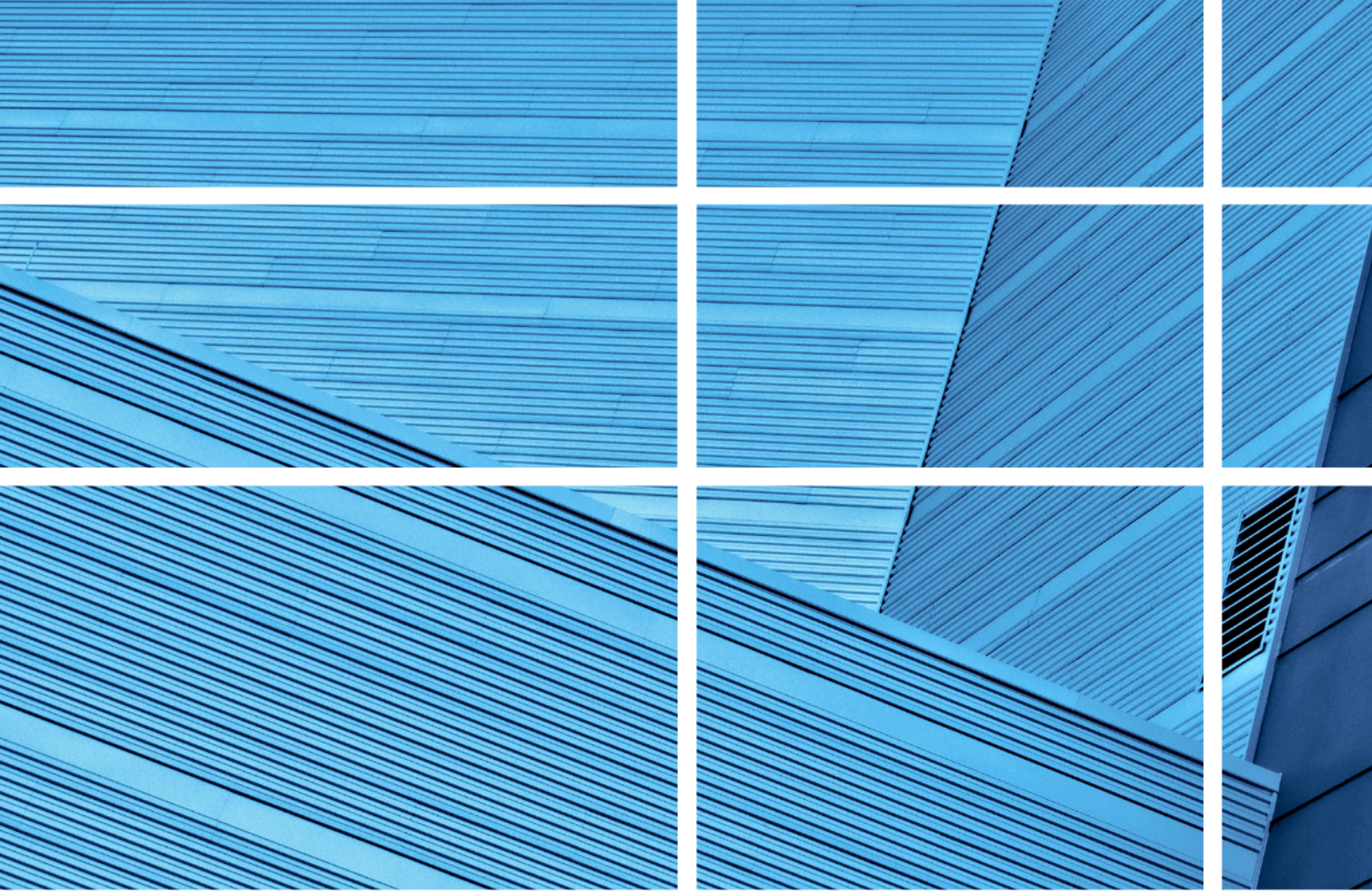


451 Research Discovery Report

January 2025

Platforms or stand-alone tools

What do SecOps teams prefer, and why?

S&P Global
Market Intelligence

©Copyright 2025 S&P Global. All Rights Reserved.

Commissioned by

SentinelOne

Table of contents

Introduction 3

Key findings 4

Platforms, or a collection of tools: Trends and trajectory 5

Figure 1: Distribution of respondents' self-categorization between stand-alone SecOps tools vs. integrated platforms 6

Case in point: SIEM 6

Figure 2: Adoption of SIEM and number of SIEM vendors in use 7

Driving the trend: Integration is essential, regardless of preference 8

Figure 3: For SecOps organizations tending more toward platforms, integration is a priority, both within multifunctional products and with third-party tools 8

Figure 4: Organizations oriented toward stand-alone SecOps tools prize integration capability and adaptability 10

Modernized architecture is key to enabling innovation 11

A forcing function for modernizing SecOps architecture 11

Figure 5: Organizations see value in new approaches to security data management such as security data lakes 12

What discourages organizations from embracing collections of tools or integrated platforms? 13

Figure 6: Factors discouraging organizations from pursuing a best-of-breed strategy of tools from multiple providers 13

Figure 7: Factors discouraging organizations from investing in a multifunctional single-vendor security platform 14

Figure 8: Trust and confidence in the provider is the key aspect of the relationship influencing purchasing decisions 15

Conclusions 16

Methodology and demographics 16

About the author 17

Introduction

One of the most visible trends in cybersecurity technology is the emergence of platforms that offer capabilities across multiple technology segments. This is hardly a new theme. Vendors have been expanding their feature sets organically as well as through acquisitions for as long as there has been demand, and when the opportunity arises to capitalize on consolidation, they have often sought to unify their products. When a vendor's offerings integrate data and functionality directly in the technology such that segments within a larger product can share data, offer expanded insight, and unify processes, workflows and actions holistically, such a product more truly meets the definition of a technology platform.

In security, major contenders have been building offerings around key "centers of gravity" where synergies across segments are evident. One of the most visible such centers today is in security operations (SecOps), where threat detection and response segments are united in broader offerings with security automation, log management, threat intelligence and other adjacencies. Client appetite for these consolidated offerings has led to significant success for some vendors and pushed platform strategies even further, intersecting increasingly with both proactive posture management and reactive detection and response in new areas such as security for cloud-native environments, another emerging center of gravity.

