



Cyber Security

Channel Market Report

Executive Summary

The global cybersecurity market is experiencing robust growth, driven by escalating cyber threats, rapid digital transformation, and increasing regulatory pressures. Valued at approximately USD 225.7 billion in 2025, the market is projected to reach USD 443.1 billion by 2032, growing at a compound annual growth rate (CAGR) of 10.2%.

Channel partners, including Managed Service Providers (MSPs), Value-Added Resellers (VARs), and system integrators, are pivotal to this ecosystem, facilitating over 90% of cybersecurity spending.

This report provides channel partners with insights into market trends, opportunities, challenges, and strategies to capitalize on the evolving cybersecurity landscape in 2025 and beyond.



Executive Summary.....	3
Market Overview.....	3
Market Trends.....	4
Opportunities for Channel Partners.....	4
Challenges for Channel Partners.....	5
Competitive Landscape.....	5
Strategic Recommendations.....	6
Conclusion.....	6

Executive Summary

The cybersecurity sector is experiencing robust growth, propelled by escalating cyber threats, rapid digital transformation, and stringent regulatory requirements. Currently valued at approximately \$225.7 billion in 2025, the market is projected to reach \$443.1 billion by 2032, growing at a compound annual growth rate of 10.2%.

Channel partners, including Managed Service Providers (MSPs), Value-Added Resellers (VARs), and system integrators, play a pivotal role in this ecosystem, facilitating over 90% of cybersecurity spending.

This report provides channel partners with a comprehensive analysis of market trends, opportunities, challenges, and strategies to thrive in the evolving cybersecurity landscape in 2025 and beyond.

Market Overview

The global cybersecurity market is poised for significant expansion, with a 2025 valuation of \$225.7 billion and an expected growth to \$443.1 billion by 2032.

North America leads the market, driven by technological advancements, rigorous regulations, and high threat levels, with the U.S. alone projected to contribute \$88.25 billion in 2025. Meanwhile, the Asia-Pacific region is the fastest-growing, fueled by rapid digitalization, increased internet penetration, and government-led cybersecurity initiatives.

The channel remains critical, with 91% of cybersecurity spending in Q2 2024 flowing through partners, underscoring their essential role in market growth. Key drivers include the rising sophistication of cyberattacks, such as ransomware, projected to cost USD 220 billion by 2030, and phishing, which accounted for 75% of attacks in 2024.

Additionally, digital transformation through cloud computing, IoT, and AI is expanding the attack surface, while regulations like GDPR and NIS2 are pushing organizations, particularly SMBs, to invest in compliance. A global shortage of 3.5 million cybersecurity professionals in 2024 further amplifies demand for managed services, creating significant opportunities for channel partners.

Market Trends

The cybersecurity landscape is evolving rapidly, with several trends shaping the market. A notable shift toward subscription-based models is enabling vendors to offer predictable revenue streams, shielding against economic slowdowns and benefiting partners through recurring revenue opportunities.

MSPs, for instance, are increasingly bundling security with IT services to meet customer demand for integrated solutions. The integration of AI and machine learning is another transformative trend, with vendors like Fortinet, CrowdStrike, and Microsoft leveraging these technologies for advanced threat detection and automated responses.

Generative AI is also gaining traction for proactive threat hunting, enhancing efficiency and reducing response times. Cloud security is a high-growth segment, expected to reach USD 85 billion by 2035, as organizations migrate to hybrid and cloud environments. Partnerships like Liquid C2 with Google Cloud underscore this focus.

SMBs represent a significant growth area due to their limited in-house capabilities, creating demand for tailored solutions and compliance support.

Additionally, the market is witnessing increased consolidation through mergers and acquisitions, such as Cisco's USD 28 billion acquisition of Splunk, which expands vendor portfolios but requires partners to adapt to shifting dynamics.

Finally, the proliferation of IoT devices and operational technology is driving demand for specialized security solutions, as seen in partnerships like Capgemini's IoT security offerings.

Opportunities for Channel Partners

Channel partners are well-positioned to capitalize on the cybersecurity market's growth.

The rise of managed security services, outpacing traditional technology deployments, offers MSPs a chance to deliver scalable, cost-effective Security-as-a-Service solutions. SMBs, lacking dedicated security teams, present a lucrative opportunity for partners to provide consulting, implementation, and ongoing management, particularly for compliance with regulations like NIS2.

Offering training and education through workshops and webinars can further enhance partner value, positioning them as trusted advisors while boosting profitability. Strategic partnerships with major vendors, such as IBM with Palo Alto Networks, enable partners to access advanced technologies and expand market reach.

With 91.5% of cybersecurity spending flowing through the channel, opportunities for upselling and cross-selling solutions like identity and access management, endpoint security, and cloud security are abundant, particularly within existing client bases.

Challenges for Channel Partners

Despite the opportunities, channel partners face several challenges. Economic uncertainties and high borrowing costs may constrain customer budgets, requiring partners to demonstrate clear ROI for cybersecurity investments.

The rapidly evolving threat landscape, driven by AI-powered attacks and infostealer malware, demands continuous upskilling, with breakout times post-exploitation averaging just 48 minutes. Vendor consolidation, while expanding solution portfolios, can disrupt partner relationships and necessitate strategic adjustments.

The global cybersecurity talent shortage, with a deficit of 3.5 million professionals, hinders partners' ability to scale services, though acquisitions of boutique firms or partnerships with specialized providers can mitigate this.

Finally, navigating complex regulations like NIS2 adds challenges, particularly for SMB clients, requiring partners to stay informed and provide expert guidance.

Competitive Landscape

The cybersecurity market is led by major vendors like Palo Alto Networks, Microsoft, Cisco, Fortinet, and CrowdStrike, which dominate through comprehensive solutions.

Emerging players like Zscaler and Okta are gaining traction in niche areas like cloud and identity security. Market share trends show Palo Alto Networks increasing from 7.8% to 9.6% between 2021 and 2023, with Fortinet and CrowdStrike also gaining ground. Within the partner ecosystem, MSPs are bundling cybersecurity with IT

services, often generating USD 1.34 for every USD 1 of vendor sales in security. VARs and system integrators focus on product selection and implementation, while consultancies like Deloitte provide strategic advisory services to align security with business goals, intensifying competition for the full customer journey.

Strategic Recommendations

To succeed in the cybersecurity market, channel partners should invest in expertise in AI-driven threat detection and cloud security to align with market trends. Targeting SMBs with tailored, cost-effective solutions and compliance support can drive growth, particularly when bundled with training services.

Strengthening relationships with leading vendors like Cisco or Microsoft provides access to advanced solutions and training, while leveraging vendor marketplaces can streamline sales.

Emphasizing subscription-based models and managed services will build predictable revenue streams, and upselling solutions like IAM and cloud security can maximize profitability. To address the talent shortage, partners should consider acquiring boutique firms or forming strategic partnerships.

Finally, offering regular customer education through workshops and webinars will reinforce partners' positions as trusted advisors, fostering long-term relationships.

Conclusion

The cybersecurity sector offers significant opportunities for channel partners in 2025, driven by rising threats, digital transformation, and regulatory pressures. With over 90% of cybersecurity spending flowing through the channel, partners are critical to market growth. By leveraging managed services, targeting SMBs, and aligning with key vendors, partners can capitalize on this dynamic market.

However, challenges like economic uncertainties, evolving threats, and talent shortages require strategic adaptation. Through investments in expertise, customer education, and

recurring revenue models, channel partners can thrive in this rapidly expanding landscape.