Cybersecurity INSIDERS

2024

Attack Surface Threat Intelligence Report

COGILITY TacitRed

Introduction

Over 80% of cyber breaches result from external threat actors conducting phishing, session hijacking, account takeover, and ransomware attacks, putting organizations under mounting pressure to improve their security posture and automate cyber response. This increase in successful attacks stems from an extended attack surface, vulnerable internet-facing assets and susceptible users, and increased coordination and advancement of cyber-attack methods. Threat Intelligence Management (TIM) and External Attack Surface Management (EASM) are core technologies for security teams to fortify their security posture, increase threat response efficiency, and improve cyber resiliency.

The 2024 Attack Surface Threat Intelligence Report report, produced by Cybersecurity Insiders, the 600,000+ member online community of information security professionals, serves as a foundation to gain insight on the challenges, advantages, maturity, and best practices for applying TIM and EASM to mitigate attack surface risks.

KEY FINDINGS INCLUDE:

- 90% of organizations experienced an increase in impactful attack surface incidents. Smaller organizations had 60% more impactful incidents than larger organizations.
- 84% of respondents reported external attack surface changes contributing to security incidents.
- 33% of organizations have mature external attack surface management programs — nearly half are early stage. Larger companies' programs are twice as mature as smaller organizations, on average.
- 66% of respondents claimed only nominal usefulness of their current threat intelligence tools with the majority (65%) seeking multi-source, curated, and prioritized threat intelligence. Not surprisingly, management found tools 30% more effective than actual operators.
- Over 40% of organizations have challenges with supply chain risk, external asset inventory, and active threat and breach detection effecting attack surface management integrity.
- Over 60% of organizations have attack surface management objectives to accelerate threat identification and response times, and to achieve complete and accurate asset inventory.
- 90% of organizations anticipate a budget increase in attack surface management and threat intelligence tools – 40% expect an increase of over 20%.

We want to thank Cogility TacitRed for supporting this important industry research. We hope you find this report informative and helpful as you continue your efforts to protect your organization against evolving threats.

Thank you,

Holger Schulze

Founder, Cybersecurity Insiders

Most Impactful Attack Vectors

As the external attack surface rapidly expands due to increases in cloud adoption, third-party integrations, hybrid work, and supply chain, understanding the operational and financial impact of external attack surface exposures is essential for prioritizing security initiatives and investments.

The survey reveals malware and ransomware (54%) continue to drain resources, from operational disruption to recovery. Compromised credentials is a close second on the list of attack vectors, with 50% of respondents reporting significant costs tied to validation, remediation efforts, account recovery, and other system-wide security enhancements. Phishing follows closely at 49%, reflecting the burden of detection, user education, and incident response. Supply chain attacks (40%) continue to introduce additional complexity by requiring investments to determine the scope of third-party cyber risk.

Lastly, 36% of respondents highlight the costs associated with targeted technologies, internet-facing assets, and cloud exposures, which demand ongoing security monitoring and threat mitigation across dispersed infrastructure.

Which of the following cyber-attack vectors have impacted expenditures and resource consumption for your organization the most of the past 12 months?

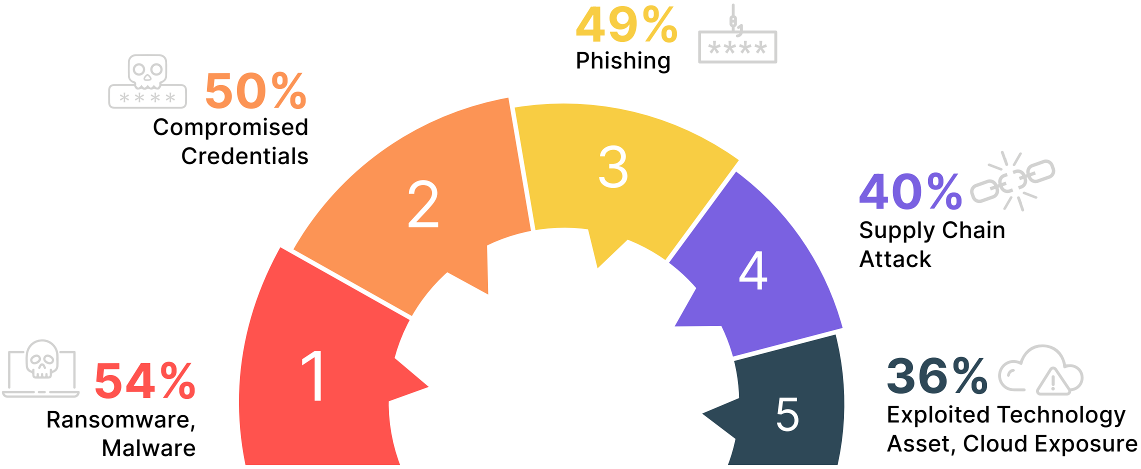


Figure 1. Top 5 most impactful external cyber-attack vectors.

Key Factors Driving External Attack Surface Incidents

The new normal of remote and hybrid work, along with Bring Your Own Device (BYOD) exposures, continues to be among top factors contributing to external attack surface security issues, as cited by 60% of respondents. Remote work has significantly expanded the perimeter, introducing personal devices and home networks into corporate ecosystems, often with insufficient security controls.

The adoption of new technologies (59%), including cloud services and IoT, further complicates security efforts, as organizations struggle to protect a dispersed and growing set of assets. Additionally, 56% point to the expansion of web applications and APIs as attack vectors frequently exploited due to weak authentication or misconfigurations. Supply-chain exposures (34%) continue to present threat actor activity against partner enterprises.