At the same time, many organizations maintain — and even expand — their inventory of stand-alone tools that each serve a more focused purpose. Sometimes, this toolset collection is the result of innovation in a newly established field, or the emergence of new functionalities that become market segments in their own right. For example, endpoint detection and response (EDR) technology became an anchor for the evolution of broader SecOps platforms that rose to challenge existing incumbents. In other cases, stand-alone tools may be a vestige of persisting legacy functions that have not been incorporated in more broadly integrated products (or for which an organization has not yet updated its toolset). But they may also be a manifestation of tools that are best fitted for a given purpose in a given organization — sometimes regarded as "best of breed" in that domain.

If there are reasons for both approaches, where do SecOps teams fall along a spectrum between a collection of stand-alone tools and a unified platform of technologies? Does platform adoption have significant or growing momentum? Do stand-alone tools prevail? Do practitioners see their organizations maintaining an even mix of both?

To gain a sense of the status and trajectory of the SecOps technology market, we asked these and related questions in a survey conducted in the second half of 2024, among 606 cybersecurity practitioners in midsized to large organizations in North America who have hands-on familiarity with SecOps tools in detection, response and associated fields.

We found that cybersecurity platforms combining multiple functionalities represent the predominant approach to SecOps tech among more than two-thirds of organizations surveyed, and additional respondents are moving in that direction. Reputation for product effectiveness is a high priority, and among those who emphasize their provider relationships as a factor in vendor selection, trust and confidence in the provider is the most significant aspect of that relationship.

Regardless of whether respondents embrace platforms, another theme is even more prevalent: Organizations prioritize the ability to integrate multiple SecOps toolsets and their data throughout their environment, no matter how those tools are deployed. This highlights the importance of emerging approaches to data integration for SecOps tech for *any* organization — for example, respondents almost universally acknowledge the value of user-friendly methods to connect individual tools to data and to each other, and of architectures for integrating data across tools, such as data fabrics and data lakes.

Such capability will be an essential enabler for the emerging next phase of SecOps tech: the integration of AI functionality that enhances and accelerates threat detection, response and security automation — an evolution that depends on ready access to data correlated across multiple tools, inputs and paths to action.

Key findings

- Among all respondents, 70% say their organizations are more oriented toward SecOps platforms. Another 8% see themselves moving in that direction within the next three years.
  - Reputation for effectiveness among security practitioners is in the top 5 criteria for vendor selection among all respondents, and in the top 4 for those respondents who see their organization tending more toward SecOps platforms.
- Regardless of whether respondents see themselves as more platform-oriented, integration is the value most often cited across all respondents, as seen in their answers to a variety of questions:
  - More than two-thirds (69%) of all respondents integrate their SecOps tools to some degree; 26% invest significantly in this integration.
  - The top criterion for vendor selection among those more oriented toward SecOps platforms today is ease of integration with third-party technologies (38%), on par with the quality of integration across features and function segments within the vendor's own offering (37%).
  - Ease of integration with third-party technologies is equally significant as the top criterion for vendor selection among those who are more oriented toward a collection of multiple SecOps tools (38%).
  - The burden of integrating disparate tools is the top factor discouraging the use of collections of tools — and thus a key motivator for embracing data integration strategies, as well as a reason for adopting platforms that offload this burden for the customer.
- Nine out of 10 respondents cite the need to invest in architectures to better integrate and manage security data:
  - Eighty-eight percent of all respondents identify the need to invest in data integration or a "data fabric" for their SecOps toolset.
  - Eighty-seven percent recognize the need for new approaches to security data management such as a data lake.
- Such architectural investment may be essential to make the most of emerging innovation in SecOps tech, such as generative AI:
  - More than half (52%) fear that the adoption of generative AI for SecOps will require a greater degree of maturity in technology implementation than they currently have (or think they can achieve), ahead of concerns about sensitive data exposure, unknown risks, or costs that outweigh benefits. This introduces opportunity for providers for whom architectural maturity is integral to their offering.
- Among the barriers to platform adoption are availability, performance or security risks arising from the wide adoption of a specific vendor (58%).
  - Platform vendors must invest in mitigating these risks and ensure consistent and reliable customer outcomes. For those respondents who prioritize the relationship with their current provider as a criterion in vendor selection, trust and confidence in the provider is the most-cited influential aspect of that relationship (59%).

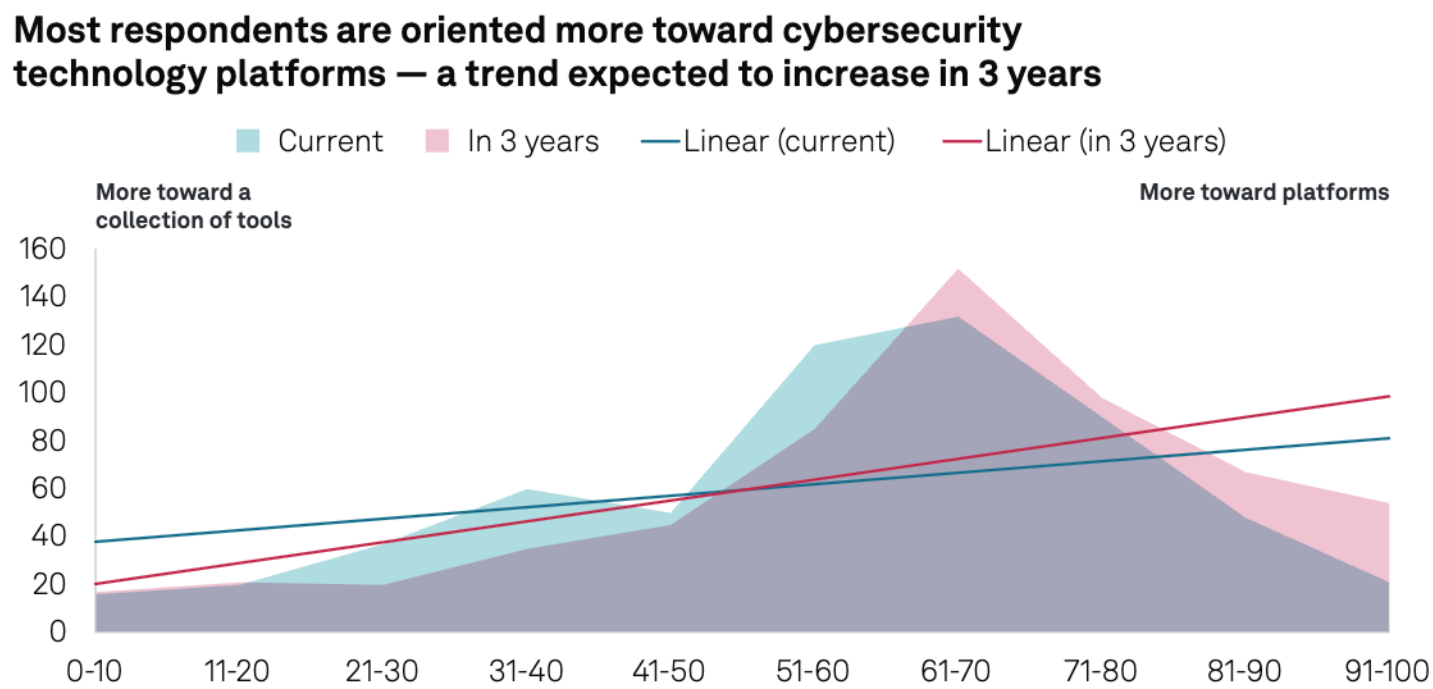
Platforms, or a collection of tools: Trends and trajectory

