OMDIA

Brought to you by Informa Tech

A CISO’s Primer for Strategic Cybersecurity Risk Reduction with Attack Surface Management (ASM)

Understanding ASM in the context of Continuous Security Protection

Table of Contents

Omdia's View

Omdia sees the emergence of a new paradigm for security architectures called Continuous Security Protection.

Proactive security solutions, a key element of Continuous Security Protection, seek out and mitigate likely threats and threat conditions across the attack surface before they become realized risks or breaches.

Identifying, assessing, and reducing the attack surface circumvents threat opportunities, reducing risk and delivering ROI.

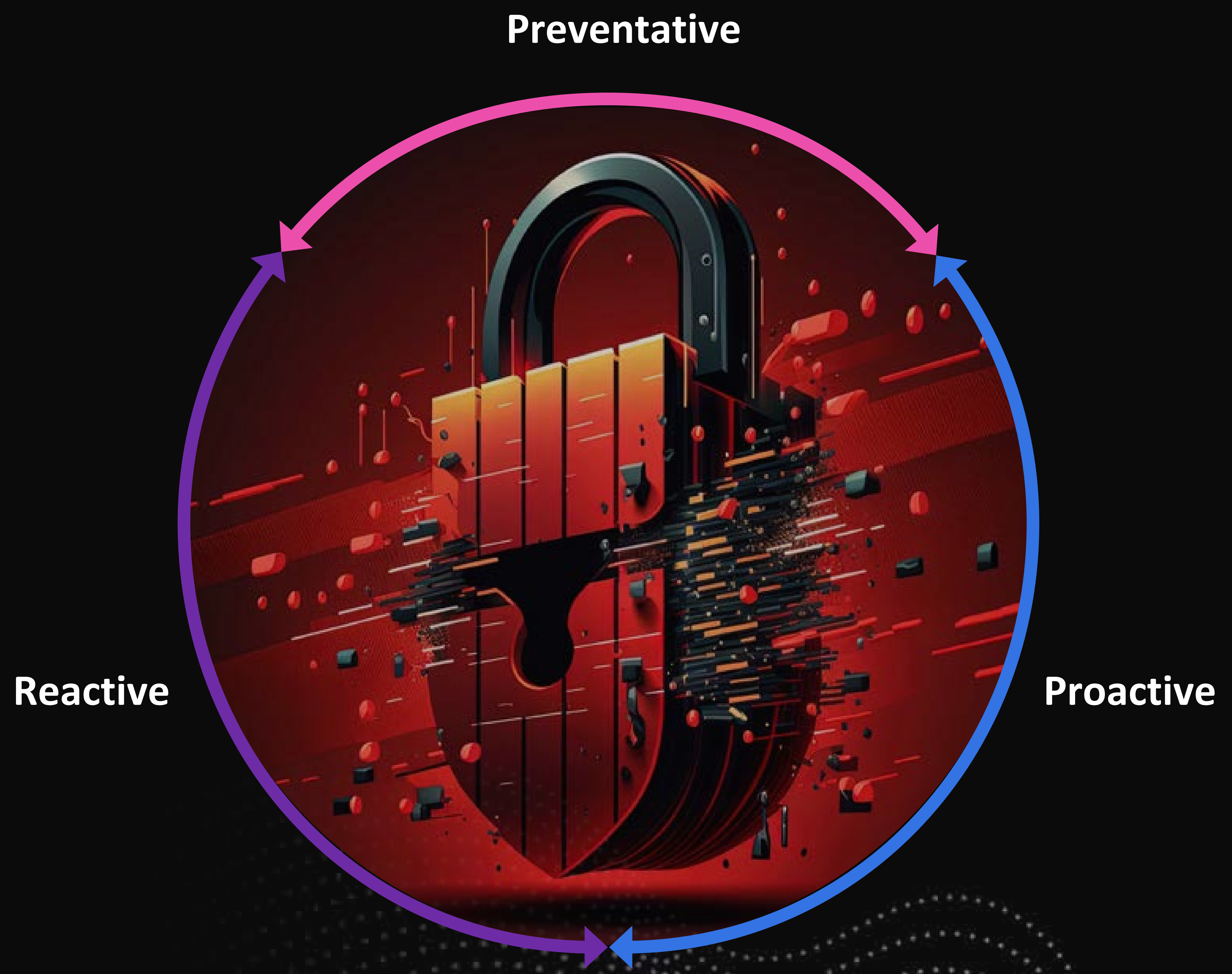
Platforms that combine proactive security with threat detection investigation and response (TDIR) advance the implementation of Continuous Security Protection.

PREVIOUS NEXT

Understanding Continuous Security Protection

Omdia defines Continuous Security Protection as cybersecurity strategy that ensures an organization can remain resilient and adaptive to the needs of its stakeholders, employees, and customers.

