

**Discovery
Report**

April 2023

The Impact of Continuous Security Validation

Commissioned by

 **SafeBreach**

S&P Global
Market Intelligence

©Copyright 2023 S&P Global. All Rights Reserved.

Introduction

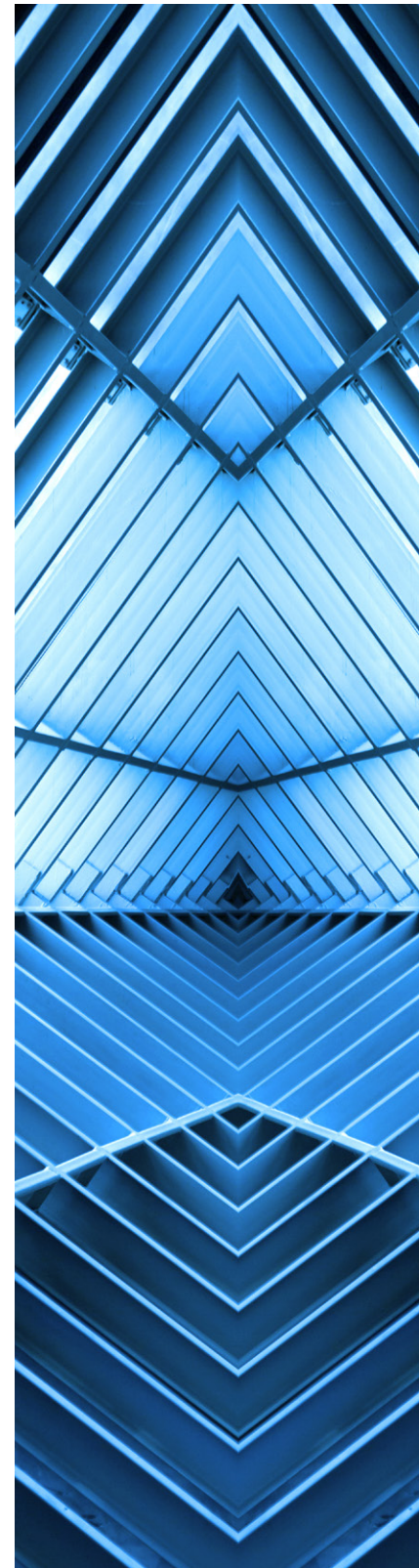
Steady increases in the size and complexity of attack surfaces, coupled with ever-more-sophisticated attackers, have prompted organizations to shift from primarily defensive approaches to more automated, proactive strategies that simulate actual attack methods and enable detection, verification and prioritization of the most dangerous risks. Continuous security validation (CSV) is an ongoing process that regularly tests an organization's security posture through continuous monitoring and verification of security controls, systems and processes, enabling identification and remediation of security weaknesses.

While technologies such as vulnerability scanners and penetration testing tools are valuable for point-in-time assessments, the dynamic nature of the threat landscape calls for a more continuous, automated approach. Unlike previous approaches, which relied on high-level scans or customized manual testing, newer CSV tools utilize automated security tools and techniques that leverage the same tactics, techniques and procedures (TTPs) used by criminals, but apply them to determine and remediate weaknesses, enabling organizations to continuously measure their security posture over time. This helps ensure the effectiveness of an organization's defenses and reduce the risk of successful breaches.

S&P Global Market Intelligence conducted a survey in late 2022 among 400 highly qualified security practitioners across the United States and Europe with the objective of understanding respondents' biggest security challenges, which CSV tools they are using, the level of adoption and maturity of those tools, and the business outcomes they achieved. This paper provides an overview of key CSV concepts, an analysis of key findings from the study and recommendations for organizations considering further investments in CSV technologies.

Key concepts

Continuous security validation is composed of several distinct, yet related, technologies. This overview of key concepts is intended to facilitate a clearer and more complete understanding of the capabilities and differentiators of the various CSV offering categories. Many of these technologies take different approaches to providing security teams the insights they need to answer questions about the state of their organization's security posture. To select a CSV tool that fits their unique needs, organizations must have a clear understanding of which products and services provide what capabilities. In addition to discussing key CSV product categories, we also define a few related terms.



