Publication date:
2 May 2024
Author:
Andrew Braunberg

Automation: A critical capability for a proactive security strategy

Adopting proactive security strategies to reduce risk

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Syxsense

Contents

Summary	2
Introduction	2
Adoption of proactive solutions as a strategic security strategy	2
Foundational capabilities	4
Moving to platforms	6
Measuring success	7
Moving forward	7
Final thoughts	7
Appendix	9

Summary

Organizations are increasingly turning to proactive security solutions to provide a modern foundation for their operational cyber-risk management strategies and to validate and optimize how existing security solutions address key security controls.

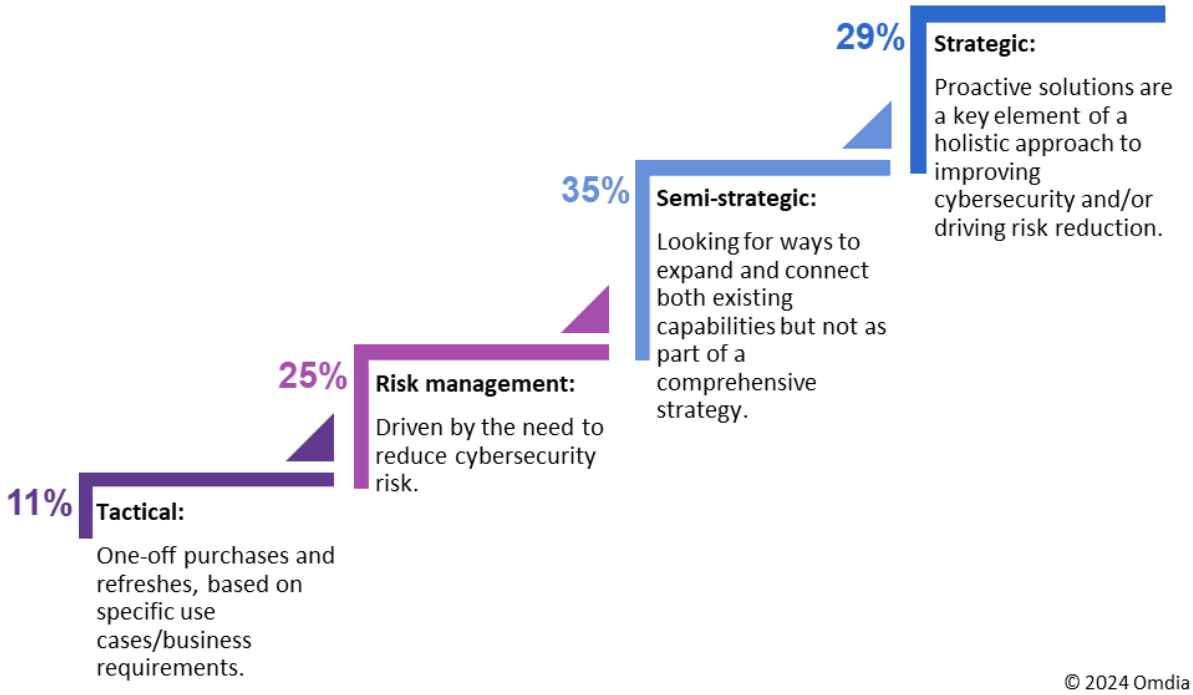
Introduction

In the first quarter of 2024, Omdia surveyed more than 400 security decision makers in North America, the UK, France, and Germany. The survey was designed to better understand the current and future use of proactive security solutions, and to determine current drivers and inhibitors to market evolution and growth. The research makes clear that organizations of all sizes and in all geographies are embracing proactive security solutions. More than 70% of respondents have increased spending on proactive security solutions versus a year ago, clearly outpacing spending on preventative and reactive solutions. Proactive security solutions are seen as fostering a comprehensive understanding of the threat landscape and attack surface. As this segment further matures, organizations strongly expect a broader integration of proactive security tools that will further improve attack surface management and security control optimization. A sizable minority of organizations are already deploying proactive security solutions strategically, with larger and more "mature" security organizations leading the way.

Adoption of proactive solutions as a strategic security strategy

The research shows that proactive security solutions are quickly taking hold in the enterprise and solving unique and critical cybersecurity problems. Most importantly, organizations are using these solutions to not only enable visibility and management of their entire attack surface, but also to optimize protections through the existing security stack. Many proactive security product segments are seeing broad adoption in 2024, and Omdia research shows that organizations are often making these proactive investments as part of broader risk reduction strategies.

Figure 1: Which of the following best describes your organization's current approach to deploying proactive security solutions?



