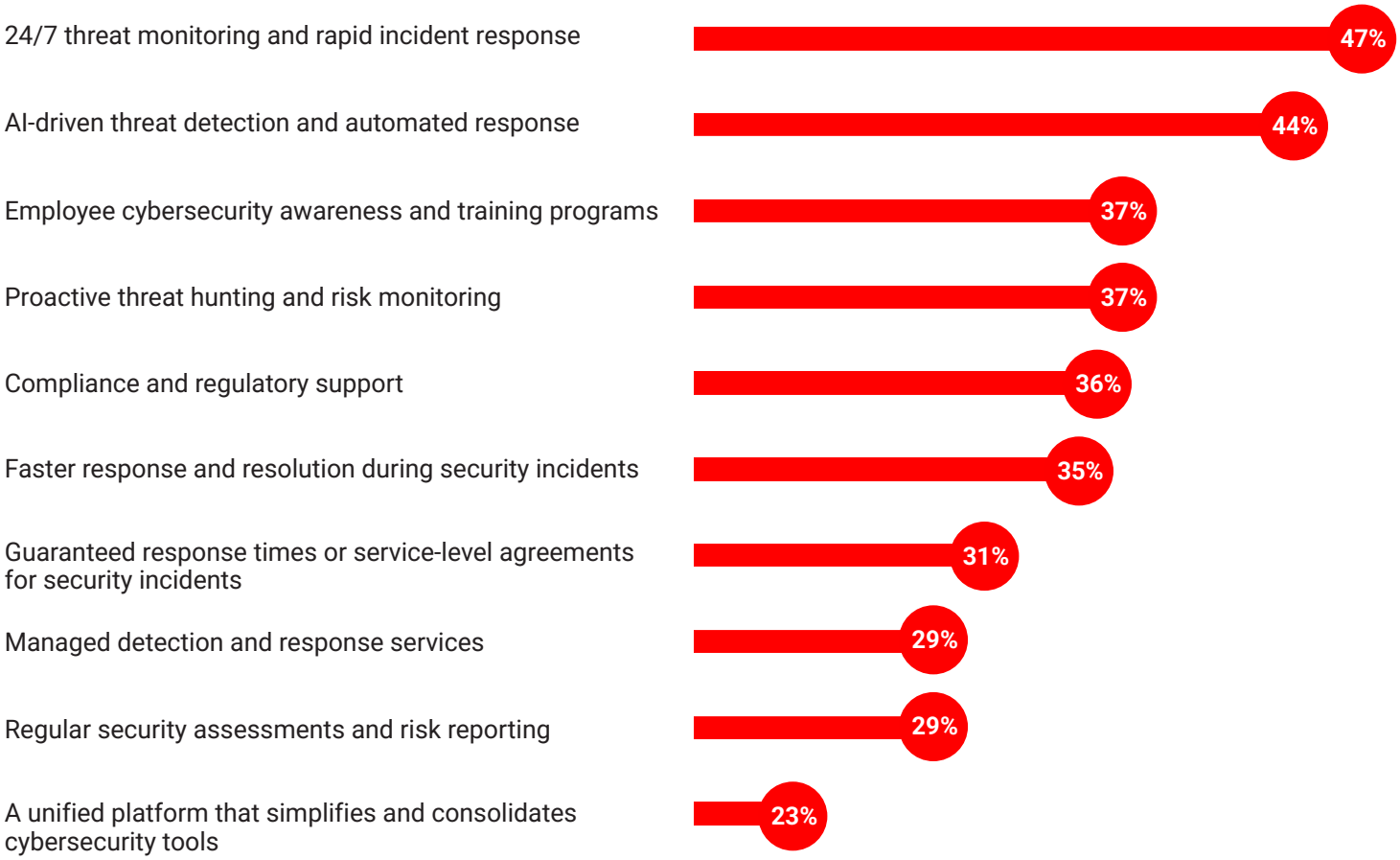

Figure 4

Switching Risk: What MSPs Must Get Right

While overall satisfaction with cybersecurity providers is strong, switching intent remains significant. More than half of organizations (58%) expect to change providers within the next three years, indicating that loyalty is increasingly tied to ongoing performance rather than long-term relationships.

The primary drivers of switching are closely tied to perceived value and operational effectiveness:

- **Rising costs without added value: 39%**
- **Major security incident: 39%**
- **Slow response times: 36%**

Additional factors include lack of innovation, poor communication, and insufficient proactive guidance—further reinforcing that customers are evaluating providers on both outcomes and experience.

Key takeaway: High satisfaction does not eliminate switching risk. As expectations rise, organizations are more willing to replace providers that fail to deliver consistent value, responsiveness, and innovation.