- **Red, blue and purple teaming** are approaches used to organize cybersecurity professionals for conducting security testing and assessments. Red teams, which act as “ethical hackers,” attempt to breach organizational security defenses using the same TTPs as a real attacker. Red teaming is usually conducted without advance notice, with the goal of identifying weaknesses and providing recommendations on how to improve security posture. In some cases, red team activities are automated, providing continuous analysis of security controls, albeit using less detailed, less customized tests. Blue teams, which represent the organization’s defensive capabilities, attempt to defend against red team attacks, with the shared goal of identifying and remediating weaknesses. Purple teaming brings red and blue teams together to share knowledge and discoveries through a common platform.
- **Vulnerability scanning and assessment**, an aspect of vulnerability management (VM), is the scanning of network endpoints for unpatched vulnerabilities and configuration errors to aid security and IT teams in building remediation actions such as patching and configuration changes. Drawbacks of this approach include difficulties in performing external scans, shallow scan results, issues with conducting authenticated scans, lengthy scan times, false positives and the inability to detect “zero-day,” non-publicly-disclosed vulnerabilities or other non-CVE-based weaknesses. On the positive side, VM products are easy to install and run, and they can be inexpensive (or even free) as the segment has become highly commodified. While vulnerability scanning and assessment is still a critical use, more advanced testing techniques are needed.
- **Automated penetration testing (automated PT)**, also known as “automated pen testing,” are practices and tools that aim to simulate real-world attacks, identify vulnerabilities and discover system weaknesses by performing non-destructive tests against production systems from the viewpoint of an attacker. Designed to mimic the TTPs used by attackers, pen testing tools provide a deeper, more customized set of tests than VM. Traditional pen tests were conducted on a manual, point-in-time basis, running custom simulations that leverage vulnerability scanners, password crackers and exploit frameworks. Automated PT tools have emerged that enable repeatable, continuous testing, although automated pen tests may be less robust than manual ones that can call upon a tester’s experience and expertise in assessing a particular exposure. While pen testing tools focus on finding ways to breach systems and access critical assets, they may not be designed to execute complex attacks such as those that include multiple kill-chain steps and dependencies. Thus, they may miss potential weaknesses such as data exfiltration and lateral movement. Legacy PT tools are not generally designed to operate at scale because they require manual intervention and considerable effort to complete, although automated pen testing at scale is on the rise.