Source: Omdia

As seen in **Figure 1**, 29% of organizations are already deploying proactive security solutions as a key component of broader cyber-risk reduction strategies, and most organizations (64%) are deploying proactive security solutions with an integration strategy in mind (i.e., strategically or semi-strategically). Omdia also asked respondents a more general question regarding their organization's "approach to cybersecurity risk governance and risk management" as a means of assessing overall security maturity. Organizations that self-reported a higher level of security maturity were more likely to approach proactive security investments strategically. For example, 60% of respondents who self-reported the highest level of general security maturity are taking a strategic approach to deploying proactive solutions, compared to only 29% among all respondents.

Not surprisingly, a large percentage (42%) of financial services organizations self-report a high level of general cybersecurity maturity. Correspondingly, they are significantly more likely (44%) to approach proactive security solution deployments as part of a strategic risk reduction program. Healthcare and retail organizations, on the other hand, are much less likely to be at the highest level of security maturity, at 18% and 21%, respectively. They are also less likely to invest in proactive security solutions strategically; in fact, they show a lower-than-average level of adoption across all proactive security segments.

Organizations that claim a high level of security maturity are, in fact, driving the adoption of proactive security tools. More than a third of these organizations plan to increase year-over-year spending on proactive solutions by 15% or more, compared to a quarter of respondents overall.

That said, 71% of all respondents are increasing proactive spending at some level. However, there is considerable differentiation in spending trends by industry. For example, 86% of all financial services organizations are increasing year-over-year spending in that category. Respondents in typically less mature industries, such as healthcare and retail, are less likely to be increasing year-over-year spending on proactive security solutions.

Foundational capabilities

There is a strong market desire for proactive security capabilities to continue to consolidate into more integrated solutions or platforms. Omdia research indicates that organizations expect more consolidated solutions to alleviate two immediate pain points more effectively:

- **61%** of all respondents rated the ability to view risks through different attack frameworks/risk lenses (e.g., MITRE ATT&CK, Threat Intel) as critically important. This capability was more important in North America (65%) than EMEA (57%).

- **60%** of all respondents rated full External (e.g., attack surface visibility, attack path mapping, security control validation) asset context as critically important. This capability is particularly important to the most security-mature organizations, 69% of which rated it critical.

Enabling these capabilities requires a full and dynamic understanding of the threat landscape and threat actors, as well as an ability to prioritize (and act on) exposures based on risk.

Proactive security technology is evolving rapidly as functionality in traditionally distinct products increasingly overlaps. For example, attack surface management, vulnerability management, and security posture management are often now discussed under the broader category of exposure management. Vulnerability management is perhaps the most mature proactive security segment, but it is a segment that has seen a large degree of innovation and evolution over the last several years. Vendors have been particularly active in the key areas of prioritization, orchestration, and automation.

Modern vulnerability management solutions, which Omdia refers to as risk-based vulnerability management, need to support persistent observability across the attack surface, enable risk-based vulnerability prioritization, and include an orchestration engine that can begin to automate patching and remediation. And while traditional patching remains a core requirement, patching is only half the story. Organizations need to patch as well as remediate a broader set of exposures.

Overwhelmingly, organizations want proactive security solutions to be actionable. For example, 79% of respondents view automated vulnerability remediation capabilities as important or mission critical. That means having a full view of operational cyber-risk and being able to remediate that risk. For that reason, Omdia believes it is critical that proactive security solutions either directly facilitate risk reduction activities, or tightly integrate with a broad set of third-party preventative and reactive

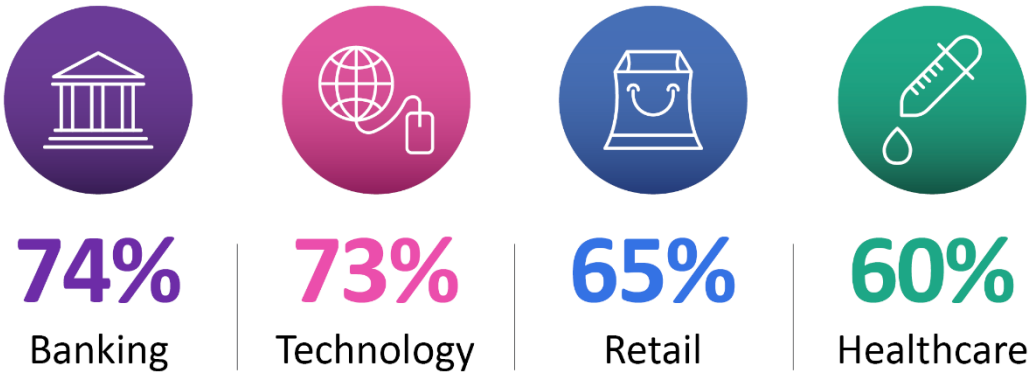
security solutions to, in turn, foster risk reduction. Integration of proactive security solutions with the existing security fabric, particularly the reactive tool suite, is also an important requirement.