Which factors have contributed the most to threats and attacks with regards to your organization's external attack surface?

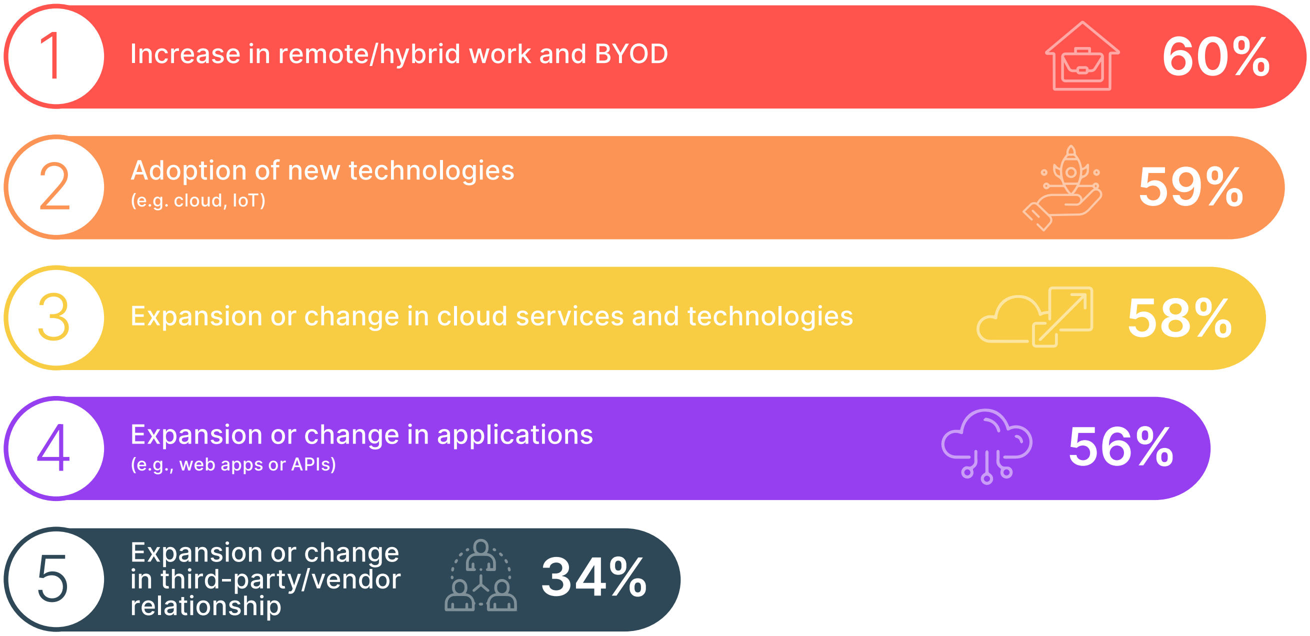


Figure 2. Top 5 factors contributing to external threats and attacks.

Expanding External Attack Surface

As organizations expand their digital footprint through hybrid cloud adoption, new technologies and modern applications, and third-party services, their external attack surface has grown significantly. This survey reveals that 84% of respondents report an increase in their external attack surface activity, with 36% observing a sharp rise in asset changes over the past year. The increased complexity of managing these distributed digital ecosystems compounds the risk, as cybercriminals exploit gaps in security across the cloud, new technologies, supply chains, and external-facing assets.