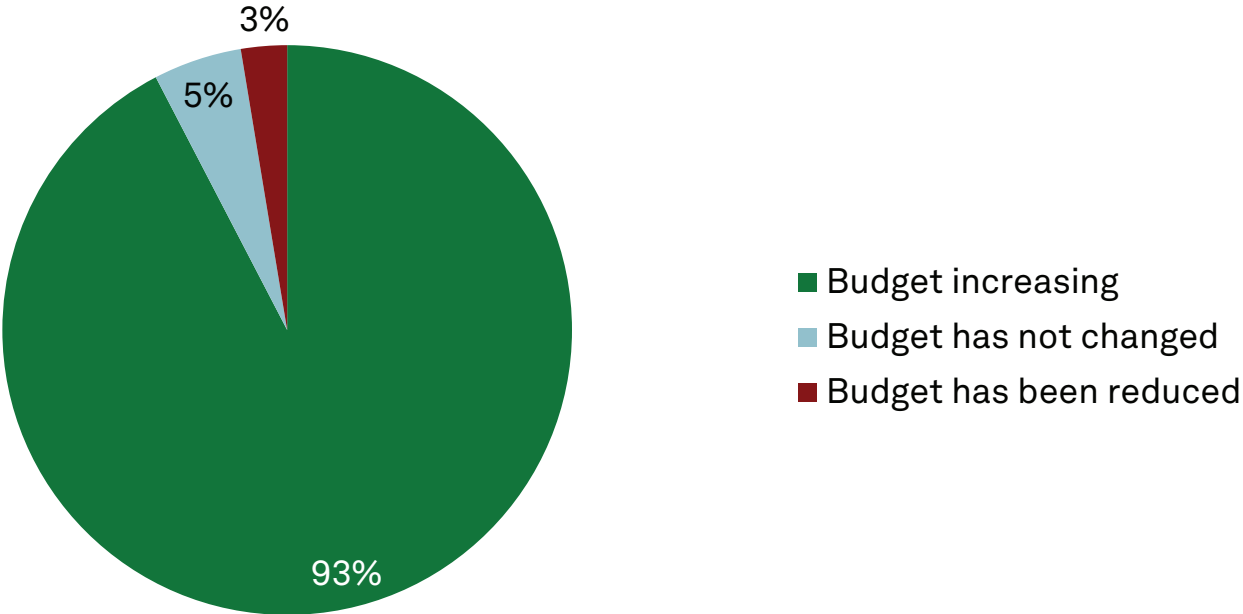
- **Attack surface management (ASM)** tools focus on discovering and minimizing risks from the perspective of an organization's attack surface. Given the steadily increasing rate of technical shifts due to digital transformation, the API economy, migration to cloud and the explosion of internet-connected devices, mapping and detecting attack surface weaknesses is critical. ASM builds on VM concepts, making them more robust and proactive while adding a dimension of risk to its analyses by mapping exposures to exploitability, in some cases referencing frameworks such as MITRE ATT&CK and supporting internal and external scanning. These tools also typically cover a wider set of targets than vulnerability management and penetration testing. The ASM category includes subdomains such as external attack surface management (EASM), cyber asset attack surface management (CAASM) and digital risk protection services (DRPS). EASM tools focus on discovery of public-facing assets, monitoring them for weaknesses and misconfigurations. CAASM tools also discover and monitor assets for security weaknesses; however, their analytics may be based on API integrations, generally limiting the scope to internal assets. DRPS technologies focus on the open web, dark web and social media, seeking threats related to an organization's digital assets as part of an overall risk management strategy. These tools do not typically provide asset inventories or risk assessments. ASM products may fall short of fully delivering on continuous security validation if they lack, for example, the ability to conduct exploitability and attack-chain analyses, which can be invaluable when determining the best course of remediation, particularly for advanced attacks.
- **Breach and attack simulation (BAS)** evolved from automated red and blue teaming with the objective of providing continuous, automated simulation of advanced breaches and attacks using actual attacker TTPs, along with supporting "purple team" collaborative processes by providing a single testing and simulation platform for offensive and defensive exercises. Testing is executed continuously against production systems using non-destructive methods. BAS platforms integrate with multiple security controls including endpoint, network, cloud, email and data loss prevention. BAS tools also correlate their attacks against alerts and events received by security information and event management (SIEM) data, improving the understanding of security control efficacy. These tools can integrate with workflow management tools such as security orchestration and response (SOAR) platforms to help optimize response and remediation processes. BAS tools can also combine multiple attack modalities into customizable, sophisticated "playbooks" composed of multiple attacker TTPs, which are placed into libraries that are continually updated as new TTPs emerge. The result is a set of tests that come very close to simulating real attacks that are designed to run continuously, providing organizations with near-real-time security control validation. BAS tests can be more thorough than other CSV tools due to extensive integrations and the use of many more TTPs.

Security trends

Security spending continues its upward trend despite macroeconomic headwinds. In 451 Research's Voice of the Enterprise (VoE): Information Security, Budgets & Outlook 2023 survey, 92.5% of respondents projected budget increases over 2022. This is consistent with 2022 and 2021 VoE data (94% and 86% of respondents projected increases, respectively), indicating that despite forecasts of potential macroeconomic headwinds, organizations continue increasing security spending year after year.



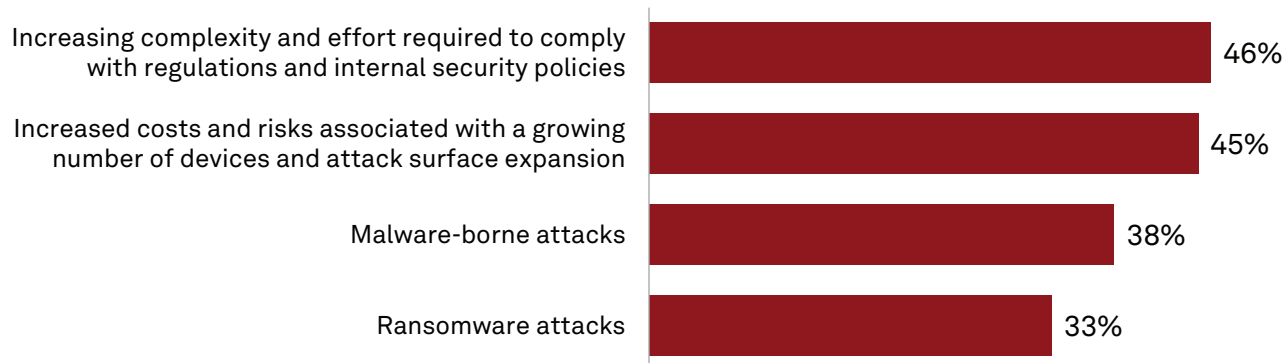
Figure 1: Trajectory of IT security spending year over year