There are persuasive drivers for investing in integrated, multifunctional cybersecurity technology platforms, just as there are for investing in tools built for a specific focus. While platforms consolidate and should offer the advantage of native integration across components, stand-alone tools may offer capabilities not found elsewhere, or may be preferred by a given organization for a host of other reasons — or they may just be the status quo that has not yet been displaced. So where do security organizations see themselves falling between these two approaches to technology?

In asking this question, we anticipated that answers would not be absolute. Among SecOps teams, we expected that most would see themselves as somewhere along a spectrum between a collection of stand-alone tools and exclusively using platforms that integrate functionality across segments such as threat detection and response, log management, automation, threat intelligence and related fields. What we were after was a sense of the prevalence of these two paradigms, as perceived by respondents. Accordingly, we asked respondents where they saw themselves along this spectrum currently, as well as where they expected to be within the next three years.

We asked respondents to choose the point along a linear scale between these two extremes that best represented their organization, and measured this position on a scale of 0-100. Of the 594 survey participants that responded, the distribution of responses — both for where they are today and where they see themselves in three years — is shown (see Figure 1) by decile along the 0-100 scale. (For ease of reference and the purposes of this report, we refer to respondents to the right of the midpoint of this scale as tending more toward platforms, and those to the left as tending more toward stand-alone tools or a collection of tools from multiple providers, using this placement to group these respondents accordingly in characterizing additional findings.)

Figure 1: Distribution of respondents' self-categorization between stand-alone SecOps tools vs. integrated platforms



Q. Where would you say your organization falls between the two points below, based on your current approach to SecOps technologies today?
Q. Where would you say your SecOps technology investments will fall between the two points below going forward (in three years from now)?
Base: All respondents (n=594).
Source: S&P Global Market Intelligence 451 Research security operations custom survey, 2025.

Nearly three-quarters (70%) say their SecOps organization is oriented more toward multifunctional security platforms. Only 30% place themselves more toward a collection of tools for specific functionalities.

Projecting ahead three years, the share who expect to orient toward platforms increases to 78%, while those who expect to orient toward a collection of tools decreases to 22%.

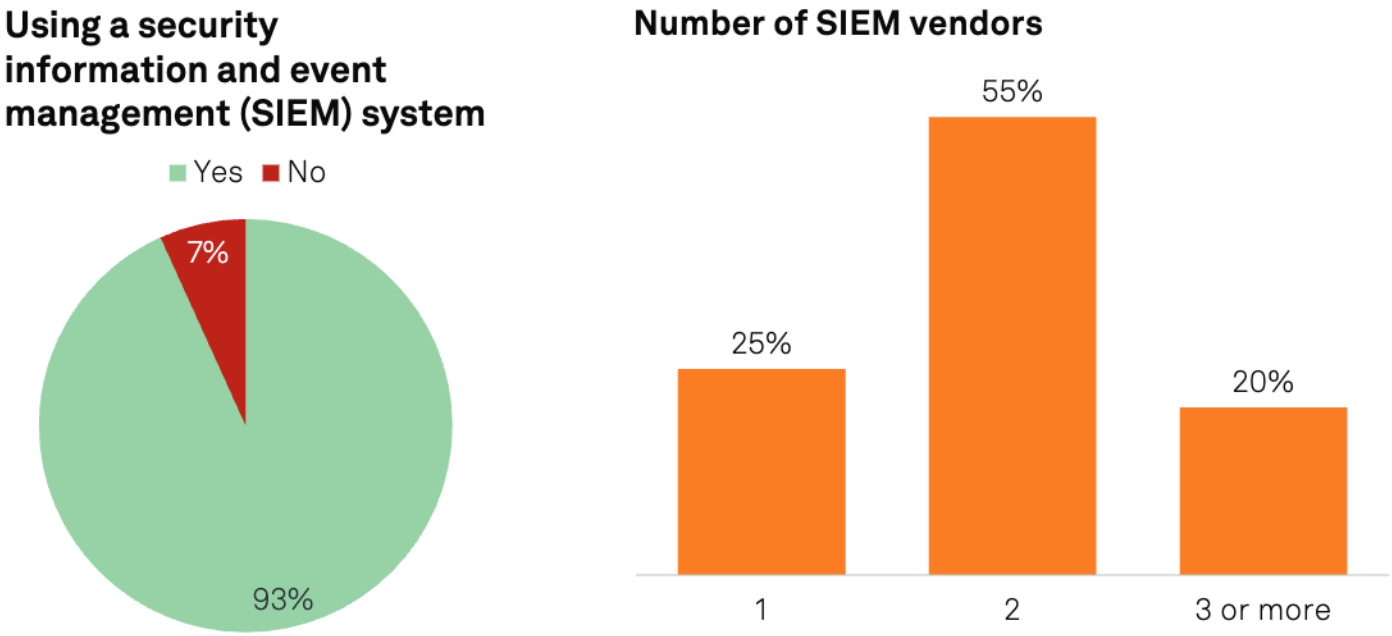
Case in point: SIEM

A broad push among organizations to consolidate investment and reduce the number of suppliers, particularly when multiple suppliers serve the same or similar use cases, factors into the trend. Security information and event management (SIEM) offers a salient example. Nearly all (93%) respondents currently use SIEM, and their primary use cases may surprise some who see SIEM as primarily supporting compliance. For example, we asked respondents to rate the usefulness of SIEM for specific use cases on a numeric scale, and their averaged responses indicate that they see threat detection as the most useful application, followed (in order) by threat hunting, regulatory compliance, incident investigation and log management. This diversity of application speaks to the attraction of SIEM as a center of SecOps platform gravity, a role that it had played consistently up to the increased disruption of SecOps technology markets by extended threat detection and response (XDR).