Primary Drivers for Switching Cybersecurity Providers

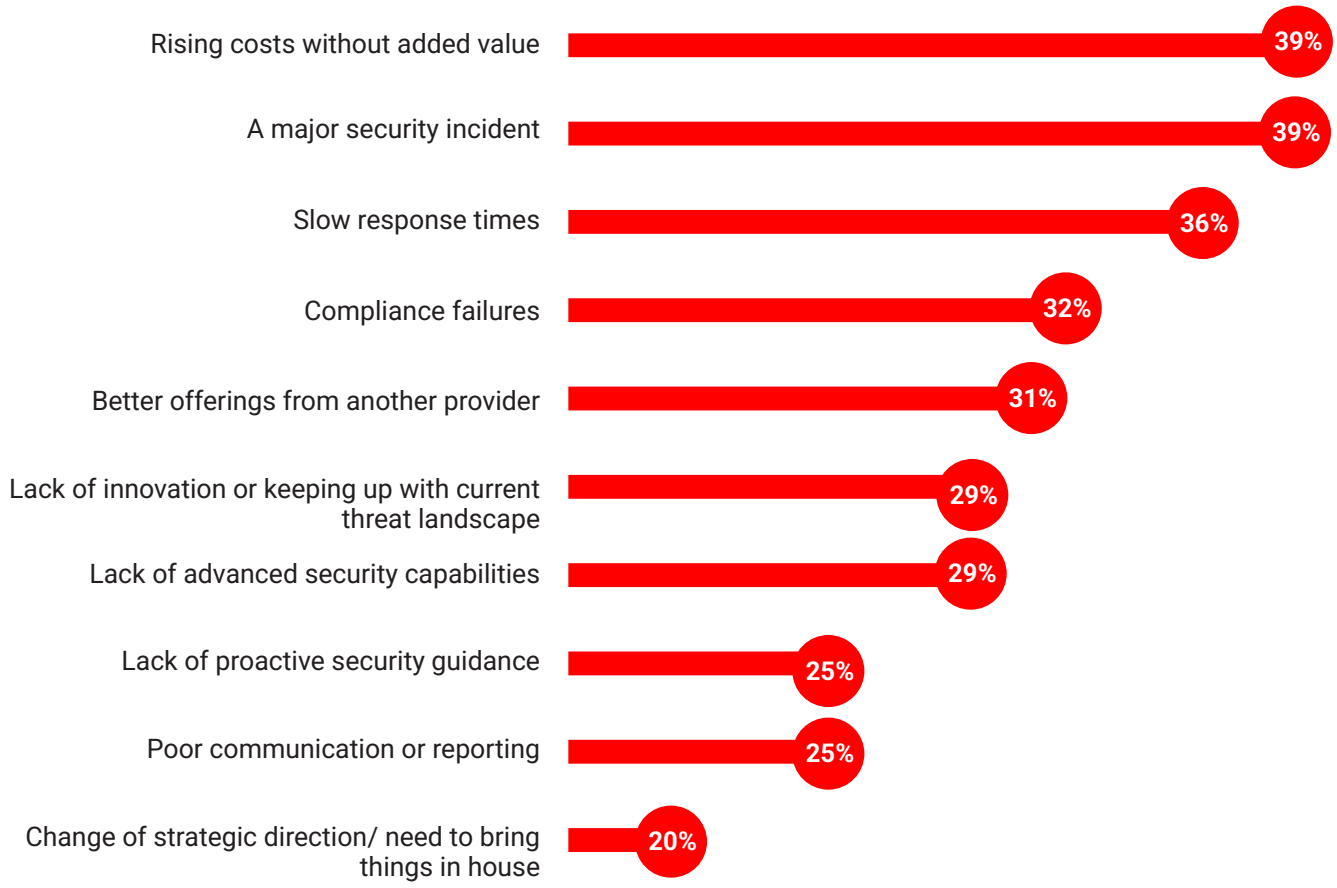

Figure 5

Regional Insights: A Fragmented but Converging Market

Adoption of external cybersecurity providers varies significantly by region, reflecting different levels of market maturity and service preferences.

- **France: Highly MSSP-driven (65%)** – mature outsourcing model
- **Mexico: VAR-dominated (49%)** – earlier-stage opportunity for MSSPs
- **Canada: Consulting-led (31%)** – advisory-focused approach
- **United States:** Balanced mix of VARs, MSPs, and telecom providers – mature but fragmented ecosystem
- **United Kingdom:** Shorter provider tenure, with 30% reporting one-to-two-year relationships – higher switching behavior

These regional differences highlight varying paths to cybersecurity maturity. More developed markets tend to adopt managed services models, while others continue to rely on traditional IT support or advisory-led approaches.

Despite this fragmentation, customer expectations are increasingly consistent across regions. Organizations globally are prioritizing:

- **24/7 monitoring and rapid response**
- **AI-driven capabilities**
- **Support for compliance and regulatory requirements**
- **Faster response times and improved service delivery**

Key takeaway: While regional maturity and provider models differ, global customer expectations are converging around speed, capability, and measurable security outcomes.