Note: Discrepancy in total is due to rounding.
Q. By what percentage do you expect your organization's total information security budget to change in 2023 compared to 2022?
Base: All respondents, abbreviated sample (n=501)
Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2023

Top security risks and issues include increasing complexity and effort required to comply with regulations and internal security policies (46%), increased costs and risks due to growing numbers of devices and attack surface expansion (45%), malware (38%) and ransomware (33%). Managing hybrid cloud security is also a top security risk (33%). Compliance clearly remains a major driver of security spending, along with increased risk due to the explosion in the quantity of internet-connected devices and cloud deployments that result in continual attack surface expansion. And unsurprisingly, ransomware and malware continue to plague organizations. In 451 Research’s Voice of the Enterprise: Information Security, Budgets & Outlook 2023 report, respondents’ top-cited strategic objective is improving security awareness (anti-phishing, training, etc.). The second, third and fourth selections are a virtual tie (implement or improve data security, improve application security and improve risk/vulnerability assessment or management). While the top response is mainly centered on training humans to be more security aware, the other three categories can all be improved through the use of security validation technologies, which can discover weaknesses in data security and application security while also performing risk/vulnerability assessments and improving the management of them. Hybrid cloud continues to gain in prominence as well, with the percentage of organizations using more than one cloud, as well as those using both cloud and on-premises architectures, growing every year.

Figure 2: Primary cybersecurity risks



Q. What are your organization’s primary cybersecurity risks/issues?
 Base: Respondents with over \$750 million in revenue (n=96).
 Source: S&P Global Market Intelligence custom survey, December 2022.

Of the top security risks and issues identified above, those most widely deemed to have high potential for negative business impact include malware (63%), ransomware (52%) and difficulties in managing hybrid cloud environments (48%), indicating that organizations are seeing more business impact from these risks, regardless of the degree of concern expressed. They also say that hybrid cloud security introduces risk, which is logical since a large part of today’s attack surface expansion is due to hybrid cloud. Adding to this issue are the number of multicloud organizations.

Phishing/whaling is the category of attack most frequently identified as increasing in the past year (43%), followed by ransomware (40%) and malware (35%). This indicates that attacks against the weakest security link (humans) are on the rise, and ransomware remains a major concern.

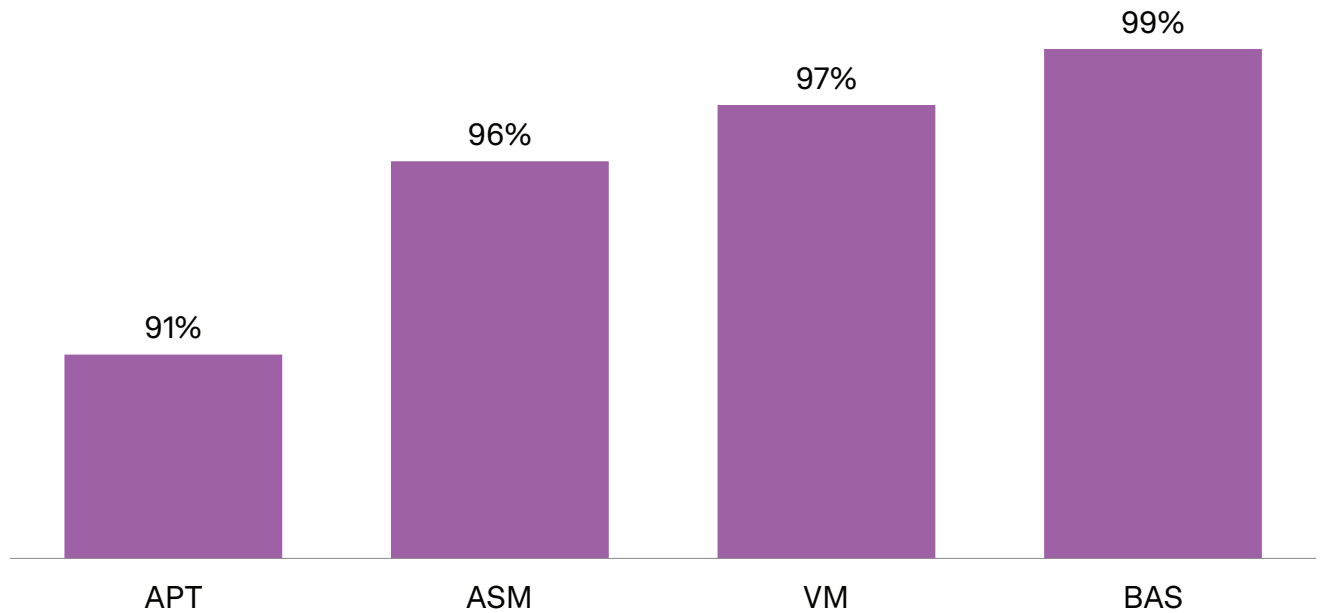
Ransomware attacks continue to plague organizations, with 47% of respondents indicating that their organization has experienced a ransomware attack in the past year. More than half (56%) of organizations that experienced an attack paid the ransom, though only about two-thirds of those payments resulted in successful recovery (39% of affected respondents). In 451 Research's Voice of the Enterprise: Information Security, Endpoint Security 2022 study, fielded nearly a year prior to the CSV study, only 22% of affected respondents paid the ransom, representing a difference of 2.5x in the rate of payments. The higher proportion of ransom payments among CSV study respondents suggests that a negative experience with an attack may have motivated CSV investments within this study population. Additionally, only 50% of those reporting a ransomware attack activated a formal ransomware recovery and remediation plan, indicating that many have yet to create and rehearse formal plans, a key success factor in organizations that successfully recovered from an attack without significant business impact.

