451 Research | BLACK & WHITE PAPER

New Survey Reveals Small and Mid-Size Enterprises Are Making Big Strides in Cybersecurity, But Big Decisions Loom Ahead

THE CLOUD, SCALABILITY AND COMBATTING NEWLY EMERGING THREATS

COMMISSIONED BY

ARMOR™

OCTOBER 2018

About this paper

A Black & White paper 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 THE AUTHOR

AARON SHERRILL

SENIOR ANALYST

Aaron Sherrill is a Senior Analyst for 451 Research covering emerging trends, innovation and disruption in the Managed Services and Managed Security Services sectors.

Introduction

Historically, cybersecurity has been a lower priority for most small and medium-sized enterprises (SME). While most have had basic security controls in place such as firewalls and antivirus products, cybersecurity has not been an area of great concern. For years, SMEs operated under the notion that they were too small to be a target for cybercrime and had too much faith in a few, often outdated, security tools. Lacking an understanding of the threats their organizations faced, many unwittingly put their companies, employees and customers at risk. But more recently, many SMEs have shown an increased awareness of the growing threat landscape and the potential impact that a security breach could have on their organizations. As a result, many SMEs have invested significant efforts and resources toward improving their cybersecurity posture.

451 Research recently conducted a custom survey targeting 250 SMEs (250-5,000 employees) to gain a better understanding of the state of cybersecurity within these organizations. We asked the executives, directors and IT/security directors at these SMEs about the current state of cybersecurity in their organizations, the security initiatives they have planned, the challenges they face and their utilization of security as a service (SECaaS). This paper examines the advancements SMEs have made toward improving their cybersecurity posture, their continuing challenges, and the path many are taking to better position their organizations to contend with a dynamic and expanding cyber threat landscape.

Key Findings

- 89% reported that their organization has a single executive leader (e.g., CISO, CSO, VP of InfoSec) whose primary responsibility is information security.
- More than 80% of SMEs said they are increasing their security budgets by an average of 14% for the coming year.
- SMEs expect to spend more of their budgets on security tools delivered from the cloud while decreasing spending on people and commercial off-the-shelf software and hardware over the next two years.
- Most SMEs reported performing log analysis with 62% ingesting more than 50% of available log sources – both cloud and on-premises.
- 59% of SMEs said that, on average, they are able to respond to alerts in less than one hour.
- 61% of SMEs reported they have experienced a significant security incident, cyberattack or data breach, and 31% said the event occurred within the last 12 months. However, many respondents said they feel optimistic about their ability to investigate and respond to incidents moving forward.

Ongoing Challenges

- SMEs reported that they are able to investigate more alerts than in the past, but the volume of alerts and ensuing alert fatigue is resulting in more than one-fourth of alerts being ignored.
- SMEs said that competing priorities, lack of resources, a lack of threat intelligence and a lack of automation are hindering their ability to investigate all security alerts.
- 64% of SMEs reported that they are handling cloud security on their own, although they indicated that cloud security is one of the top security challenges for their organizations.
- SMEs are struggling to secure data and applications in the cloud, as well as legacy IT.
- Scaling security operations and managing the complexity of protecting an expanding and dynamic attack surface is a significant challenge for SMEs.

SMEs Are Making Substantial Progress

An internet search on the terms 'cybersecurity' and 'SME' reveals disheartening results. Website after website and article after article paint a picture of how ill-prepared, underfunded and unknowledgeable SMEs are when it comes to cybersecurity. Contrary to many of those sources, however, the SMEs that participated in our survey painted a more positive outlook; they reported that they have been able to make substantial strides and improvements in securing their organizations.

These improvements start at the top with executive leadership. Eighty-nine percent of the survey respondents reported having a single executive leader (e.g., CISO, CSO, VP of Information Security) whose primary responsibility is information security. This is a significant improvement compared to previous survey data where only 53% of enterprises reported having an executive leader solely responsible for security. Having a security leader on the executive team is crucial because a lack of security leadership has been deemed as a major factor contributing to some of the largest breaches on record.

Not surprisingly, companies in regulated industries such as finance/banking, insurance, public utilities, and telecommunications were more likely to have a security executive in place. Healthcare service organizations, however, are trailing other regulated industries; more than 20% of the survey respondents in the healthcare industry reported that they do not have a security leader on their executive team.