Regarding the challenges organizations face with SIEM today, the top two responses from those using SIEM are the difficulty of sourcing and retaining the necessary personnel and skills, and the cost of services for deployment and operational management (each cited by 30%). But those are not the only issues with the current SIEM market. In this space, the proliferation of tools includes the proliferation of multiple tools in the *same* technology segment.

The majority of those using SIEM (55%) have subscriptions or licenses from two SIEM vendors, and another 20% have them from three vendors or more. Among respondents who have SIEM, 96% say that all licenses or subscriptions are in use. In some cases, multiple SIEM platforms may be a function of a business having multiple divisions or business units, each with its own preferred technology. M&A is one scenario that can introduce multiple SIEM platforms in the post-acquisition organization. In other cases, SIEM may be included in a new vendor's product portfolio, which may motivate its investigation and use regardless of prior or existing investments. Some SIEM tools may be seen as better purposed for some use cases than others. Movement among providers of XDR platforms to incorporate SIEM functionality such as log aggregation and analysis is fueled by the desire not only to consolidate disparate SecOps segments, but also to unify overlapping investments in the *same* segment where possible and desirable for the customer.

Figure 2: Adoption of SIEM and number of SIEM vendors in use



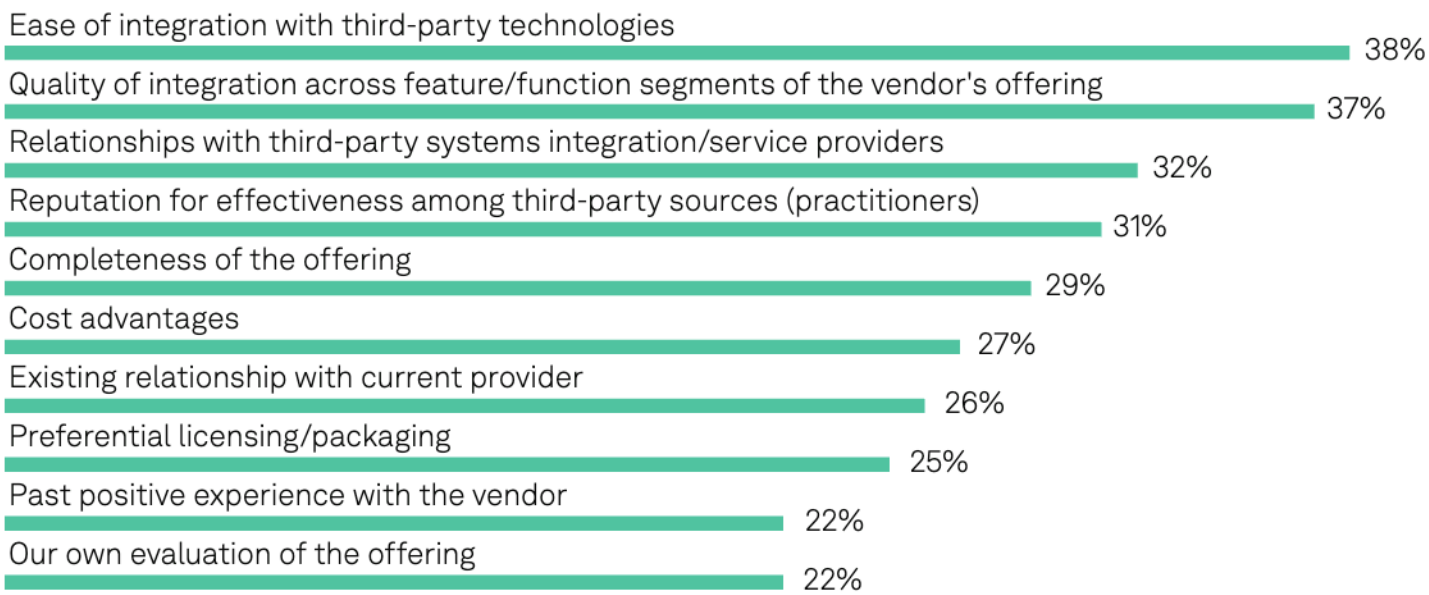
Q. Are you currently using a security information and event management (SIEM) system?
Base: All respondents (n=606).
Q. How many SIEM systems from different vendors do you have subscription(s)/license(s) for?
Base: Respondents currently using a security information and event management (SIEM) system (n=565).
Source: S&P Global Market Intelligence 451 Research Security Operations custom survey, 2025.

Driving the trend: Integration is essential, regardless of preference

Regardless of where respondents place their organization along the continuum between platforms and stand-alone tools, integration across SecOps functionalities stands out as a primary requirement.

For those who say their organization gravitates more toward platforms, we asked about their most important criteria for purchasing multiple SecOps functionalities from a single vendor. In other words, what qualities of a multifunctional platform and its provider matter most in vendor selection? Among this group, ease of integration with **third-party** tools was the most-cited criterion, while quality of integration **within** a single vendor's offering was reported nearly as often (38% and 37%, respectively).

Figure 3: For SecOps organizations tending more toward platforms, integration is a priority, both within multifunctional products and with third-party tools