“Swivel chair management,” also known as tool overload, is prevalent. Security analysts are overwhelmed by the quantity of security tooling available to them, making it difficult to perform their jobs effectively. In practice, many security tools are deployed tactically, often to satisfy a specific use case or compliance requirement, with little thought given to how (or whether) analysts will use them in their day-to-day jobs. Respondents indicate that, on average, analysts have access to 21-30 tools and use 11-20 of them at least weekly. This is a sobering statistic given the amount of time and money required to install and maintain all those tools and train staff to use them, as well as the amount of churn and delays in incident response due to the number of tools in use. Organizations leveraging CSV technologies may recognize the need for a tool that can help them validate security controls and the effectiveness of other tools already in place, assisting in identifying and reducing the count of ineffective security tools.

The cyber skills shortage continues to plague organizations. About half (48%) of respondents indicate they are very concerned, and 43% are somewhat concerned about the skills shortage, amounting to 91% showing concern about staffing. Interestingly, 451 Research's Voice of the Enterprise: Information Security, Organizational Behavior 2022 report indicates that only 37% of respondents believe that staffing levels are inadequate. This provides strong evidence that organizations considering or deploying CSV technologies are much more concerned about sourcing expertise than the more general population of security professionals. Reductions in tooling quantity, improved tool integration and automation all assist with these issues.

Continuous security validation tools provide significant business value across the spectrum, with breach and attack simulation taking the top spot (99% of respondents reporting a positive ROI). Vulnerability management is next (97%), followed closely by attack surface management (96%) and then automated penetration testing (91%).