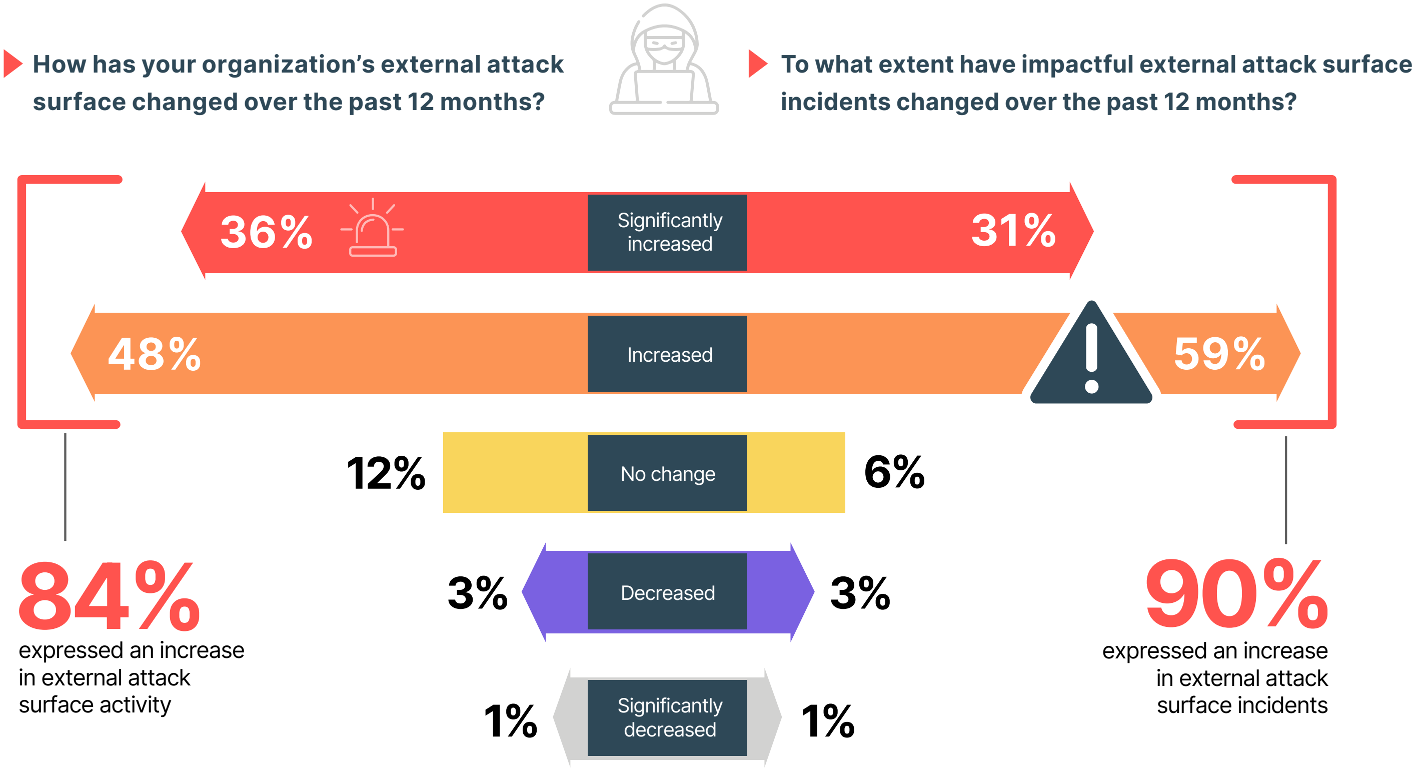


Figure 3. Extent of external attack surface dynamics/change impacting risk and resulting impactful incidents.

This expansion is closely tied to a significant rise in impactful external attack surface management threats. A combined 90% of respondents report an increase in significant incidents, with 31% seeing a substantial rise in attacks and incidents over the past year. The sheer expansion and dynamics of the attack surface has made it more difficult for organizations to manage vulnerabilities, with adversaries exploiting new entry points more aggressively.

Smaller organizations (<2,500 employees) experienced 60% more impactful incidents compared to larger enterprises (>2,500 employees), underscoring the disproportionate risk they face despite having fewer resources. Additionally, technology and financial services sectors reported slightly more impactful incidents than the government sector, reflecting their higher exposure to external threats due to their reliance on a more dynamic and greater connected infrastructure.

Challenges in Managing Attack Surface Risk

Managing the external attack surface presents several challenges, particularly in identifying active third-party exposures, which 45% of respondents cited as their top pain point. As organizations become more dependent on external vendors and partners, the complexity of securing these third-party connections increases, introducing new attack vectors across the supply chain. Additionally, maintaining an accurate inventory of internet-facing assets (41%) has become a significant hurdle. The sheer scale of digital assets across cloud services, applications, and remote work environments makes it difficult for security teams to maintain up-to-date visibility.

Detecting active external actor-engaged threats and breaches (40%) demonstrates the burden and volume of potential security threats, violations, and issues that SecOps teams must filter, validate, and respond to. Filtering through all the threat noise, highlighted by 39% of respondents, remains a key challenge as security teams struggle with excessive data, alerts, and false positives.

What external attack surface management challenges have increased for your organization over the past 12 months?

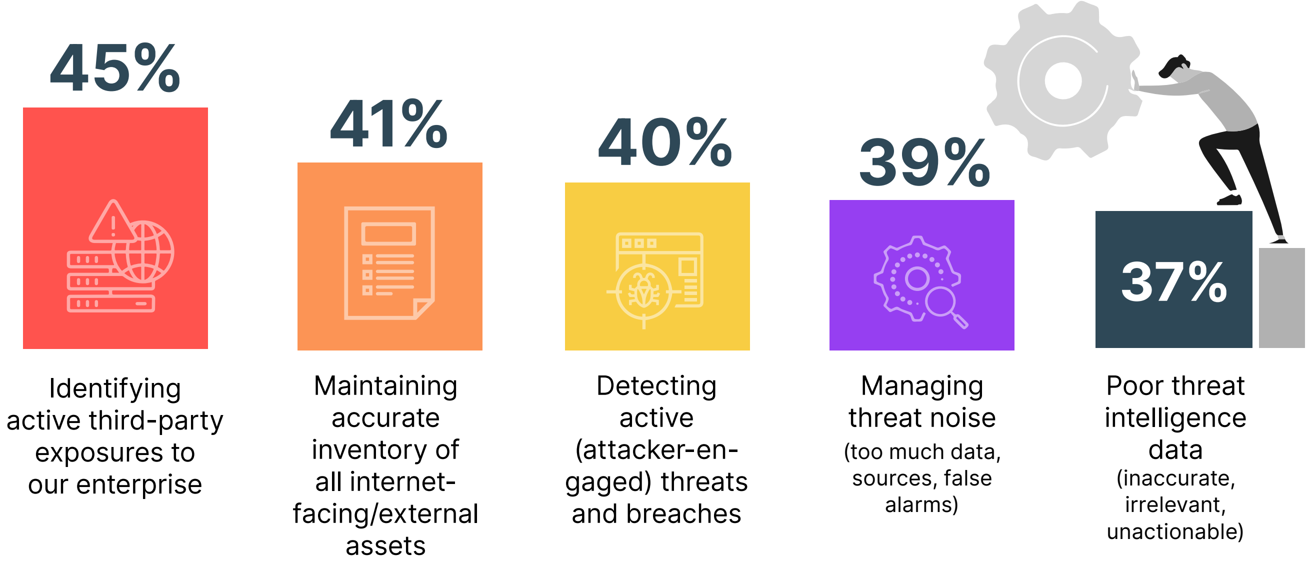


Figure 4. Top 5 external attack surface management challenges.