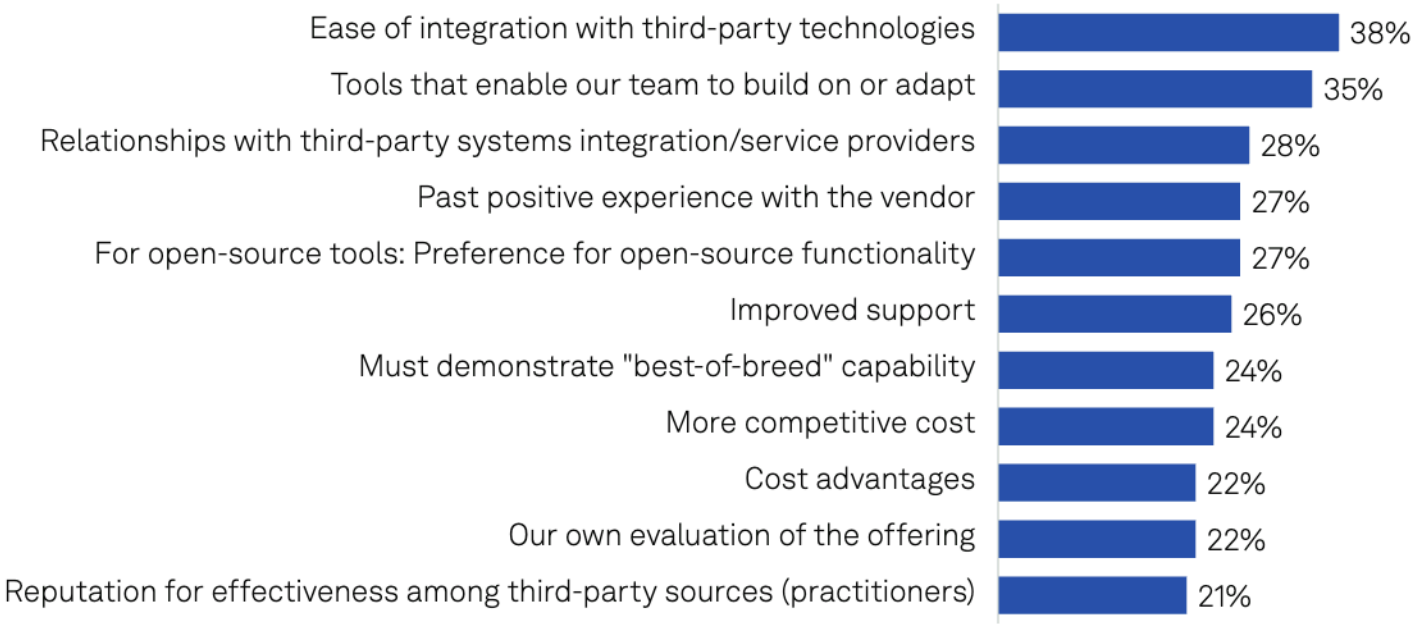
Q. When purchasing multiple SecOps functionalities from a single vendor, what are your most important criteria for vendor selection? Select up to three.
Base: Respondents currently tending more toward platform (n=411).
Source: S&P Global Market Intelligence 451 Research Security Operations custom survey, 2025.

The priority given to integration within a platform as well as with third-party tools speaks to the interest of all respondents in having their SecOps tools work more effectively together. Such a holistic approach to SecOps tooling offers the potential to deliver more effective insight and response across the toolset and eliminate blind spots between technology silos. Platforms appeal to customers in part because of the potential they offer for offloading much of the burden of integration among the functionalities they combine. Platforms further offer maintenance and updating of integrations across functionalities as customer demands — and the threat landscape — change. When offered as SaaS, they can deliver maintenance and updates in real time, with high transparency to customers (provided they do so using practices that reduce risks arising from updates of live targets in production deployments).

Platforms that enable extensibility to third-party tools take this priority even further for the customer. That extensibility acknowledges the reality that virtually every organization will retain some stand-alone or narrowly focused tools that are not part of their preferred platforms. These may represent new or emerging categories not yet integrated with platforms of choice — categories that the platform provider may ultimately embrace if they become valuable enough to the market. Stand-alone tools may be sources of data beyond SecOps technology per se, such as identity management systems that correlate attempted compromise with the user privileges sought. Indeed, they may offer context beyond security, such as business systems that handle high-value data or tangible assets, from which telemetry must be obtained and controls employed to detect and respond to threats.

For those more oriented toward stand-alone tools, we asked a similar question, but one that focused on a "multi-tool" environment: When purchasing SecOps technology tools from multiple vendors, what are your most important criteria for vendor selection? In this group as well, we see a similar priority placed on the ability to integrate. In this case, integration with other tools is the top-rated criterion. This group also emphasizes the ability to customize and combine tools — that is, they prioritize tools that enable them to build on or adapt — a feature valued even more highly than "best-of-breed" capability.

Figure 4: Organizations oriented toward stand-alone SecOps tools prize integration capability and adaptability



Q. When purchasing SecOps technology tools from multiple vendors, what are your most important criteria for vendor selection? Select up to three.
Base: Respondents that see their organization currently as more oriented toward a collection of tools from multiple providers (n=183).
Source: S&P Global Market Intelligence 451 Research Security Operations custom survey, 2025.

This suggests that while these organizations may value the capabilities of individual, independent tools, they also place a high priority on making those tools part of a more holistic environment in which detection, response and supporting technologies yield greater value when brought together.

Modernized architecture is key to enabling innovation

When it comes to SecOps tech, few disruptors have had the impact of AI and machine learning (ML) with their rapid evolution. The promise of AI/ML factors into a larger ambition of SecOps technology providers: to evolve technology more toward "autonomous" security operations. Such a future seems even more likely as AI systems develop the ability to take self-informed action with limited or no human intervention. So-called "agentic AI" is an increasingly visible example of this trend.

Because of generative AI's ability to quickly recognize patterns, correlate learnings from a large volume of data and produce a range of outputs from conversational language to code and other content, survey respondents see a variety of benefits in the application of generative AI to SecOps. Just over half (51%) of all respondents expect to see improved performance in recognizing and mitigating security exposures and threats, and 50% believe it will improve the actionability of threat detection and response. Just under half (49%) see the potential for reducing the burden of integrating findings across multiple tools and techniques, and 47% expect these benefits to improve the productivity of security staff, while 39% expect them to reduce dependence on human correlation. A third (33%) see it reducing "blind spots" in current approaches.