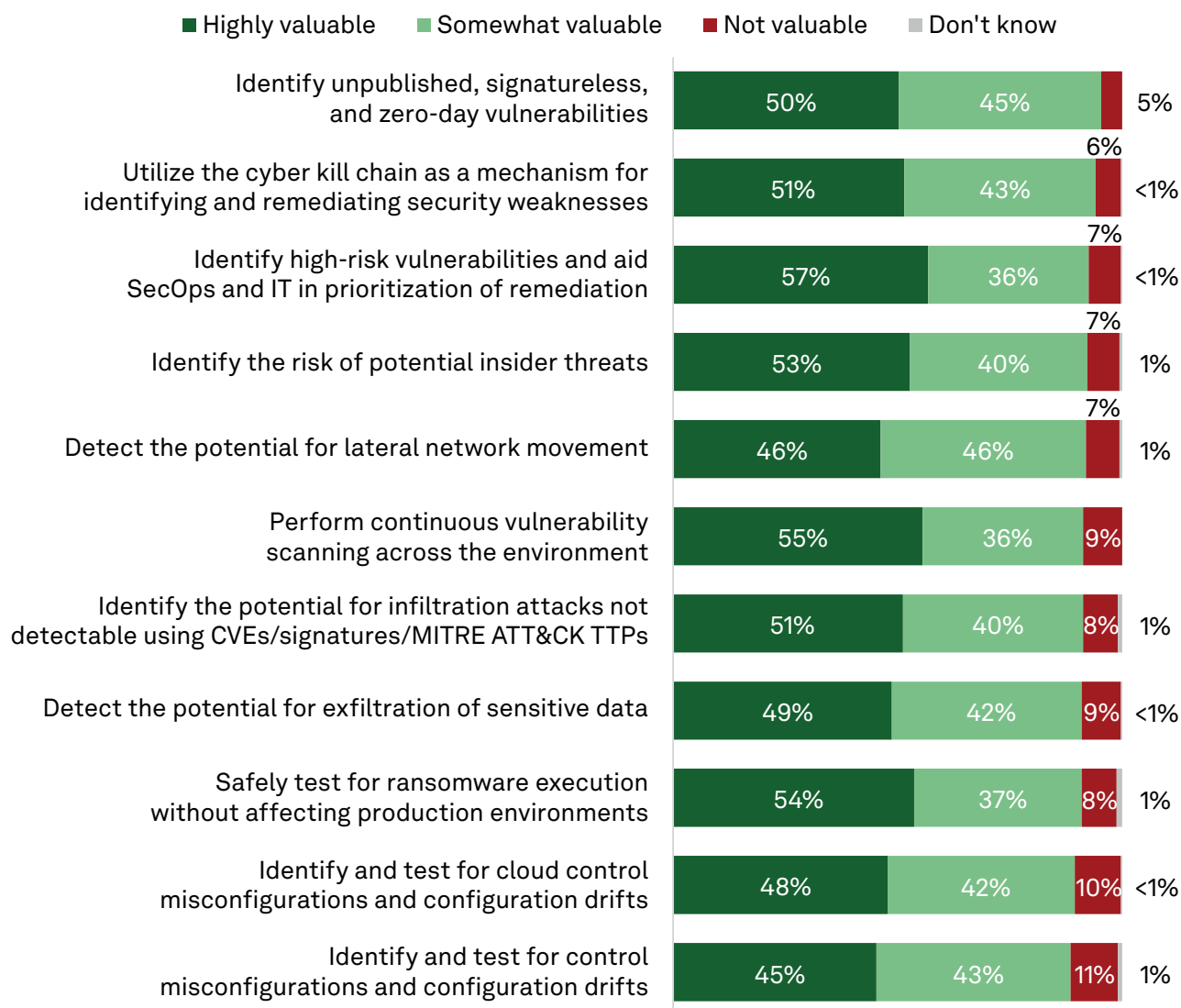
Figure 3: CSV return on investment



Q. To what level do you agree that your current [CSV product category] tools provide a positive return on investment (ROI)?
Base: Respondents with over \$750 million in revenue (n=96).
Source: S&P Global Market Intelligence custom survey, December 2022.

Respondents are particularly bullish on the effectiveness of BAS capabilities in reducing business and operational risk, including identifying unpublished, signatureless and zero-day vulnerabilities, which 95% of respondents rank as highly or somewhat valuable. Utilizing the cyber kill chain as a mechanism for identifying and remediating security weaknesses followed closely (94%), and then identifying high-risk vulnerabilities and aiding SecOps and IT in prioritization of remediation (93%). BAS is clearly emerging as a significant player in the CSV market, as these capabilities are major differentiators between BAS and other CSV product offerings.

Figure 4: BAS capabilities in terms of business and operational risk reduction



Q. How effective are your organization's breach and attack simulation (BAS) capabilities?
 Base: Respondents with over \$750 million in revenue (n=96).
 Source: S&P Global Market Intelligence custom survey, December 2022.

Primary drivers of return on investment for breach and attack simulation include increased visibility into security control performance and overall security posture (54%), quantifiable risk reduction based on the ability to minimize the number of attacks and breaches (33%) and SecOps staff augmentation/staffing cost reduction (11%).

Figure 5: Benefits of BAS that drive significant ROI

- Increased visibility into security control performance and overall security posture
- Quantifiable risk reduction based on the ability to minimize the number of attacks and breaches
- The ability to augment the SecOps team and reduce staffing costs
- Savings based on the ability to reduce the number of tools required



Q: Which of the following is the most significant driver of ROI that your current breach and attack simulation (BAS) tools provide?

Base: Respondents with over \$750 million in revenue (n=96).

Source: S&P Global Market Intelligence custom survey, December 2022.