From a technology perspective, this means not only investing in technology to address active threats, but also to reduce the attack surface before threats materialize.

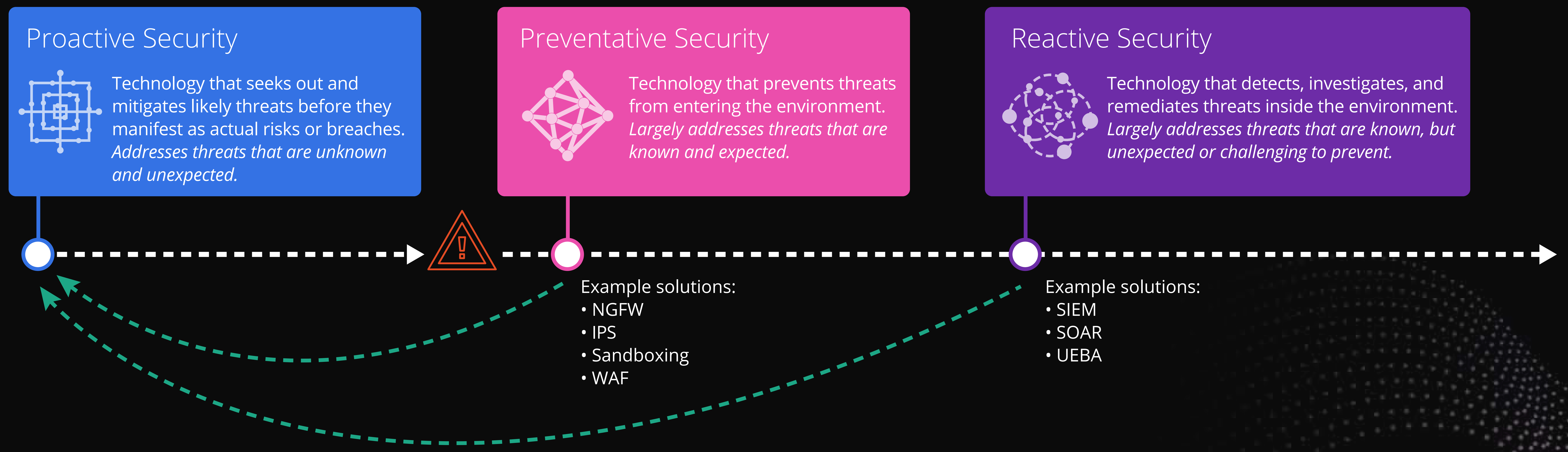


OMDIA

Omdia Continuous Security Protection Lifecycle

Traditional preventative and reactive solutions remain essential but are primarily effective at addressing threats only after they are active and targeting the environment.

Proactive security solutions operationalize processes that eliminate opportunities for threats before they strike.



Proactive Security

Technology that seeks out and mitigates likely threats before they manifest as actual risks or breaches. *Addresses threats that are unknown and unexpected.*

Preventative Security

Technology that prevents threats from entering the environment. *Largely addresses threats that are known and expected.*

Example solutions:

- NGFW
- IPS
- Sandboxing
- WAF

Reactive Security

Technology that detects, investigates, and remediates threats inside the environment. *Largely addresses threats that are known, but unexpected or challenging to prevent.*

Example solutions:

- SIEM
- SOAR
- UEBA

Source: Omdia

Improving Risk Prioritization

The Emergence of Continuous Security Protection Highlights the Importance of Attack Surface Management

Having full and continuous visibility into all externally facing assets is particularly important as Internet facing assets are often used as initial point of access into a network. A full inventory of these assets can assist in attack path validation, and threat hunting.