A forcing function for modernizing SecOps architecture

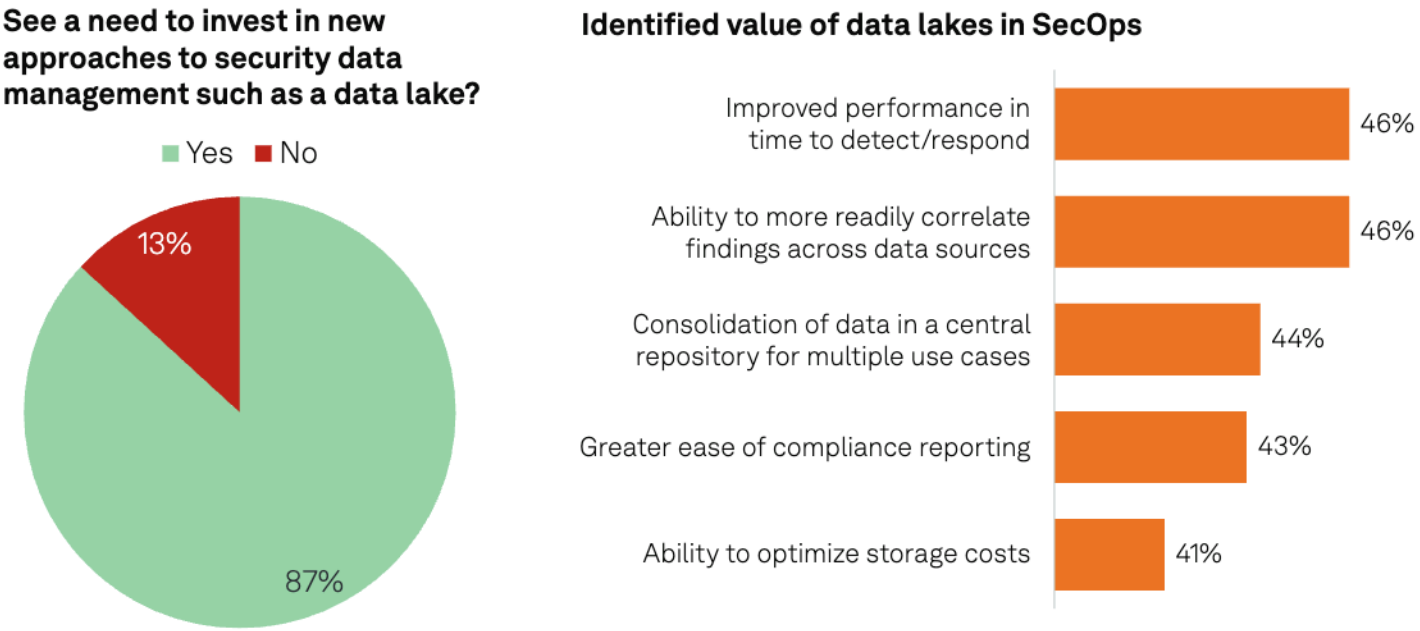
Respondents' biggest concern about embracing generative AI for SecOps is not the risk of sensitive data exposure, or the unknown nature of associated risks, nor that costs will outweigh benefits or that budgets will be inadequate. Their greatest concern is that their environments will not be mature enough to support it (52% of all respondents). Potential exposure of sensitive information beyond the organization's control is also a big concern (50%), followed by risks not yet being known well enough (41%), benefits not outweighing costs (34%) and lack of budget or prohibitive cost (22%).

Respondents are recognizing that to make the most of AI innovation, they must meet requirements in the supporting architecture. Data on which AI can be trained and which it must consume must be made available at sufficient scale to enable AI to perform as expected. These systems must be able to access data, process it and respond with high performance and low latency, all while protecting sensitive information without diluting the impact of results. This again speaks to the high priority that respondents place on integration across tools and functionalities, but it speaks even more to the need for more modern capacity and performance capabilities in the underlying environment.

This recognition introduces an opportunity for platform providers to bring together the architecture necessary to deliver these capabilities through their products. Indeed, the imperative to deliver forward-looking architecture that can support these expectations is a competitive priority. It is not lost on these contenders that security is one of the primary realms where generative AI is expected to yield real benefits. Key aspects of that architecture are the data collection, aggregation, integration and management capabilities required not only for effective SecOps — or even AI — but to enable whatever may come next in the evolution of the SecOps tech stack. Because cloud technologies can embrace economies of scale as well as performance supported by a high degree of responsive elasticity, much of today's forward-looking innovation in SecOps technology is necessarily cloud native.

Survey respondents are already aware of the architectural alternatives available to support transformation in SecOps technology. Given the imperative for integration across all respondents, it is not surprising that 88% acknowledge the need to invest in data integration or a "data fabric" for their SecOps toolset to make the most of available context for data enrichment, threat recognition and response, forensic and historical analysis, meeting compliance requirements, better integrating more effective workflows, and a variety of other use cases. A similarly large majority (87%) recognize the need for new approaches to security data management such as a data lake, with explicit value seen in the investment.

Figure 5: Organizations see value in new approaches to security data management such as security data lakes



Q. Do you see a need to invest in new approaches to security data management such as a data lake?
Base: All respondents (n=606).
Q. What are the values you see in investing in a data lake for SecOps?
Base: Respondents answering "yes" to the previous question (n=526).
Source: S&P Global Market Intelligence 451 Research Security Operations custom survey, 2025.

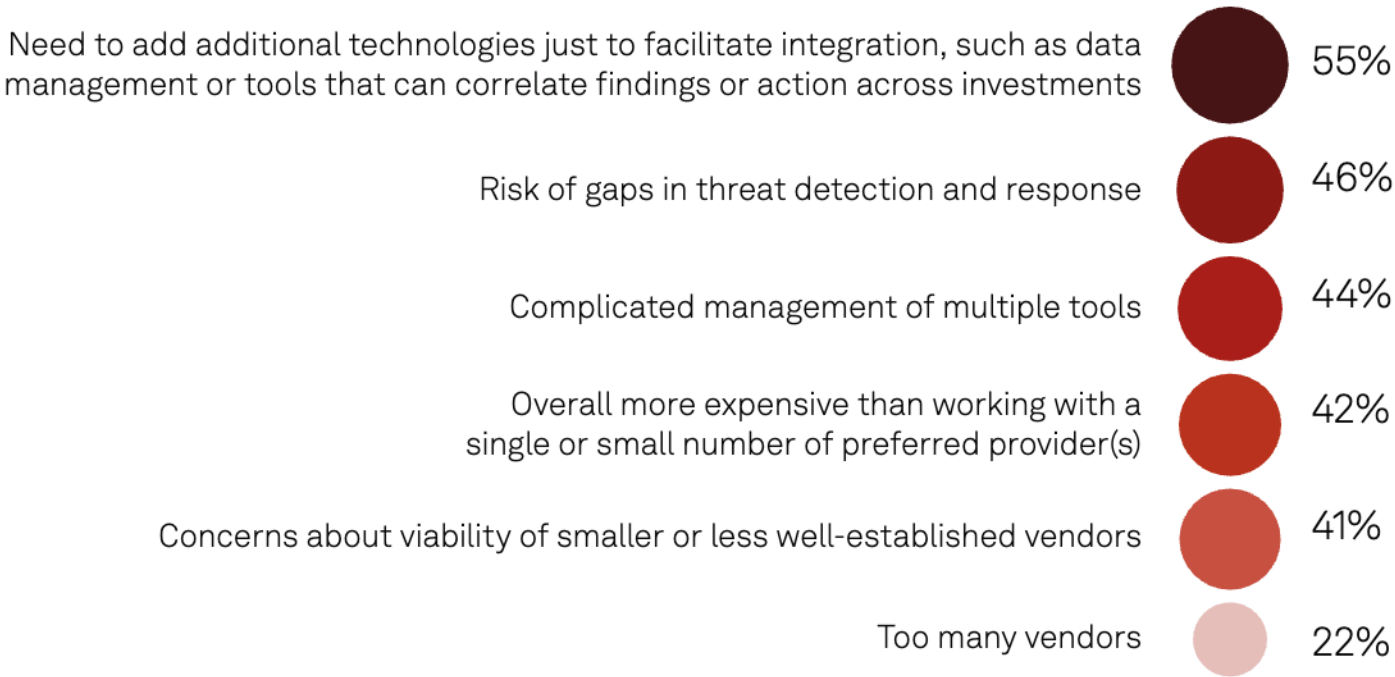
Perhaps surprisingly, while storage costs have often been emphasized as a motivator for moving toward more affordably scalable options such as data lakes, cost optimization is the lowest-ranked value cited by survey respondents. More important to them are improved response performance, findings more readily correlated across data sources and the ability to consolidate their security data, all of which can capitalize on the scale and performance advantages of cloud-native architectures.