Conclusions

The study reveals a number of key use cases and pain points that CSV tools can solve. Study findings also show that breach and attack simulation solves use cases that other CSV technologies do not — such as identifying unpublished, signatureless and recently discovered vulnerabilities, detecting the potential for lateral movement, utilizing the cyber kill chain as a mechanism for identifying and remediating security weaknesses, and identifying high-risk vulnerabilities to guide remediation activities — all of which rank highly in the survey in terms of business and operational risk reduction. A major advantage of BAS approaches is continuous, automated validation of deployed security controls, enabling organizations to detect and remediate issues more quickly than more traditional, point-in-time approaches.

While organizations continue spending more on security every year, increasing compliance requirements, increased costs and risks due to the growing number of devices and the size of attack surfaces, and malware/ransomware continue to plague businesses around the globe. In the face of economic headwinds, executive teams and boards will demand evidence that their organization is protected and that budgets are being spent prudently. Survey data provides evidence that CSV buyers are more motivated to invest in technologies that should be a priority for all. Compared with others, they have sustained higher incidences of attacks such as ransomware, which could help explain their recognition of a need for tools that could better protect them from similar attacks. Testing and validation technologies are becoming increasingly useful in terms of prioritizing security investments, understanding the impact of environmental changes from business transformation and modernization, and validating the efficacy of security controls. The survey bears this out, with BAS getting the top ranking in terms of business value among CSV buyers.

From a regulatory compliance perspective, the trend is toward more automated, continuous testing. In response, traditional assessment firms have already begun incorporating automation into their solutions, which is only logical because it makes good business sense for them as well. Automation by itself, however, does not satisfy the full set of use cases required to successfully achieve CSV.

The growth of cloud environments — and multicloud organizations — is exacerbating these issues by further extending organizational boundaries. Additionally, staff shortages and tool overload run counter to one another, as fewer personnel clearly do not benefit from even more tooling unless those tools make them more effective or result in tool consolidation. Investments that provide value from automation combined with increases in visibility, transparency and productivity will continue to gain in popularity as organizations realize that security posture cannot be validated through infrequent, manual, point-in-time events.



When evaluating continuous security validation offerings, it is critical to understand the specific functionality and use cases solved by specific product categories and vendors. As evidenced in the study, many security professionals are confused by the dizzying array of functionalities that vendors say are available across the CSV spectrum — and clear overlaps exist. Consumers of these technologies need to focus on their own critical security use cases, mapping them to the matrix of vendor capabilities. This is particularly true for cloud use cases, since many traditional security tools were not designed for cloud. For example, automated penetration testing technologies, which may perform wholesale scanning of ports, IPs and endpoints, can trigger cloud provider distributed denial-of-service responses, particularly in shared infrastructure environments.

Breach and attack simulation has emerged as a well-differentiated CSV technology by fulfilling use cases that other products may not cover, including the ability to detect potential issues across all stages of an attack chain, pre- and post-compromise, across on-premises and cloud, typically utilizing MITRE ATT&CK TTPs to aid in detection and remediation. BAS tools leverage real-time threat feeds and data from organizational security platforms, helping to ensure that simulations use the latest threat data and environmental telemetry. This enables these tools to perform continuous control validations across multiple attack surface layers, including networks, endpoints and cloud environments. Integration with other systems, such as SIEM, SOAR, service desks and workflow management tools also simplifies the process of acting on needed remediations. Further, the ability to perform continuous, automated, customizable simulations, which can run against internal and external resources, calls out values that BAS tools are purpose-built to address.