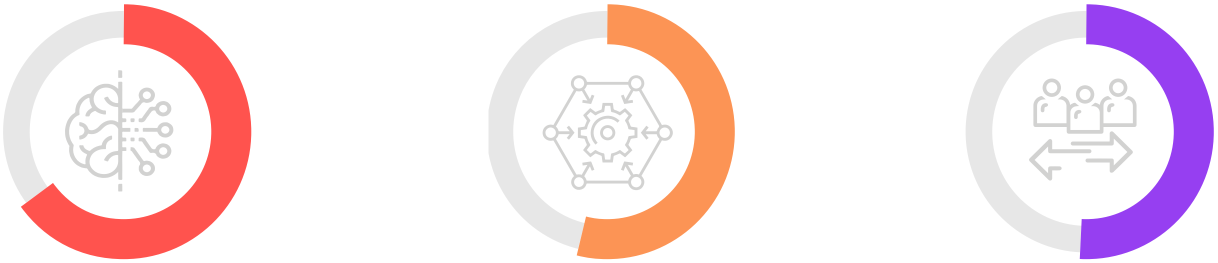
An overload of irrelevant and inaccurate information not only contributes to analyst workload problems and burnout, but can also lead to missed detections and delayed responses to genuine security issues. Compounding external attack surface management obstacles, 37% of respondents cited difficulties with poor-quality threat intelligence, where data is often inaccurate or unactionable, further hampering the ability to respond efficiently to security incidents.

Most Useful Threat Intelligence Sources

In the face of growing external attack surface security issues, organizations rely heavily on threat intelligence to inform their defense strategies and attack response. The survey results indicate a clear preference for multi-source, curated, and prioritized threat intelligence, with 65% of respondents finding it the most useful. This underscores the importance of intelligence that is not merely aggregated or relatively comprehensive, but validated, correlated, refined, and actionable—enabling security teams to focus on the most critical threats and with information to expedite mitigation efforts. This attack surface threat intelligence greatly reduces the burden on security teams to identify, triage, and respond to active exposures – also helping to reduce analyst's efforts to manage through extraneous threat intelligence noise and data overload.

Half of respondents (54%) are using aggregation platforms that organize multiple intelligence sources, from vulnerability alerts to dark web sources. These popular platforms attempt to bring vast amounts of threat intelligence and data feeds into searchable a context, although they may not have as much perceived operational value as per the findings expressed earlier. Additionally, community and industry exchanges, such as ISACs and sector-specific sharing groups, also have value to half of organizations (51%). These exchanges provide sector-relevant intelligence, fostering collaboration across industry peers to address shared threats.

What types of threat intelligence sources does your organization find most useful?



65%
Multi-source, curated, prioritized threat intelligence

54%
Aggregation platform provider
(e.g., consolidate and analyze multiple threat intelligence sources)

51%
Community/industry exchanges
(e.g., ISACs, sector-specific sharing groups)

Figure 5. Most useful threat intelligence sources.

Notably, open-source and government intelligence sources are perceived as lower value, with less than 30% of respondents citing these as useful. This suggests a growing preference for intelligence that is more actionable, curated, and relevant to an organization, rather than the broad, often uncontextualized data from open-source or governmental sources.

To enhance their threat intelligence capabilities, organizations should prioritize platforms that offer curated, multi-source intelligence and invest in solutions that offer detailed, yet prioritized insights. These tools not only enhance the efficiency of security teams but also ensure that resources are directed toward mitigating the most relevant and immediate threats.

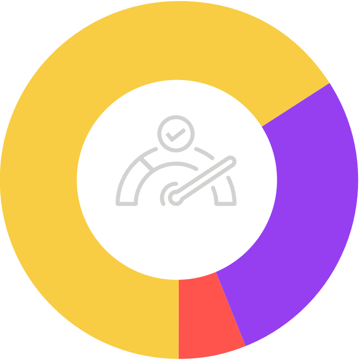
Effectiveness of Threat Intelligence Tools

The survey results reveal a negative outlook on the effectiveness of current attack surface intelligence tools, with only a portion of the market realizing full value from their capabilities. While 28% of respondents rate their tools as useful—indicating that these solutions deliver some degree of curated, pre-validated, and prioritized threat data—the majority (66%) find them only nominally useful.

This suggests that while some organizations are benefiting from advanced attack surface intelligence that enables proactive responses and reduces investigation time, most still struggle with tools that provide only more generalized threat intellience, requiring analysts to do more investigative analysis and inference. The fact that 6% of respondents find their tools not useful at all, citing irrelevant data and an increase in alert noise, highlights that many attack surface intelligence solutions have not met the market's needs.

Smaller organizations found their attack surface threat intelligence tools 20% less effective compared to larger organizations, likely reflecting the advantage larger enterprises have in both size and specialized personnel. Unsurprisingly, management reported finding these tools 30% more effective than those in operational roles, indicating a potential gap between tool perception and hands-on efficacy.

How would you rate the usefulness of your organization's attack surface threat intelligence tools?



66%
Nominally Useful
Threat data varies in relevance or substantiation - mostly used to enrich investigation after discovery.

28%
Useful
Threat data is often curated and active threat details are pre-validated and prioritized.

6%
Not useful
Threat data is informational but not always relevant - it often increases alert noise levels and prolongs investigation efforts.

Figure 6. Extent of attack surface threat intelligence tool effectiveness.

The gap in usefulness underscores that vendors providing these solutions have much room for improvement. It suggests that most attack surface intelligence tools are still not reducing investigative burdens on security analysts. Many organizations still face overwhelming data and noise, with tools that fall short in filtering and prioritizing actual threats. To improve value, organizations should focus on those tools that not only provide comprehensive threat data but also prioritize actionable intelligence. Solutions that reduce the investigation burden by delivering pre-validated threat details allow security teams to act more efficiently and proactively, ultimately improving their overall threat response capabilities.