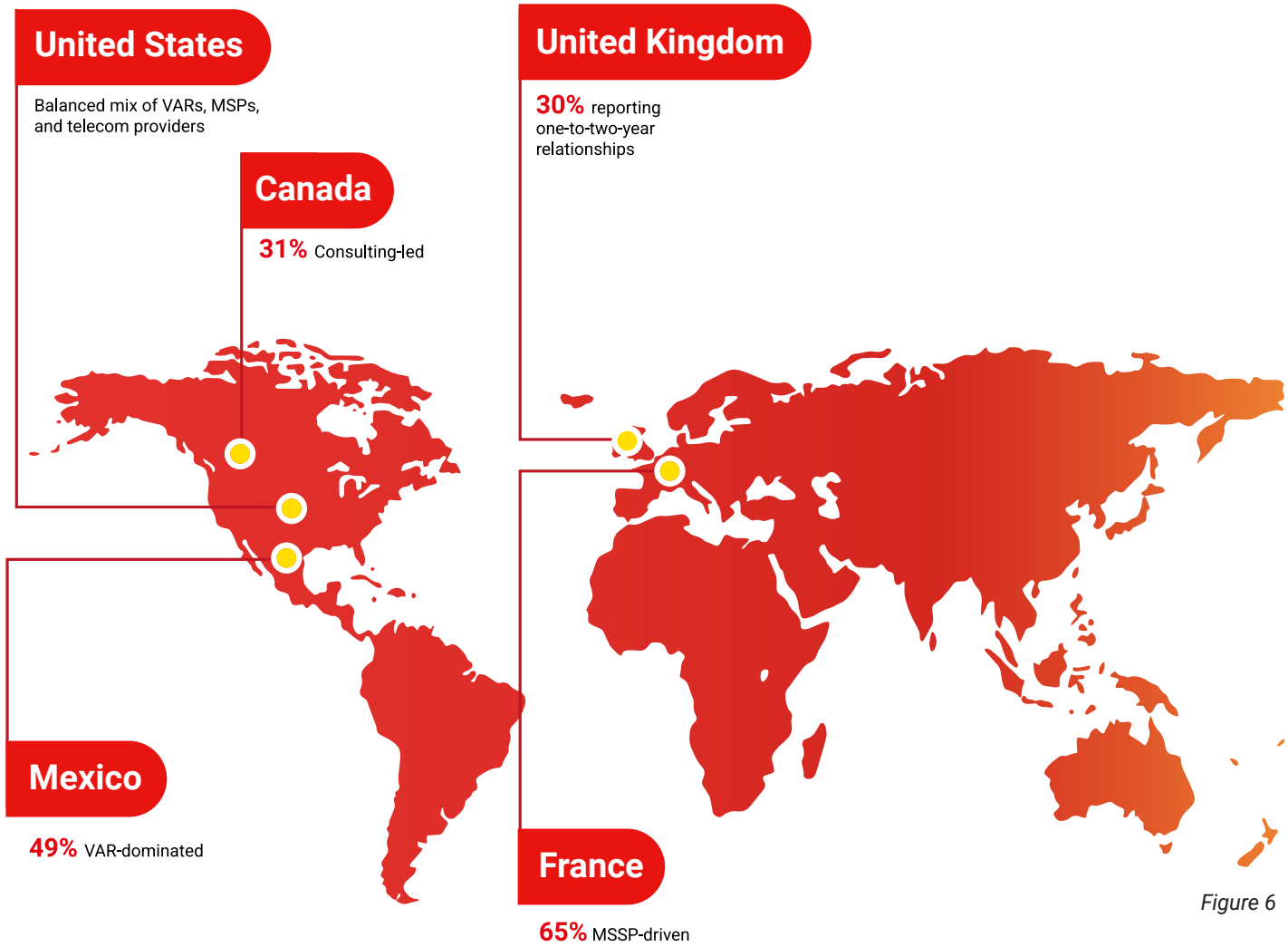

Figure 6

What This Means for MSPs: Strategic Recommendations from WatchGuard

To compete in this evolving market, MSPs must transform how they position, deliver, and monetize their services. WatchGuard recommends that MSPs take the following six actions:

1

Evolve from Service Provider to Strategic Security Partner

Customers want proactive advisors – not reactive vendors. MSPs should:

- Provide continuous risk assessment and strategic guidance
- Deliver outcome-based reporting
- Position as long-term advisors

2

Expand Advanced Security Capabilities

Demand is strongest for modern, integrated security services. MSPs should prioritize:

- AI-driven detection and response
- Managed detection and response (MDR)
- Identity and access security / zero trust