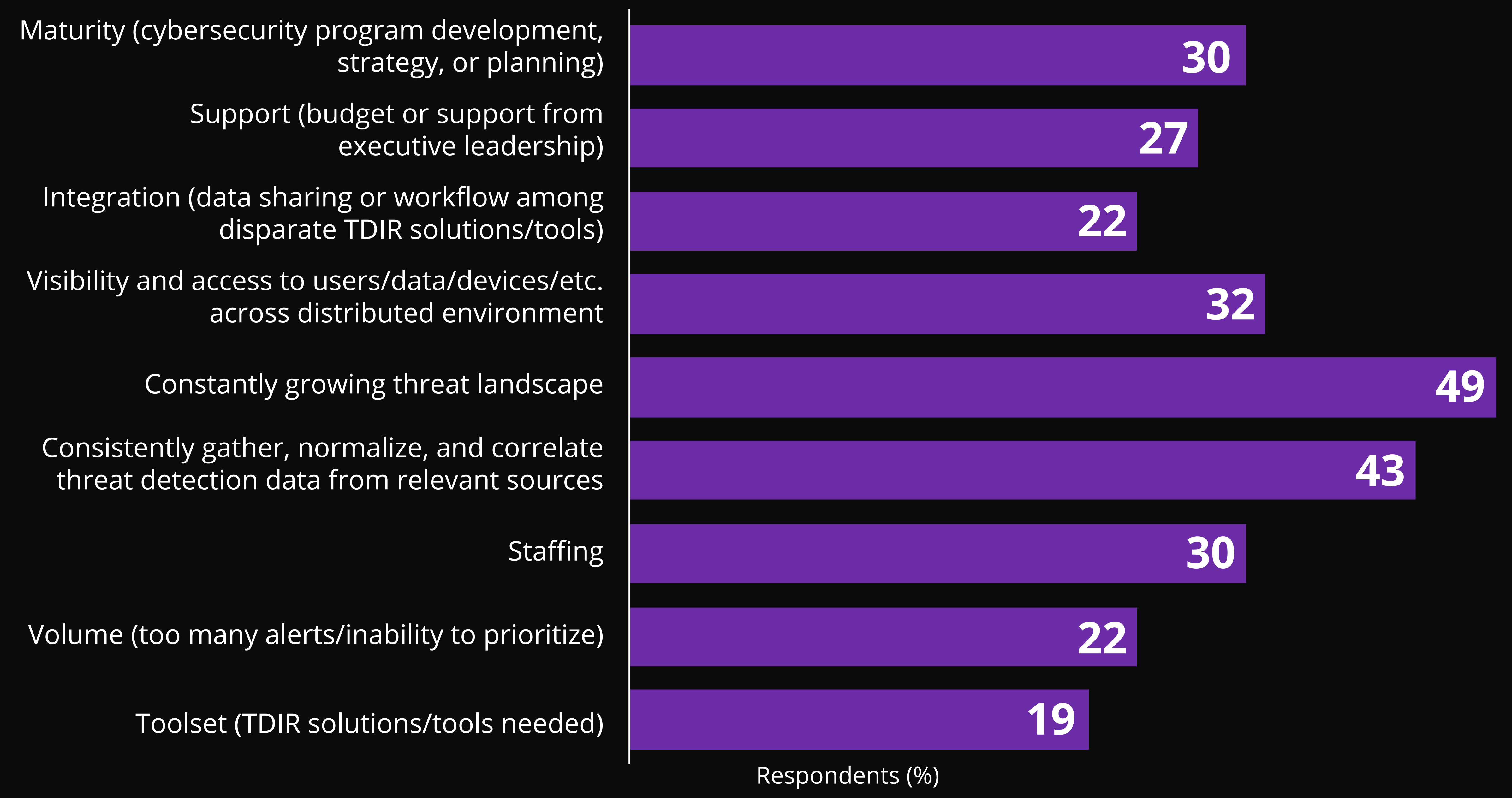
Because Internet-facing assets are particularly attractive targets, attackers often perform their own version of External Attack Surface Management (EASM) as an early step in their attack chain. These tools are very effective, and they regularly discover unknown, externally facing assets within all types of organizations.

When combined with risk analytics, ASM can improve remediation recommendations as well. A key benefit of overlaying risk analytic capabilities on top of traditional reactive and proactive solutions is the ability to better assess and contextualize cyber risk and prioritize remedial action. An integrated platform approach can enhance these insights by bringing all of these capabilities together holistically.

A key benefit of adding risk management features to reactive and proactive solutions is the ability to better assess cyber risk and prioritize remedial action. An integrated platform approach can enhance these insights.

The Dynamic Threat Landscape Leaves Organizations of All Sizes Struggling with the Scale of the Attack Surface

What are the top challenges to your organization's cybersecurity threat detection, investigation, and response (TDIR) capability?



Source: Omdia

© 2023 Omdia

Omdia research shows that the top TDIR challenge for enterprises is keeping up with the ever-growing threat landscape.

For large enterprises, these problems are especially pronounced: 58% of organizations with more than 10,000 employees consider the growing threat landscape a top concern, compared to 51% of organizations with from 5,000 to 10,000 employees, and just 44% of organizations with under 5,000 employees.

All organizations, large ones especially, must have a technology strategy for managing the attack surface, amid a threat landscape that grows increasingly diverse and challenging.