Perceived Trends for EASM and Threat Intelligence

Perceived future trends driving the evolution of EASM are centered on the convergence of Vulnerability Assessment (VA), Continuous Automated Attack Surface Management (CAASM), and EASM solutions, cited by 63% of respondents. This convergence reflects the industry's shift toward Continuous Threat Exposure Management (CTEM), where processes and supporting tools work together to enable security teams to achieve comprehensive visibility, proactive remediation, efficient incident response, and greater resiliency, across all layers of an organization's attack surface. Additionally, 51% of respondents anticipate greater reliance on generative artificial intelligence (AI) to facilitate threat response and mitigation, as AI rapidly analyzes large datasets and automates noise reduction, threat validation, and mitigation triage processes. Respondents also anticipate easier to use tools (33%) and broader integration capabilities (28%) to enhance their SecOps team's ability to improve their cyber security posture.

What future trends do you think will have the most significant impact on your organization's EASM programs and threat intelligence tools?

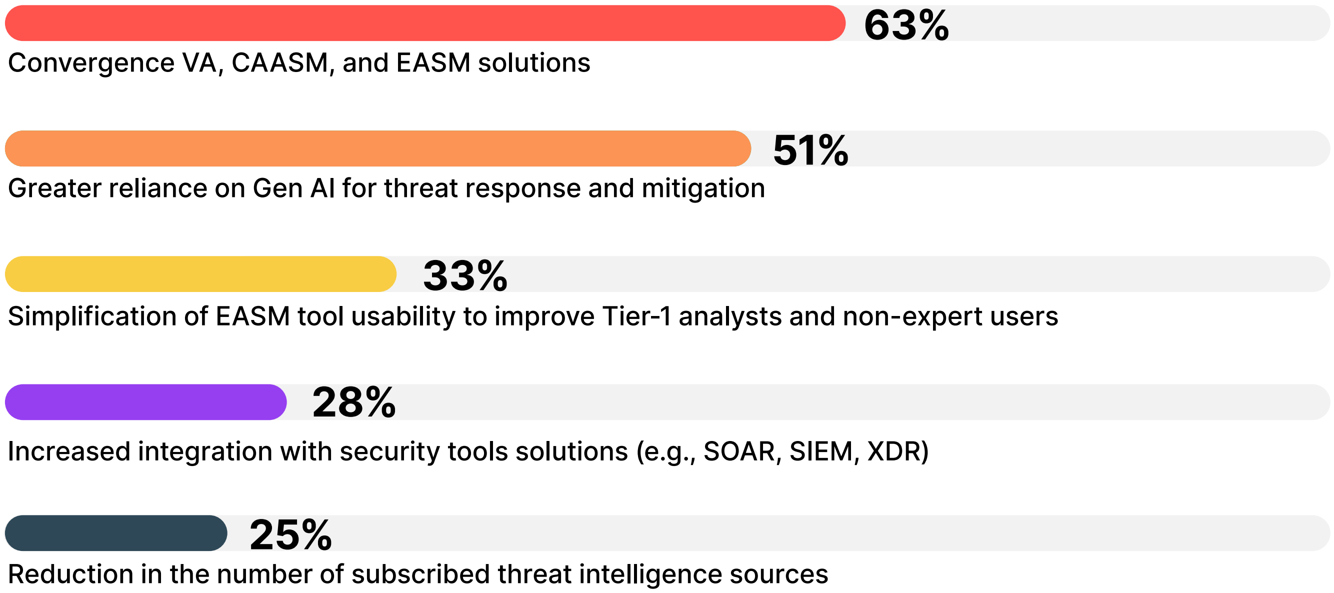


Figure 7. Top 5 perceived trends that will significantly impact EASM programs and TIM.

Interestingly, 25% of respondents foresee a reduction in the number of subscribed threat intelligence sources, pointing to a shift toward fewer, more effective attack surface threat intelligence solutions.

EASM Program Maturity

The maturity of EASM programs varies significantly across organizations. Nearly 50% of respondents report that their programs are in the early stages of development, either in the "Initial" or "Repeatable" phases, where processes remains unstructured and reactive. Only 33% of respondents are in the most advanced stages of maturity, with 22% reporting proactive, managed programs and 11% achieving optimized automation and continuous threat assessment. Perhaps the anticipated increase in EASM expenditure may be applied to progress program capabilities (and tool sets), and in turn, maturity.

Larger companies (>2,500 employees) report EASM maturity levels twice that of smaller organizations (20% vs. 10%). Operations teams (16%) are less positive about maturity than senior management (18%). Government and critical infrastructure sectors (25%) trail slightly behind financial services, healthcare, and technology, with technology and healthcare reporting stronger maturity (23%).

How would you describe the maturity of your organization's external attack surface management program?