3

Differentiate Through Speed, Automation, and Innovation

Slow response times and lack of innovation are leading drivers of provider switching. MSPs must:

- Invest in automation for faster response
- Offer SLAs and guaranteed response times
- Continuously evolve capabilities

4

Deliver Integrated, Simplified Security Platforms

Customers value simplicity and consolidation. MSPs can increase value by:

- Offering unified cybersecurity platforms that reduce tool sprawl
- Integrating endpoint, network, identity, and cloud security
- Consolidating tools into unified platforms
- Providing centralized visibility and reporting

5

Monetize Value-Based Services

With SMB and midmarket customers showing a strong willingness to pay for advanced capabilities, MSPs should:

- Package premium offerings such as MDR, threat hunting, and compliance
- Align pricing with outcomes – such as risk reduction, uptime, compliance readiness – not inputs
- Clearly communicate ROI and value delivered

6

Strengthen Customer Experience

Beyond technology, customer service experience remains critical. Therefore, MSPs should:

- Improve communication, reporting, and transparency
- Offer cybersecurity awareness training and education for employees
- Reinforce trust and value through proactive support and regular engagement

Conclusion

The research confirms that the MSP market is undergoing a fundamental shift. SMB and midmarket organizations are overwhelmed by cybersecurity complexity and are actively seeking more capable, proactive partners who can deliver measurable outcomes.

MSPs that invest in AI, expand advanced capabilities, improve speed and transparency, and position themselves as strategic advisors will capture growing demand, increase customer loyalty, and drive higher-value recurring revenue.

The WatchGuard View:
Insights from CEO Joe Smolarski

As a CEO in the cybersecurity industry, I see this moment as a tremendous opportunity for MSPs. The data is clear: SMB and midmarket organizations are not lacking commitment or awareness; they are simply overwhelmed by the scale, speed, and sophistication of today's threat landscape. This creates a powerful opening for MSPs to step forward as trusted security leaders. The providers who succeed will be those who recognize that their role is no longer to "support IT," but to actively defend businesses, enable resilience, and deliver measurable security outcomes.

To meet this moment, MSPs must fully embrace their evolution into strategic cybersecurity partners. That means moving beyond reactive service delivery and leaning into proactive risk management, continuous monitoring, and executive-level guidance. Your customers are looking for clarity in chaos: they need partners who can translate complex threats into actionable strategies and business value. The MSPs who invest in advisory capabilities, outcome-based reporting, and consistent engagement will not only differentiate themselves but will also become indispensable to their clients' long-term success.

At the same time, the path forward requires bold investment in advanced capabilities, particularly in AI-driven security. AI is redefining both the threat and the defense, and customers are signaling loud and clear that they are willing to invest in providers who can harness it effectively. This is your moment to lead with innovation: adopt AI-powered detection and response, automate where speed matters most, and build integrated security platforms that simplify complexity for your customers. Those who hesitate risk falling behind; those who act decisively will set the new standard for the industry.

Equally important is the experience you deliver. In a market where switching intent is high, responsiveness, transparency, and trust are just as critical as technology. Fast incident response, clear communication, and ongoing education are not "nice to have". They are core to customer retention and growth. MSPs that consistently demonstrate value, align pricing with outcomes, and communicate their impact in business terms will not only retain clients but also expand relationships and drive higher lifetime value.

Finally, and perhaps most importantly, MSPs should feel confident about the future. The demand signals are undeniable: rising cybersecurity budgets, increasing reliance on external expertise, and a clear preference for providers who deliver real outcomes. This is a growth market fueled by necessity, not trend. If you invest in innovation, lead with expertise, and commit to delivering measurable protection, your role will only become more critical. The organizations you serve need you now more than ever. And for MSPs willing to rise to the occasion, the future is not just bright, it is foundational to the next era of cybersecurity.

WatchGuard Technologies is a global leader in unified cybersecurity, purpose-built for managed service providers (MSPs). For more than 30 years, WatchGuard has defined how MSPs deliver security at scale, continuously innovating to stay ahead of every major shift in the threat landscape. WatchGuard's AI-powered Unified Security Platform® delivers zero trust-aligned network, endpoint, and identity protection in a single, integrated platform, enabling MSPs to reduce operational complexity, improve security outcomes, and grow their businesses more efficiently. Trusted by more than 25,000 MSPs protecting over 1.5 million customers worldwide, WatchGuard enables partners to deliver strong, measurable security outcomes for customers across the globe. Learn more at **WatchGuard.com**.

The findings are based on an independent online survey of 842 IT and cybersecurity professionals at organizations with 2 to 2,499 employees. The survey was conducted in April 2026 across 20 countries, including the United States, Canada, Mexico, Germany, the United Kingdom, France, Australia, Colombia, and Argentina, with results weighted to reflect global economic distribution.