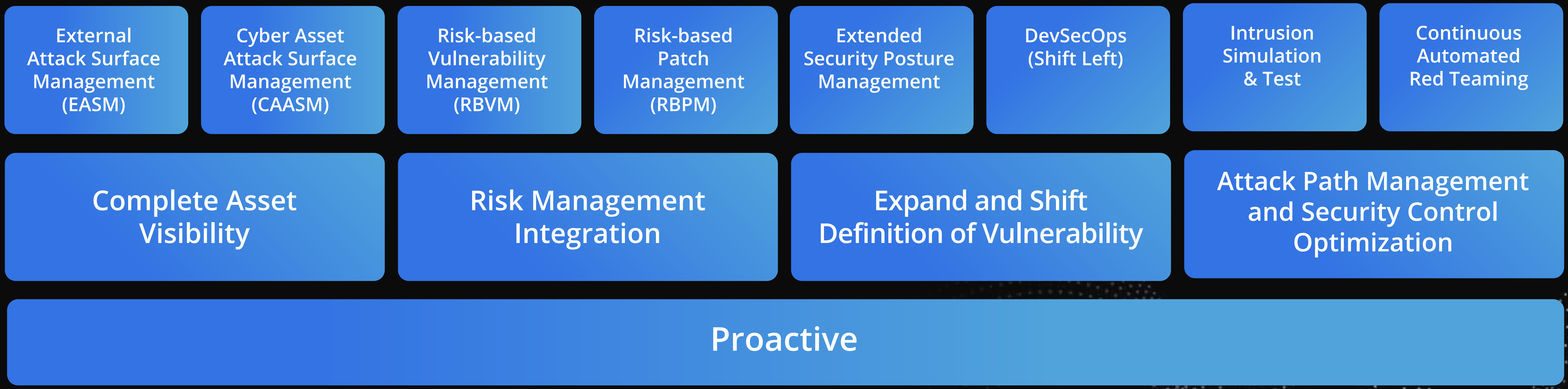
PREVIOUS NEXT

OMDIA

Popularity of Proactive Security Grows to Augment Existing Investments and Strategies

Over the last several years, Omdia has identified a growing trend towards a more proactive approach to security as organizations strive to find and fix issues before threat actors have an opportunity to exploit them. This includes proactively reducing the attack surface and thereby mitigating the opportunity for successful attacks.

Proactive Security Controls



External Attack Surface Management (EASM)

Cyber Asset Attack Surface Management (CAASM)

Risk-based Vulnerability Management (RBVM)

Risk-based Patch Management (RBPM)

Extended Security Posture Management

DevSecOps (Shift Left)

Intrusion Simulation & Test

Continuous Automated Red Teaming

Complete Asset Visibility

Risk Management Integration

Expand and Shift Definition of Vulnerability

Attack Path Management and Security Control Optimization

Proactive

Source: Omdia

PREVIOUS

NEXT

Enabling Optimized Risk Reduction

Visibility across the extended IT estate is critical to understanding and reducing risk

Telemetry comes from many sources: Posture management, DevSecOps, VM/RBVM, endpoint and network sensors, and more

But security teams are challenged to consolidate all that data and put it in context, never mind use it to assess, prioritize, and respond

The next step, and what is missing from today's solutions, is actioning that visibility to ask,

> ***What risk insights does the visibility offer?***

> ***What actions should be taken based on that risk?***

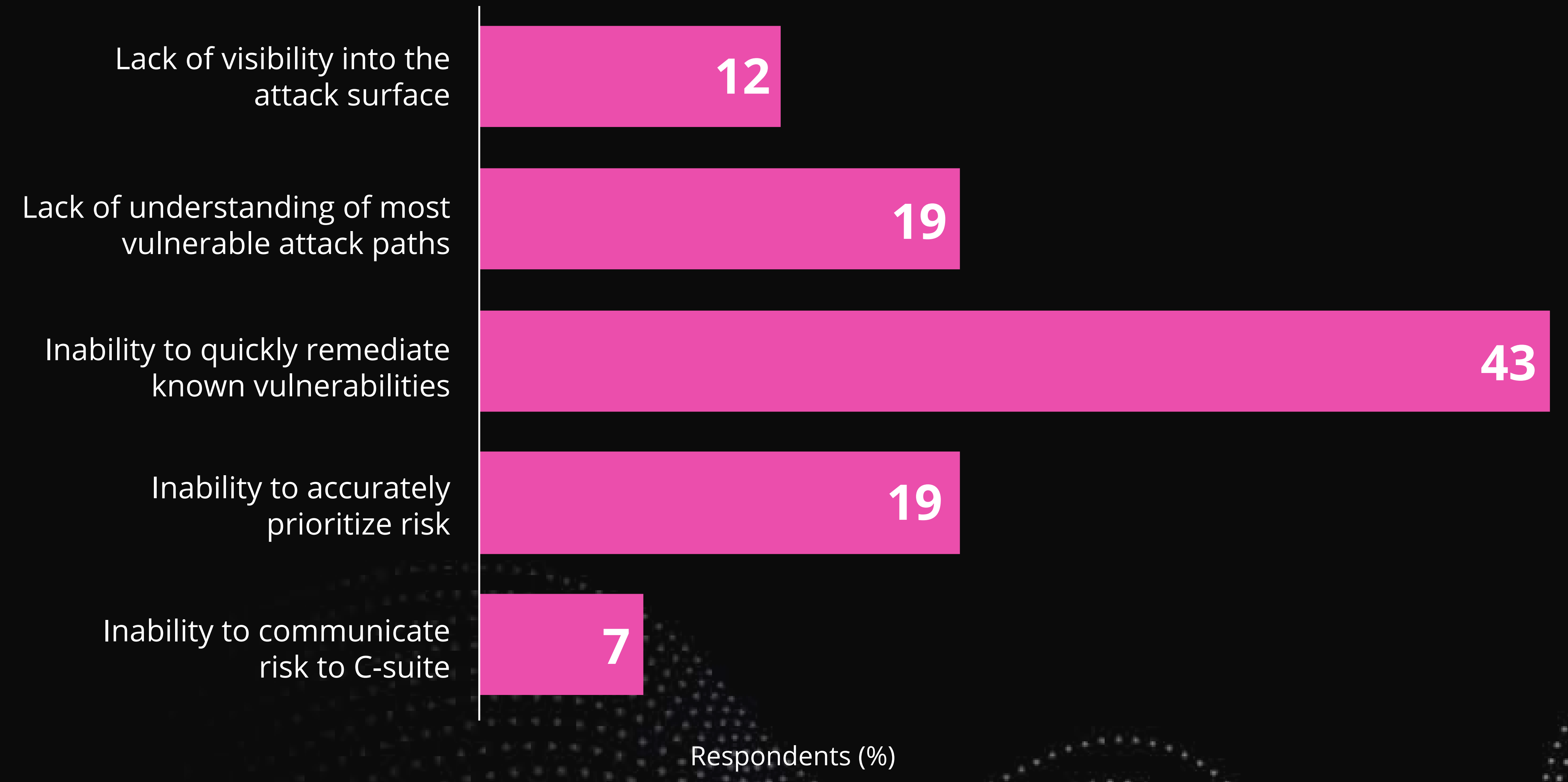
Full Visibility of Exposed Assets Enables Better Risk Prioritization