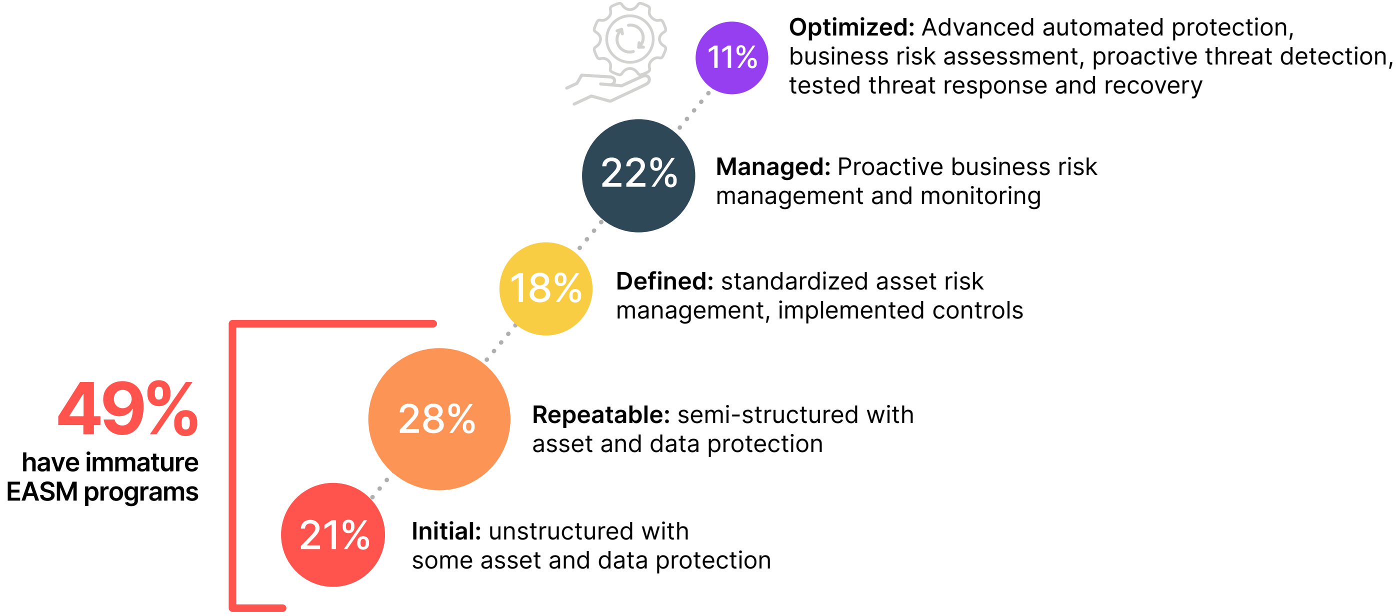


Figure 8. EASM program maturity.

These findings underscore ample room for growth in maturing the people, processes, and tools necessary for effective EASM. Organizations must move beyond ad hoc and reactive measures and invest in more advanced, proactive, and automated approaches that help mature attack surface management to enhance their overall security posture and resilience.

Near-Term EASM Program Objectives

As organizations continue to face new threats across an expanding attack surface, their near-term focus is on improving speed, accuracy, and intelligence in managing attack surface exposures. A top priority for 65% of respondents is accelerating identification and remediation speed. This indicates a clear recognition of the need for faster responses to emerging threats as organizations deal with more sophisticated and dangerous threats against an increasingly dispersed and vulnerable digital landscape. Additionally, 59% seek to achieve a complete and accurate inventory of all internet-facing assets, underscoring the risks associated with attack surface dynamics as previously expressed by respondents, including the ongoing challenge of maintaining visibility across cloud environments, remote endpoints, and web applications.

Enhancing proactive remediation is a goal for 48% of respondents, highlighting the shift from reactive defenses to more forward-looking strategies aimed at stopping threats before they escalate. This aligns with Continuous Threat Exposure Management (CTEM) initiatives taking ground in many organizations. Similarly, 44% are focused on enriching the quality of threat intelligence data in existing tools (SIEM, XDR, SOAR), seeking to amalgamate internal with external attack surface insights. This would also serve to enhance overall capabilities for security posture risk assessment, as well as help further automate remediation and containment. Notably, 30% aim to reduce the volume and noise of threat intelligence data, emphasizing that while more intelligence is being gathered, filtering out irrelevant and outdated information remains a critical challenge for security teams.

What are your organization's near-term objectives for advancing your external attack surface management program and threat intelligence tools?

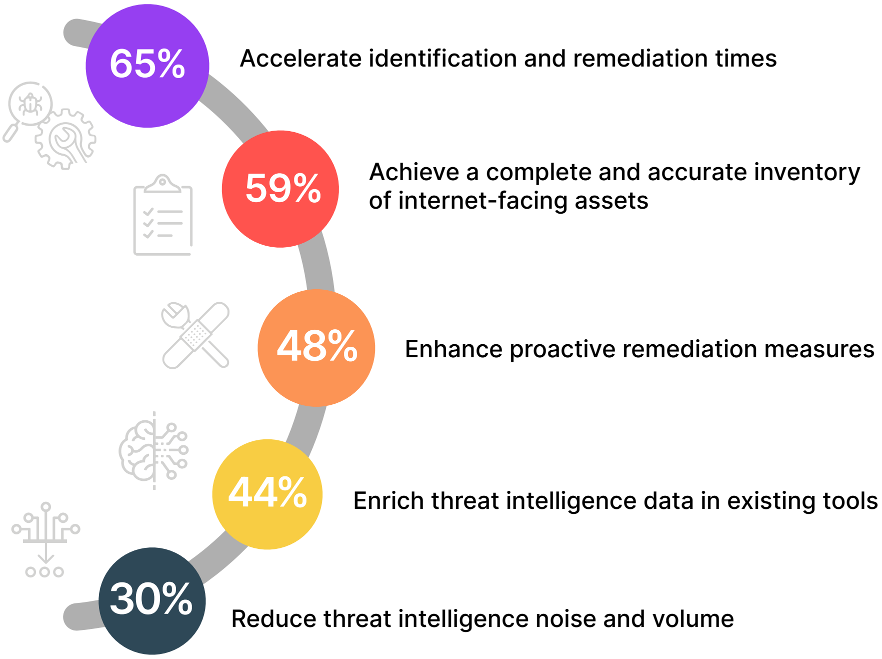


Figure 9. Top 5 near-term EASM program objectives.