Note that these are findings from all respondents, meaning that platform providers have an opportunity to capitalize on these priorities for all current or potential customers, regardless of where they fall on the spectrum of platforms vs. stand-alone tools. The platform approach further extends forward-looking capability to help customers realize greater benefit from consolidating their SecOps toolsets, while at the same time potentially extending the values of integration focused on more modern data architectures to all tools in the customer's portfolio.

What discourages organizations from embracing collections of tools or integrated platforms?

Given the emphasis placed by all respondents on integration across SecOps technologies, it is hardly surprising that the primary discouragement to embracing the "collection of tools" approach is the burden of making a whole out of the sum of several parts.

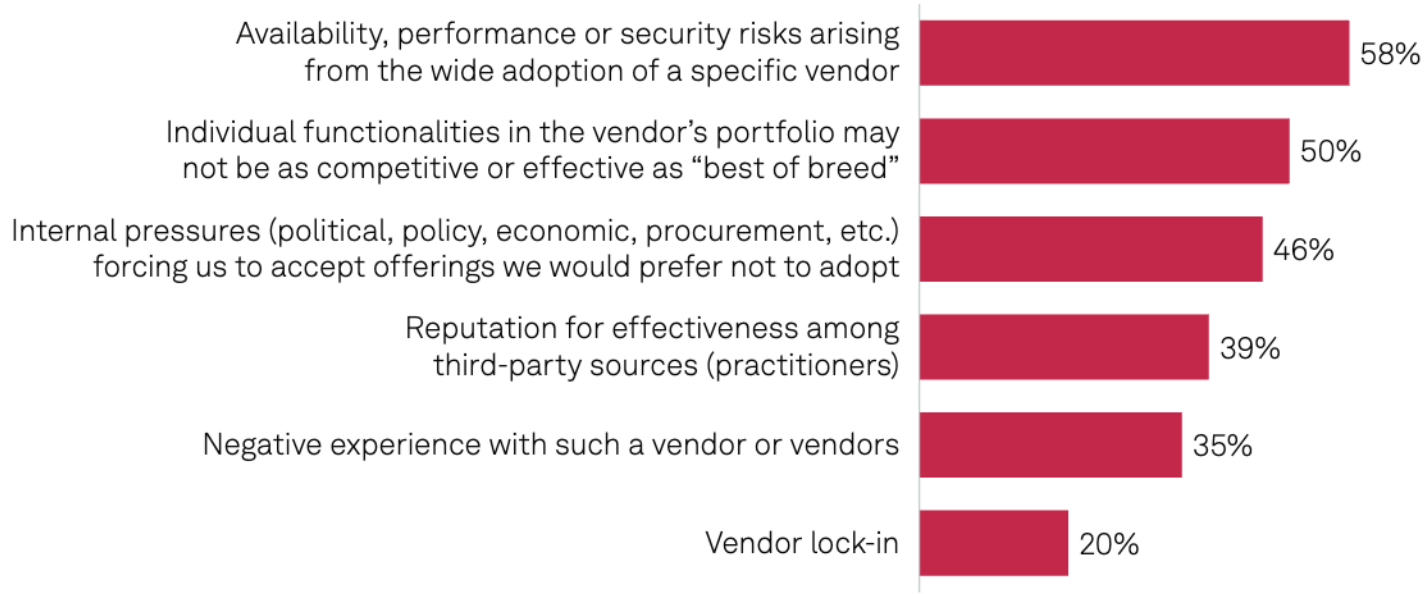
Figure 6: Factors discouraging organizations from pursuing a best-of-breed strategy of tools from multiple providers



Q. Which of the following would discourage you from pursuing a "best of breed" strategy of tools from multiple providers [versus a single-vendor security "platform" in which the vendor integrates its own products]?
Base: All respondents (n=606).
Source: S&P Global Market Intelligence 451 Research Security Operations custom survey, 2025.

By integrating functionalities, closing gaps between them and reducing management complexity and cost, platform providers have an opportunity to address these concerns directly, but there are inhibitors to platform adoption as well.

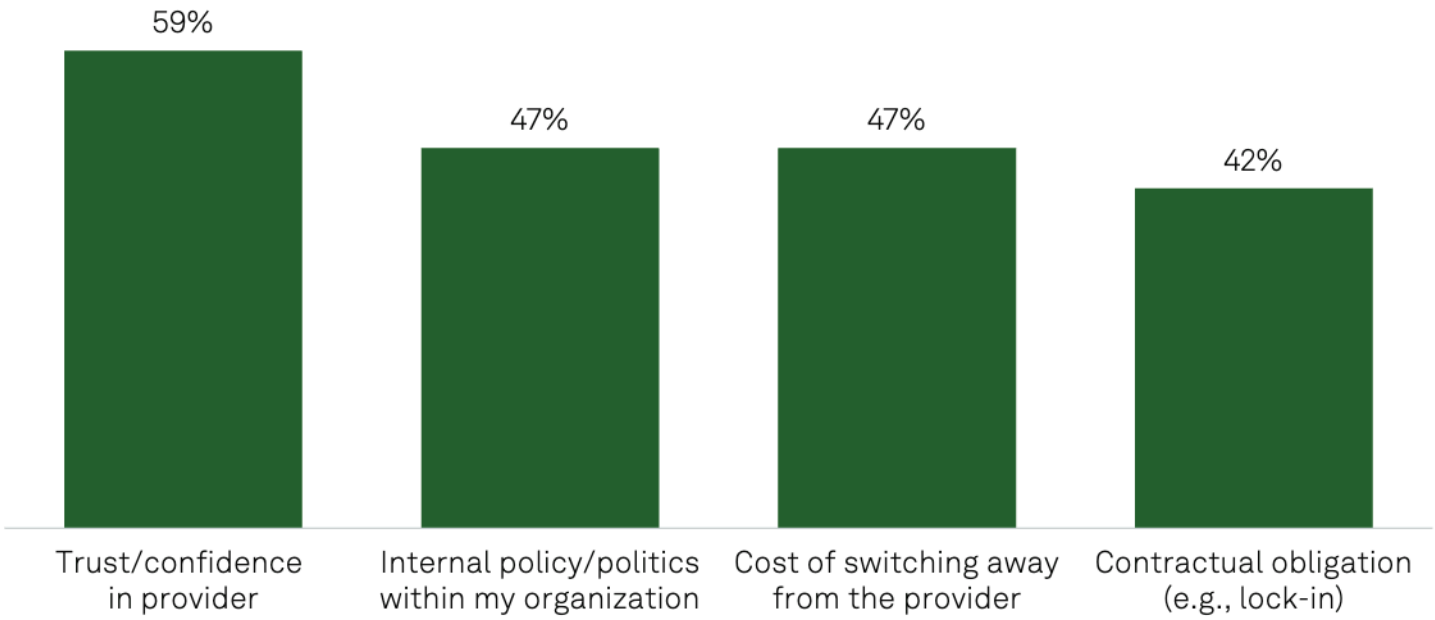
Figure 7: Factors discouraging organizations from investing in a multifunctional single-vendor security platform