While Omdia research shows the most pressing cyber risk management problem related to Threat Detection Investigation and Response (TDIR) is the constantly growing threat landscape, the most pressing problem associated with proactive risk management is an inability to quickly remediate known vulnerabilities (43%).

According to FIRST (Forum of Incident Response and Security Teams), past research indicates that firms are only able to fix between 5% and 20% of known vulnerabilities per month.

Visibility into the attack surface is becoming a better-understood problem. Externally exposed assets can be particularly vulnerable and can provide attackers with an initial foothold into a network.

What is the most pressing cyber risk management problem related to proactive risk management?



Source: Omdia

PREVIOUS ⌂ NEXT

Effective Risk Reduction Requires a Holistic View of the Entire Attack Surface

CISOs must rethink the definition of attack surface.

Today’s widened aperture must not only include vulnerabilities, but also misconfigurations, bad credentials, open APIs, badly implemented SaaS apps, shadow accounts, policy management, and even human risks.

Remediation recommendations should consider existing security controls and attack paths, as well as the active threat environment.

To create an accurate risk score to consistently define and weigh risk, organizations need a dynamic understanding of the current threat landscape as well as the risk posed by their attack surface posture, weighted with organizational context such as existence and effectiveness of existing controls.

This process should highlight opportunities to take action on unmitigated risk, supported by risk data.

- Software Vulnerabilities
- Misconfigured System Components
- Weak Credentials
- Weak Encryption
- Inadequate Authentication
- Sensitive Data Exposure
- Shared Tenancy Vulnerabilities
- CWE Flaws

PREVIOUS ⌂ NEXT

OMDIA

Enabling Strategic Risk Reduction

The primary team for managing and mitigating cyber risk varies significantly by company size. While SOC analysts play a large role in any organization that has a SOC team, for the largest organizations (10k employees or more) a dedicated risk management team is more commonly involved, while for smaller organization (5k employees or smaller) general cyber security teams are more common. According to recent Omdia research:

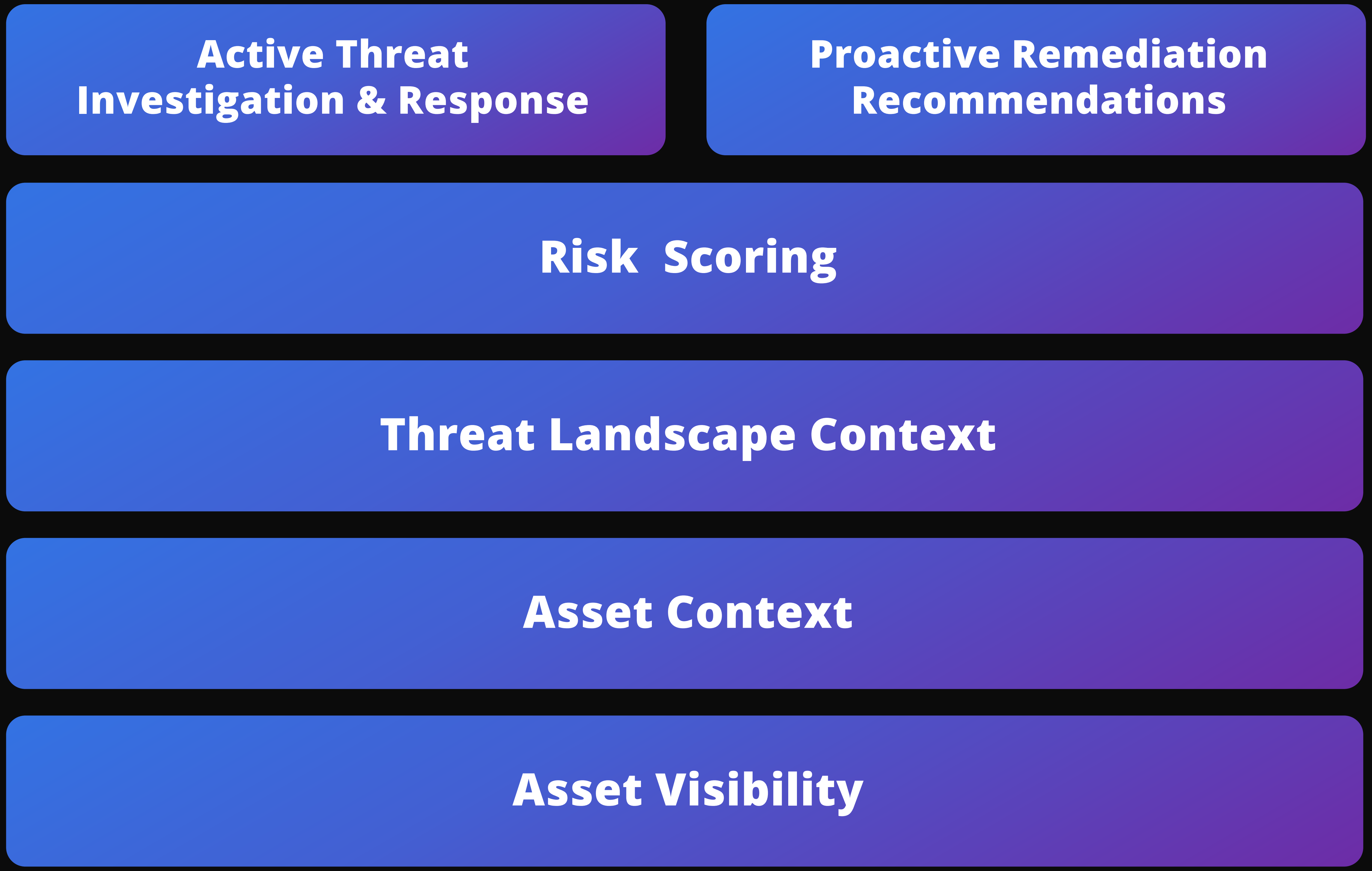
60% of large Enterprises (10k+) have moved to dedicated cybersecurity risk management teams. That number jumps to 76% for managing risk proactively.

On the other hand, 64% of organizations with under 5,000 employees rely on generalist cybersecurity personnel for addressing cyber risk. (That number drops to 56% for proactive risk.)

Respondents based in Europe were significantly less likely to involve general security teams with proactive risk decisions, relying more heavily on SOC teams.

Reactive and proactive security tools need to address the needs of a broad set of users with varying skill sets and primary use cases.

Integrating Proactive and Reactive Functionality


Active Threat Investigation & Response
Proactive Remediation Recommendations
Risk Scoring
Threat Landscape Context
Asset Context
Asset Visibility

ASM technology is considered a key component of broader proactive suites (or platforms) today.

ASM is also increasingly critical to a combined proactive and reactive strategy. The visibility provided by ASM supports threat detection, and further enables risk based prioritization during investigation and response.

Leading detection and response suites are incorporating ASM, particularly EASM, and Omdia research shows strong demand for this integration. Full visibility into exposed assets is foundational to risk assessment, regardless of whether it is pre- or post breach.