These priorities show that while organizations are advancing their attack surface management programs, they still have significant hurdles to overcome, particularly in balancing comprehensive visibility with the reduction of threat noise. Solutions that offer real-time monitoring, actionable insights, and improved filtering capabilities will be critical in helping security teams keep pace with the evolving digital landscape.

Expanding Budgets

The financial and resource commitment to EASM is on the rise, with 90% of respondents expecting budget increases in the coming year. Of these, 40% anticipate significant increases of more than 20%, reflecting the growing recognition of EASM's importance in mitigating risks and securing the expanding attack surface.

To what extent do you expect your organization's budget for external attack surface management tools and threat intelligence data to change next year?

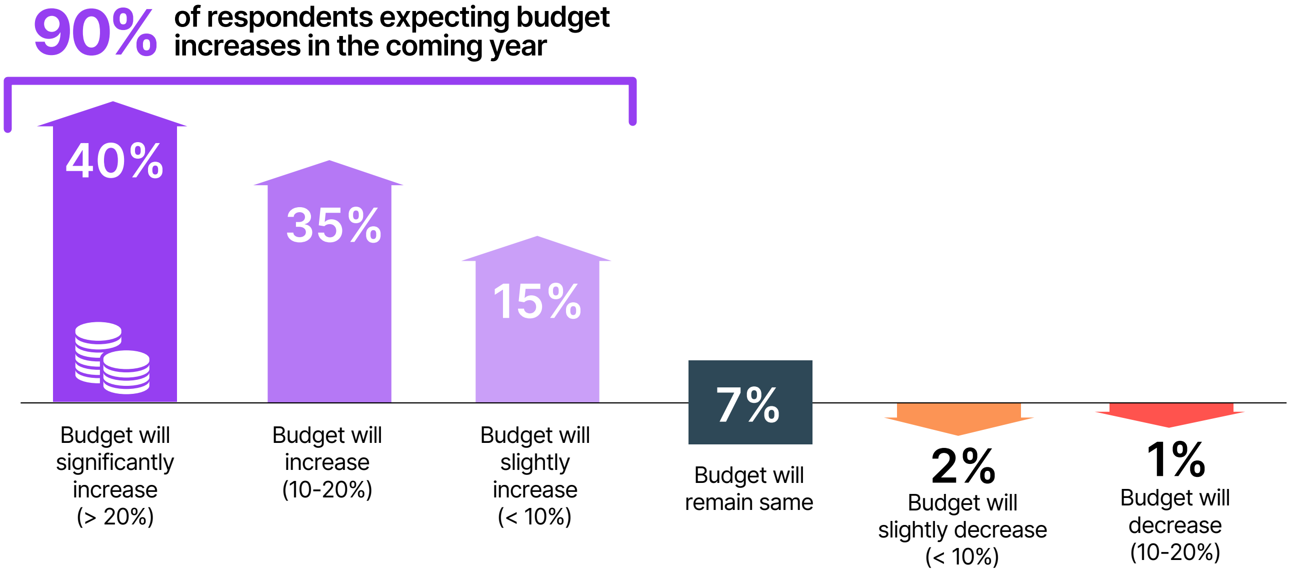
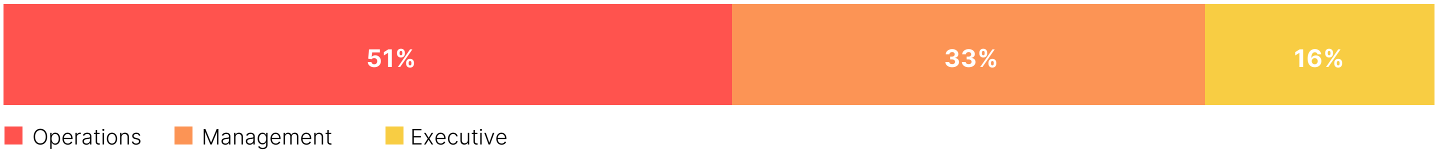


Figure 10. Planned budget for external attack surface management and threat intelligence.

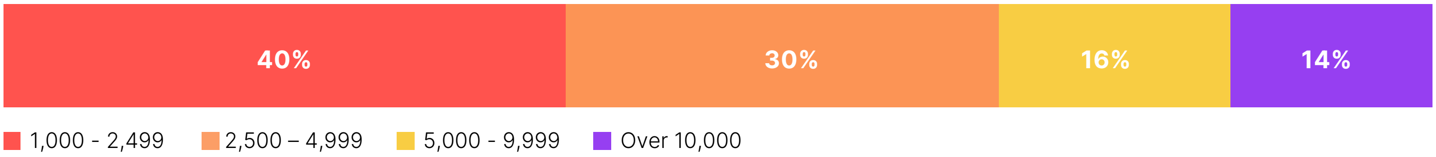
Methodology and Demographics

The 2024 Attack Surface Threat Intelligence Report is based on a comprehensive online survey of 312 cybersecurity professionals conducted in September 2024 to gain insight into the challenges, advantages, maturity, and best practices for using threat intelligence and managing external attack surface risk. All respondents manage programs and teams or use threat intelligence and external attack surface management tools daily.