However, proactive security solutions will not deliver their full potential without strong security automation capabilities. Overall, 79% of respondents view automated vulnerability remediation capabilities as important or mission critical. This support holds relatively steady across company size, security maturity, and key industries.

The strong demand for security automation from the most security-mature organizations suggests that adopting automation to achieve proactive security is a best practice of leading organizations. Of all respondents, 61% percent believe that automation is foundationally critical to achieving proactive security. This includes 69% of organizations with over $1bn in revenue and 77% of organizations with the highest security maturity.

As can be seen in **Figure 2**, there is higher demand for security automation capabilities in proactive solutions among organizations in industries with a higher level of security maturity. Less mature and smaller organizations are less likely to view automation as "foundationally critical," but Omdia research suggests that rather than not seeing the value of automation, these organizations often feel that automation is simply out of reach.

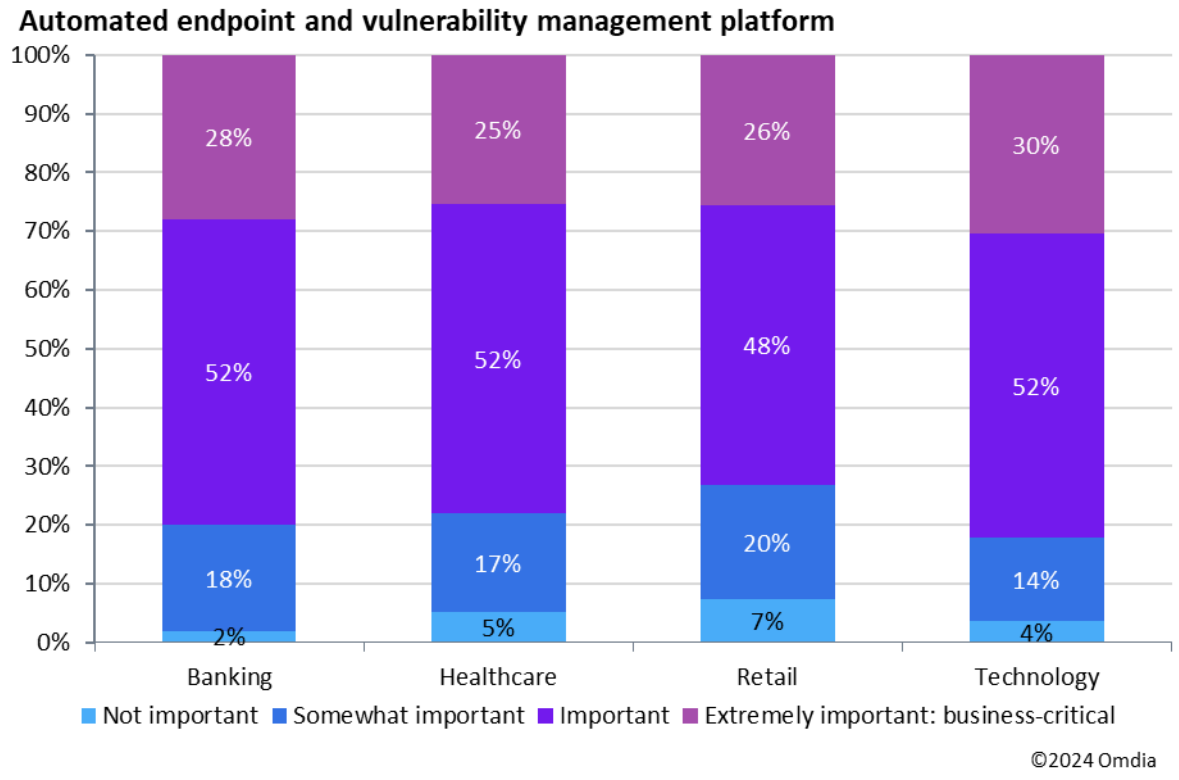
Figure 2: Automation is critical in proactive security solutions



Moving to platforms

Omdia expects that proactive security solutions will consolidate further in response to strong end-user demand for proactive security platforms. Organizations with high maturity levels, a group that has been an early adopter of proactive security tools, are particularly supportive of this consolidation trend. For example, the most security-mature organizations find an automated endpoint and vulnerability management platform significantly more attractive than less mature organizations. That said, there is consistent support for automated endpoint and vulnerability management platforms, with 77% of all respondents reporting that these platforms are important or business-critical.

Figure 3: Importance of consolidated endpoint and vulnerability management capabilities, by key industries



Source: Omdia

Omdia research found that automated network infrastructure and vulnerability management platforms are also strongly supported. Of all respondents, 65% report that such platforms are important or business-critical. This support is relatively consistent across industries and by company size. Again, however, the most security-mature organizations are much more likely to view these

platforms as business critical (31% compared to 15%), and 80% of the most security-mature respondents see these platforms as important or critical.