PREVIOUS NEXT

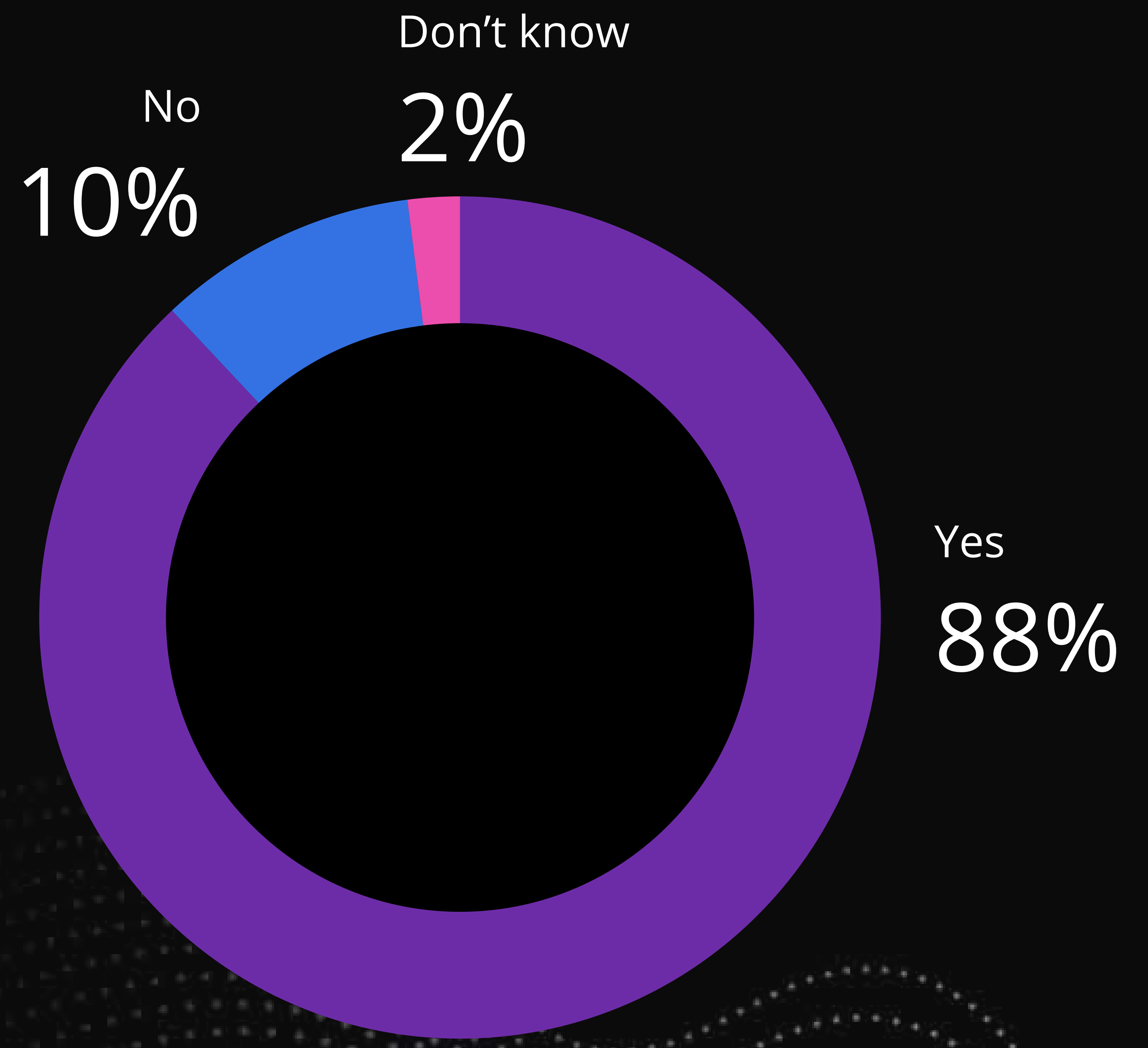
Same Swing, Different Clubs

Comprehensive attack surface management from a SecOps standpoint combines both Proactive and Reactive capabilities.

Omdia research shows strong support (88%) for replacing existing threat detection, investigation, and response (TDIR) point solutions with a single platform that integrates proactive and reactive components.

An obvious avenue for this integration would be adding attack surface management into an Extended Detection & Response (XDR) suite.

Would your organization consider replacing its existing TDIR solutions with a single platform integrating ASM and XDR?



Source: Omdia

Benefits of Integration

Omdia believes a consolidated solution offers numerous benefits, which span security effectiveness, cost, and usability. Benefits that are viewed as very likely by more than half of respondents include:

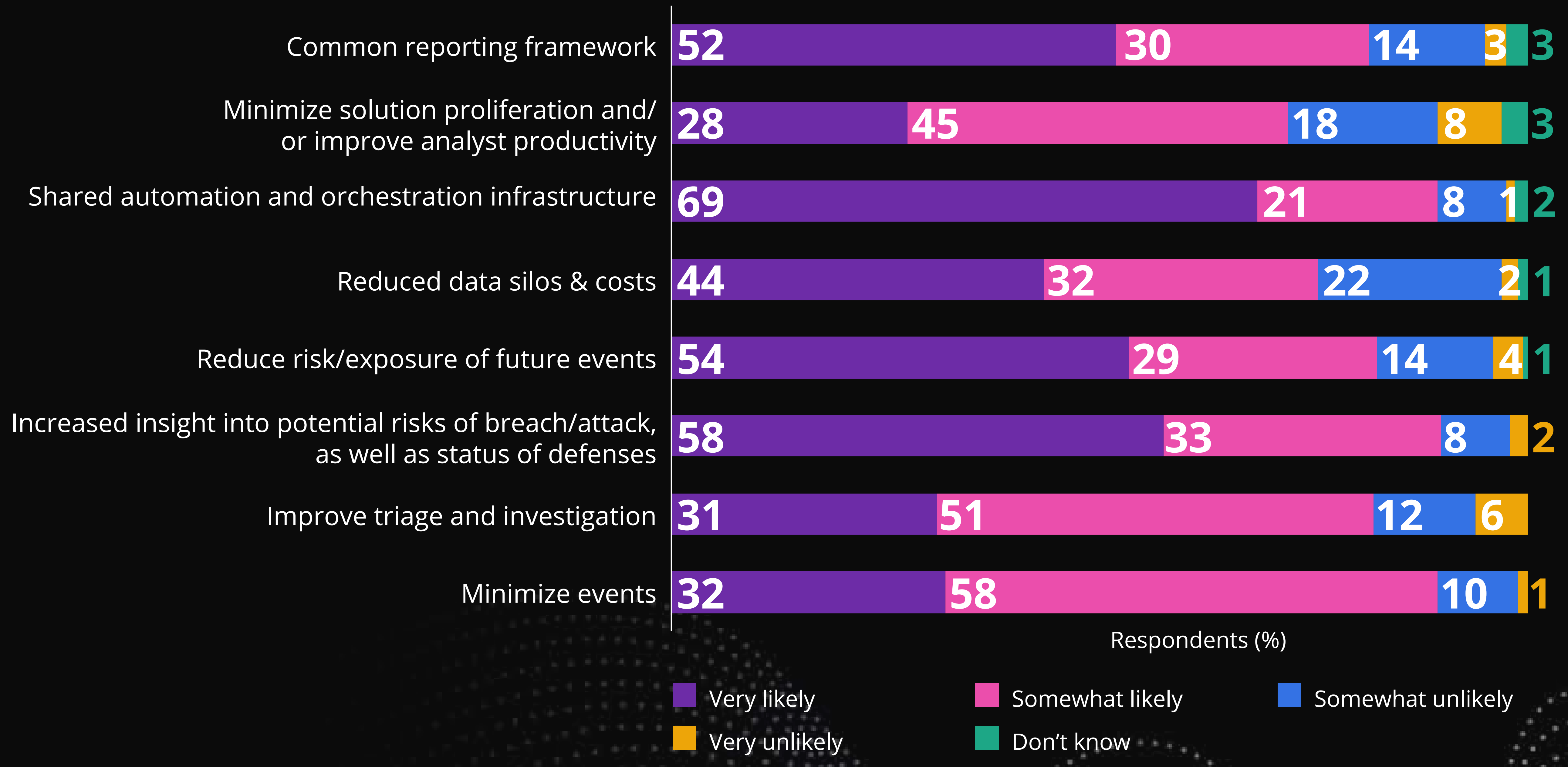
- Increased insight into potential risks of breach/attack, as well as status of defenses.
- Shared automation and orchestration.
- Reducing the risk/exposure from future events.
- Creation of a common reporting framework.

Improved triage and an ability to minimize events is also seen broadly as somewhat likely because of this integration.

A unified ASM-XDR solution also enables cross-functional teams and helps break down organization siloes.

Ultimately, Omdia believes the TDIR lifecycle is more effective when input cycles in from and back to Proactive capabilities, serving to enable Continuous Security Protection.

Which of the following benefits could your organization most likely obtain from an integrated ASM and XDR platform?



Source: Omdia

PREVIOUS ⌂ NEXT

Key Takeaways

- The adoption of proactive security is driven, in part, by a growing desire to optimize security resources by actively avoiding breaches or discovering breaches earlier in the attack chain.
- A comprehensive understanding of an organization's entire attack surface is an enabler of both TDIR and proactive risk-based security.
- Optimizing remedial action through risk-based prioritization a key capability and benefit of proactive security.
- The integration of proactive and reactive capabilities is broadly expected to improve security outcomes and enable shared costs.

OMDIA

Conclusions and Recommendations

The benefits to integrating proactive risk management capabilities with XDR to create a unified platform, including:

- Improved risk insight through integrated threat/detection telemetry.
- Improved efficiencies through shared orchestration and automation.
- Potential cost savings resulting from shared infrastructure.

ASM is a key enabler of Continuous Security Protection, which employs multiple techniques to identify and assess threats and threat conditions across the attack surface before they pose a danger to the environment.

Platforms that combine proactive capabilities with TDIR lifecycle management advance the implementation of Continuous Security Protection.

PREVIOUS

NEXT

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact. The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result. Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials. To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, and agents disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

PREVIOUS