Q. Which of the following would discourage you from pursuing a strategy of investing in a single-vendor security "platform"?
Base: All respondents (n=606).
Source: S&P Global Market Intelligence 451 Research Security Operations custom survey, 2025.

It is not lost on practitioners that a concentration of functionality among a smaller number of vendors may also introduce a concentration of risk. For respondents to this survey, this is a greater concern than a platform not providing best-of-breed capability. Platform providers must recognize their obligation to address these concerns and work closely with their customers to mitigate them by delivering consistent and reliable outcomes that justify the investment. This is reflected in the top response from respondents who cite a current provider relationship as an important criterion for vendor selection: Trust and confidence in the provider is the most significant aspect of that relationship in the decision to purchase from them.

Figure 8: Trust and confidence in the provider is the key aspect of the relationship influencing purchasing decisions



Q. Which of these aspects of your current provider relationship are most significant to purchasing from them? Select all that apply.
Base: Respondents who indicated that an existing relationship with current provider is an important criterion for vendor selection (n=146).
Source: S&P Global Market Intelligence 451 Research Security Operations custom survey, 2025.

Conclusions

With 70% of respondents more oriented toward SecOps platforms today and an additional 8% moving in that direction within the next three years, security organizations expect a great deal from platform providers. Those that best meet these expectations while mitigating risks and concerns stand the best chance of making the most of the opportunity.

It is important to recognize that today's successful security platform may have begun as yesterday's emerging stand-alone tool. This elevates the recognition that organizations often embrace such narrowly focused tools for good reason: They could be tomorrow's disruptors. Recall that the ability to build on and adapt a tool is one of the top selection criteria for organizations purchasing multiple tools from a variety of security technology providers.

Today's generation of security platforms is not the first. It is the most recent example of success being predicated on disruptive innovation — in this case, more modern threat detection and response technology extended to the source of telemetry, which shook up prior techniques predicated on centralized data collection and correlation. This means that in the modern security operations center (SOC), stand-alone or narrowly focused tools that deliver specific results as well as platforms that demonstrate their breadth of capability have become recognized for their value in working together for the good of the whole.

Architectures that succeed in making the most of this combined investment and reducing complexity in the toolset where warranted may well be a determinant in what the SOC becomes tomorrow. Providers that succeed will recognize disruption today and embrace it competitively, while at the same time placing the customer first, mitigating their risks in embarking on the journey, and justifying the trust and confidence they have placed in their preferred providers.

Methodology and demographics

This report is based on an online quantitative survey involving 606 full-time employees in North America, focusing on SOC and threat detection and response. Respondents were screened based on their responsibilities and roles, and included security analysts, threat researchers and chief information security officers. The survey targeted a diverse representation of industries, including a focus on finance (17%), energy (17%) and technology (20%). All respondents were from companies with 500 or more full-time employees and annual revenues of $50 million or more. Respondents were predominantly from the United States (77%) and Canada (23%).

SentinelOne (NYSE:S) is a global leader in AI-powered cybersecurity, empowering the world to run securely with enterprise-wide protection. The Singularity™ Platform brings all your data together to eliminate risk and protect the future. Watch a demo of the Singularity Platform. To learn more about SentinelOne and the Autonomous SOC: sentinelone.com.

About the author

Scott Crawford

Research Director, Information Security

Scott Crawford is research director of the Information Security channel at S&P Global Market Intelligence 451 Research, where he leads the industry analyst team covering innovation, disruption and strategic players in cybersecurity and cyber risk. Scott joined S&P Global through its 2019 acquisition of 451 Research, where he has led the Information Security channel since 2015.

In addition to directing the Information Security channel's research efforts, Scott covers forces and events shaping cybersecurity. He maintains a focus on areas including security operations, cyber risk management, the intersection of AI/machine learning and cybersecurity, and related interests.

As a practitioner, Scott was the first information security officer for the Comprehensive Nuclear-Test-Ban Treaty Organization's International Data Centre in Vienna, with a background including systems and security management at the University Corporation for Atmospheric Research in Boulder, Colorado. His private-sector experience ranges from startups to leading industry players such as IBM, where Scott was a senior strategist with IBM Security.

Scott holds a Bachelor of Arts in molecular, cellular and developmental biology from the University of Colorado and a postgraduate Master of Science from the University of Salford (UK), with additional graduate study in telecommunications at the University of Colorado and in information systems at the 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

At S&P Global Market Intelligence, we understand the importance of accurate, deep and insightful information. Our team of experts delivers unrivaled insights and leading data and technology solutions, partnering with customers to expand their perspective, operate with confidence, and make decisions with conviction.

S&P Global Market Intelligence is a division of S&P Global (NYSE: SPGI). S&P Global is the world's foremost provider of credit ratings, benchmarks, analytics and workflow solutions in the global capital, commodity and automotive markets. With every one of our offerings, we help many of the world's leading organizations navigate the economic landscape so they can plan for tomorrow, today. For more information, visit www.spglobal.com/marketintelligence.

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 © 2025 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.