Measuring success

The proactive security era is in its early days, and organizations typically frame success around the standard metrics of improved remediation or mitigation rates when evaluating these tools. Proactive security platforms that can deliver better orchestration and automation will further support these success measures. Omdia believes that stronger automated remediation could significantly affect or reduce the traditional mean-time-to-respond metric and have a positive downward pressure on other security stats.

More generally, organizations believe that success is about aligning shared objectives across IT operations and security operations teams. Respondents strongly believe that these groups should report to the same executive leader (50% of all respondents) or, at a minimum, share common objectives and key performance indicators (KPIs) (33%). This is a significant finding because respondents also show a high level of concern regarding expected disruption to organizational structure resulting from a broader adoption of proactive solutions. Adopting proactive tools will likely be the easiest part of the transition to a proactive strategy, while implementing organizational change will be the higher hurdle to full implementation.

Moving forward

To fully exploit the potential of a proactive strategy, organizations will need to maintain a comprehensive and dynamic view of their entire attack surface, and historically, this has been a difficult problem to solve. However, increasingly, automation can be employed to facilitate many of the tasks associated with this goal. Not surprisingly, 82% of the most mature organizations think automated vulnerability remediation capabilities are important or extremely important. Organizations should ensure that proactive security solutions embrace security orchestration and automation, particularly for patch scanning, patch deployment, vulnerability scanning, and vulnerability remediation.

Omdia expects the adoption of proactive security solutions to increasingly be seen as a best practice that will further drive the view that security operations are a strategic enabler of broader operational risk reduction. Security leaders will increasingly need to communicate risk metrics in a way that is understandable within and beyond security teams. This will require agreement on the level of visibility required to fully understand operational cyber-risk across the enterprise as well as the appropriate measures for assessing and communicating that risk.

Final thoughts

Cybersecurity products and services can be broadly classified depending on how they approach the problem of keeping data and infrastructure safe from attackers. Omdia splits the entire universe of security solutions into three categories:

- Preventative products and services add layers of security (traditionally referred to as “defense in depth”) that compensate for weaknesses and exposures in the people, processes, and technology that comprise digital infrastructure.

- Reactive solutions search for indicators of compromise that are used to determine where preventative solutions failed, or were bypassed, and quickly determine how to shut down and remediate attacks.

- Proactive security solutions, however, search for indicators of exposure and recommend and perform actions to eliminate or mitigate those exposures before they are exploited. Omdia includes the following solutions within the proactive category: attack surface management, risk-based vulnerability management, security posture management, incident simulation and testing, penetration testing, and red teaming, among others.

One of the benefits of categorizing the solution market based on these three categories is that it broadly aligns with the evolution of cybersecurity. When the digital age dawned, it was thought that preventive products would ward off all bad actors. And while preventive solutions continue to be deployed broadly and serve an important purpose, they are not sufficient alone. Then came the era of assuming breaches and building security operations centers (SOCs), with the focus shifting to the deployment of reactive solutions. While threat detection, investigation, and response (TDIR) solutions are still needed, the limits of these reactive approaches to security are clear: finding and remediating critical threats at scale is costly, complex, and prone to frequent failure. Now, Omdia believes the industry is entering a new era that emphasizes proactive security solutions. Preventative and reactive solutions will not disappear, but organizations are shuffling their spending priorities and looking for the better return on investment that proactive security solutions promise to deliver.

Appendix

Methodology

While the cybersecurity industry has clung to the 'assume breach' mantra with its preventative and reactive solutions, organizations are awakening to a smarter strategy: proactively understanding attack surfaces, mapping attack paths, and plugging vulnerabilities to prevent breaches. While a host of standalone proactive tools have been available for many years, Proactive Security Platforms are emerging that can provide much more holistic risk discovery, prioritization, and automated remediation.

In Q1 2024, Omdia fielded a custom survey to 405 global security decision makers to better understand the current market landscape and approaches, investment trends and preferences, attitudes towards risk management and organizational pain points associated with Proactive Security. Respondents included decision makers from North America and EMEA, at SMB+ sized companies across a variety of industries. Respondents included individuals from Manager level through C-level positions, who have responsibility for cybersecurity product investment decisions.

Author

Andrew Braunberg
Principal Analyst, Security Operations
andrew.braunberg@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Syxsense
3090 Bristol St. | Ste 400
Costa Mesa | CA 92626 | USA
+1 (949) 270-1903
+44 (0) 1256 806567
info@syxsense.com
www.syxsense.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 Tech, a B2B 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.

Copyright notice and disclaimer