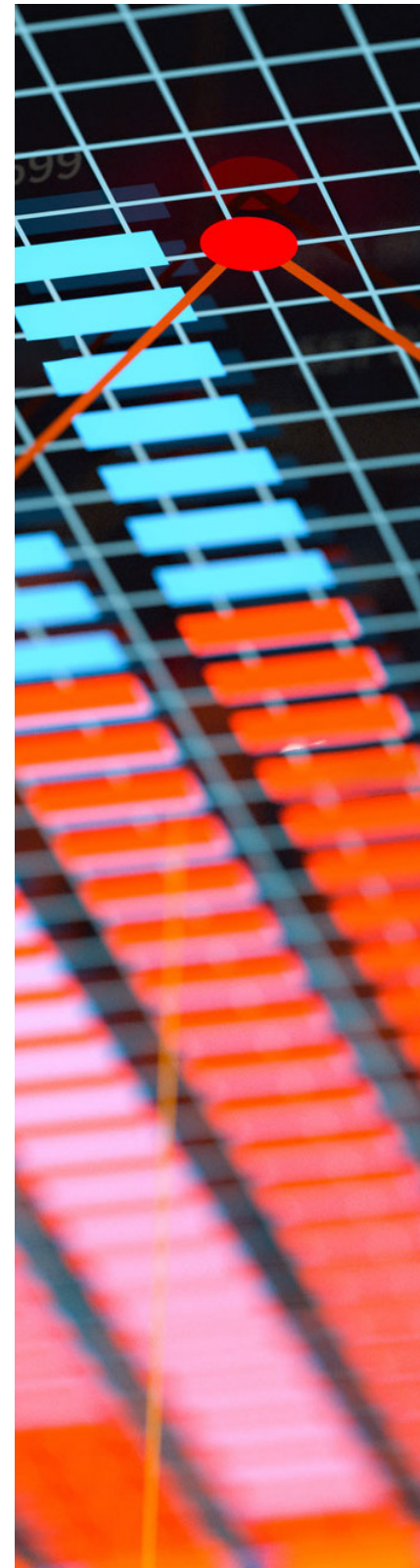
Today's organizations suffer from an embarrassment of riches — an excess of security data and tooling — and too often, an acute inability to translate the vast sea of data into actionable, risk-prioritized actions. And while security tools that focus on searching and analyzing all this data to detect incident scenarios such as breaches in progress (or those that occurred in the past) are clearly valuable, BAS tools can allow organizations to shift to a more proactive stance by focusing on prevention. Today's enterprises are looking to increase visibility across the entire IT ecosystem, gaining insights into their security posture as a basis for constructing more resilient cybersecurity programs. For this to happen, a shift in tactics is required. The pace, volume and variety of threats may make point-in-time snapshots conducted at weekly or monthly intervals less viable than more continuous approaches. Breach and attack simulation has emerged as a distinctive innovation for further instantiating the vision of continuous security validation, and organizations concerned with implementing a complete CSV solution should consider adding BAS tools to satisfy key use cases not provided by other CSV products.

Methodology

The findings presented in this report draw on a custom US and UK survey fielded in December 2022 (n=401; US 63%, UK 37%). Respondents were from a wide variety of industries and organizations with 1,000+ employees in the US and 500+ employees in the UK. All survey respondents were screened for being involved in the decision-making process for the purchase and/or deployment of cybersecurity technologies within their organization. Respondents' organizations were screened for adopting/using at least one of the following technologies: automated penetration testing, attack surface management, vulnerability management, or breach and attack simulation. This report also draws on contextual knowledge of additional research conducted by S&P Global Market Intelligence.

SafeBreach

While there may be some market confusion about CSV and the technologies that are best suited to support it, organizations can overcome this challenge by developing a solid understanding of the use cases and capabilities supported by various CSV tools in order to select one that best suits their needs. To learn more about the available technology approaches to CSV, including the pros, cons, and ideal environments for each, download a copy of [SafeBreach's white paper](#) today.



About the author



Mark Ehr

Senior Consulting Analyst

Mark Ehr is a Senior Consulting Analyst in the S&P Global TMT team based in Denver, Colorado, USA. Prior to joining S&P, he spent 12 years at IBM in roles including worldwide security sales enablement and QRadar SIEM product management.

Prior to IBM, he worked for BigFix, Cabletron, Enterprise Management Associates, Ping Identity, Polarsoft, Siebel Systems, and Sybase, in roles including consultant, entrepreneur, industry analyst, product marketer, software developer, and tech seller.

Mark holds a bachelor's degree in Computer Science from Metropolitan State University of Denver.

About this report

A Discovery report is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the “on the ground” experience and opinions of real practitioners — what they are doing, and why they are doing it.

About S&P Global Market Intelligence

S&P Global Market Intelligence's Technology, Media and Telecommunications (TMT) Research provides essential insight into the pace and extent of digital transformation across the global TMT landscape. Through the 451 Research and Kagan products, TMT Research offers differentiated insight and data on adoption, innovation and disruption across the telecom, media and technology markets, backed by a global team of industry experts, and delivered via a range of syndicated research, consulting and go-to-market services, and live events.

CONTACTS

Americas: +1 800 447 2273

Japan: +81 3 6262 1887

Asia Pacific: +60 4 291 3600

Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence

www.spglobal.com/en/enterprise/about/contact-us.html

Copyright © 2023 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.