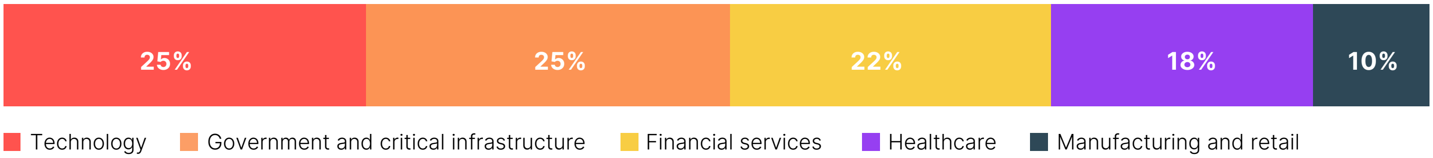
DEPARTMENT



COMPANY SIZE



INDUSTRY



Reuse of content

We encourage the reuse of data, charts, and text published in this report under the terms of this Creative Commons Attribution 4.0 International License. You're free to share and make commercial use of the finding in this report as long as you attribute the information you leverage from the report as follows:

"2024 Attack Surface Threat Intelligence Report" produced by Cybersecurity Insiders, Cogility, and TacitRed.

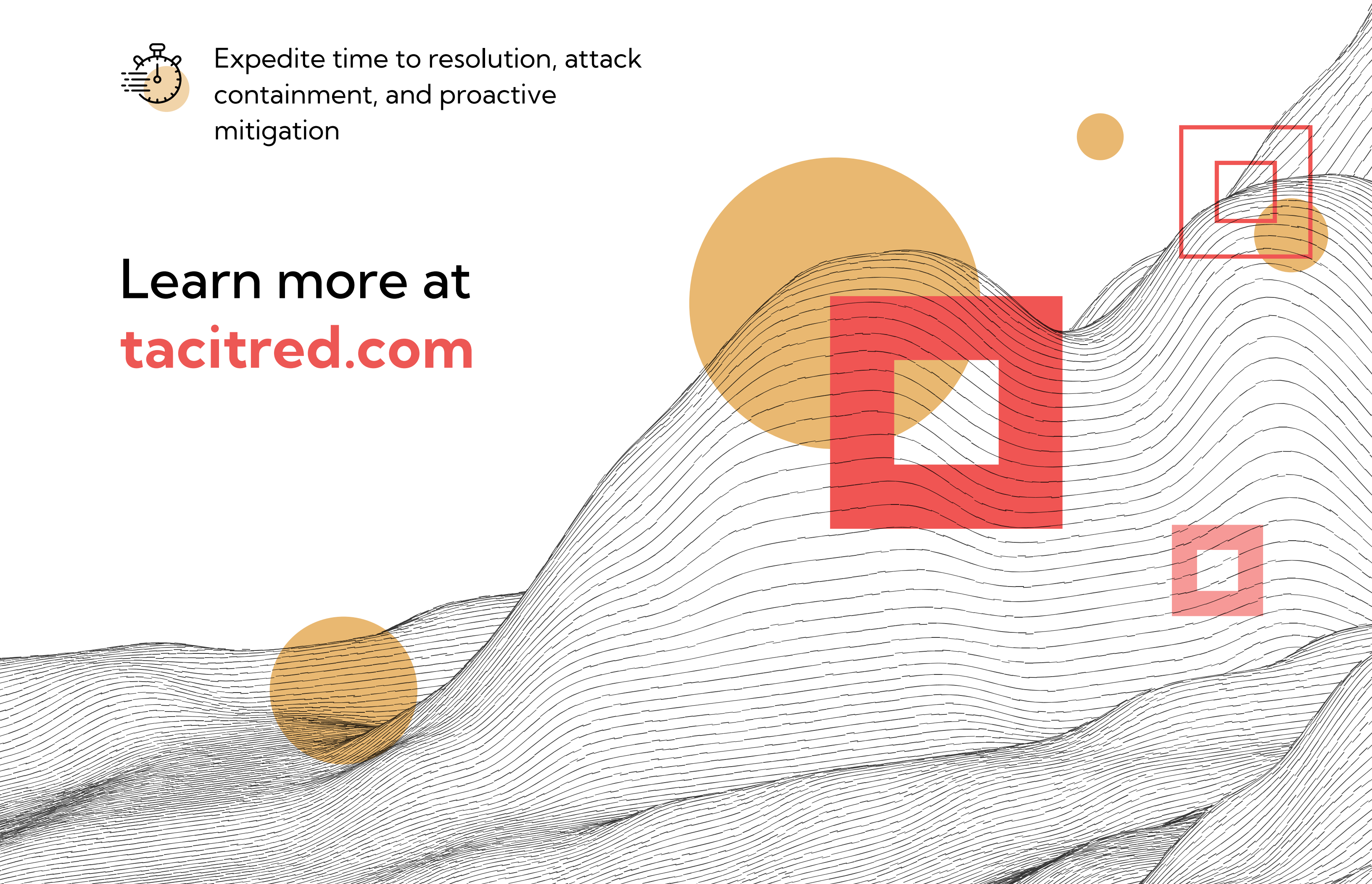
TacitRed

Tactical Attack Surface Intelligence

Today, over 80% of security breaches originate from threat actors successfully conducting phishing, session, and malware attacks, and exploiting vulnerable internet-facing assets. Cogility TacitRed™ empowers security analysts to take immediate, decisive actions to mitigate impactful cyber exposures by taking advantage of unparalleled tactical attack surface intelligence.

- Continuous intelligence: on-demand, curated, prioritized, and detailed
- Active attack surface exploits and exposures of over 18 million U.S. entities
- In-depth findings: scoring, threat type, attack stage, severity, and full context
- Comprehensive, actionable third-party risk assessment
- Expedite time to resolution, attack containment, and proactive mitigation

Learn more at **tacitred.com**



Cybersecurity

INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today’s most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today’s complex cybersecurity challenges.

For more information:
email us info@cybersecurity-insiders.com or visit cybersecurity-insiders.com