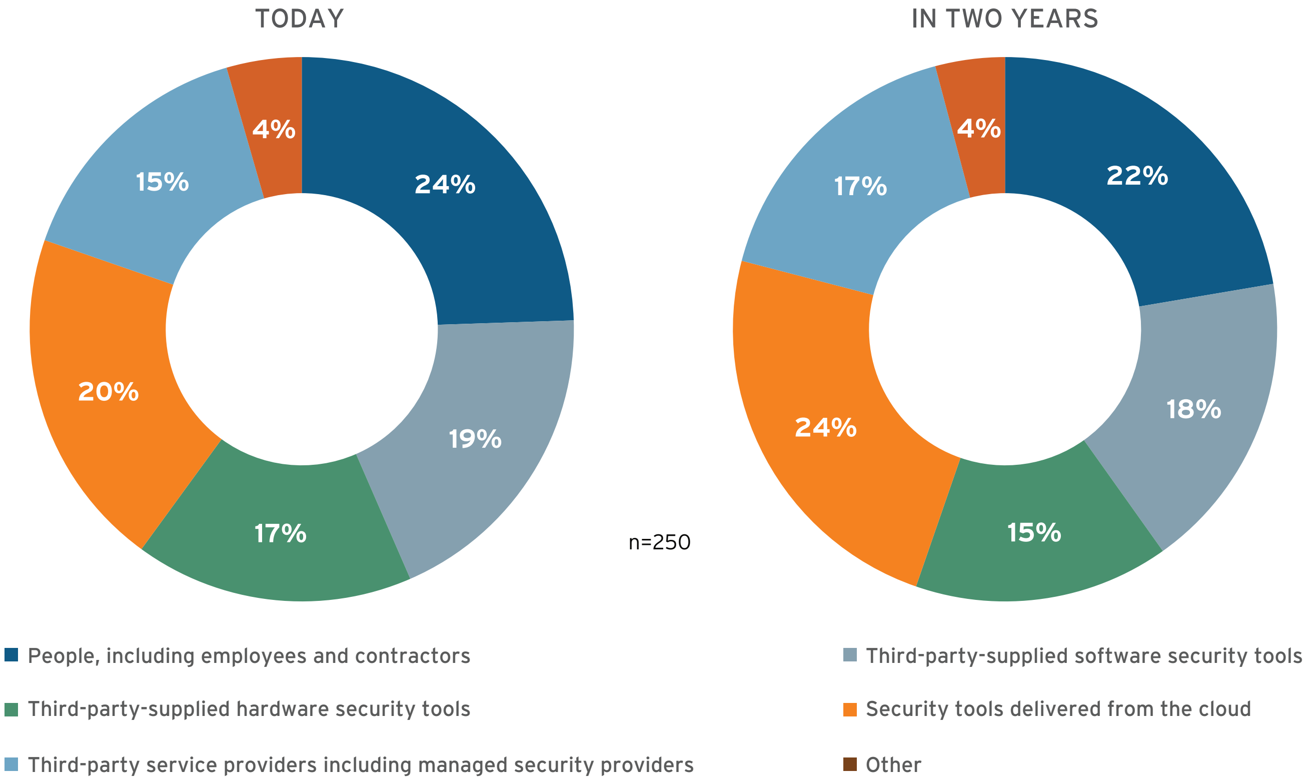
Increased executive support of cybersecurity programs and initiatives is helping fuel SMEs' progress in securing their organizations. Only 6% of SMEs believe that a lack of executive support or organizational politics is a major challenge for their organization when it comes to cybersecurity. This is another significant shift for SMEs. CEOs and executive leadership are becoming more aware of the business impact of cybersecurity and the importance of strategically reducing risk in their organizations. As a result, they have set the tone for cybersecurity 'at the top' and have helped establish a cybersecurity-minded culture that was missing for most SMEs.

According to our research, SMEs are investing more in securing their organizations and protecting their customers' data. More than 80% of the SMEs in 451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook survey said they are increasing their security budgets by an average of 14% for the coming year. As expected, security budgets typically increase as the size of the organization and revenue increase. Today, SMEs are spending the largest percentage of their security budgets on people, although most believe there will be a shift in their security spending over the next two years. SMEs expect to spend more of their budgets on security tools delivered from the cloud and on security service providers while decreasing spending on people and software and hardware security tools. This shift is in line with the trend of reallocating more IT spending in general to operating expenses versus capital expenses.

Figure 1: SME security spending

Source: 451 Research

Q. What percentage of your security spending is allocated to the following categories?



The survey results revealed that SMEs have made several improvements in their security operations. Overall, SMEs are realizing a balance of time and effort across a wide range of security tasks and are no longer consumed by any one area of security. Fundamental tasks, such as patch management, that were once significant challenges for SMEs now rank near the bottom of the security challenges facing their organizations. SMEs also have made significant improvements in log analysis and response efforts, with 62% of the SMEs surveyed reporting that they are ingesting more than 50% of available log sources – both cloud and on-premises.

Although 61% of SMEs said they have experienced a significant security incident, cyberattack or data breach in the recent past, many respondents said they feel optimistic about their ability to investigate and respond to incidents moving forward. Fifty-nine percent said that, on average, they are able to respond to security alerts in less than one hour, and 83% indicated that, on average, they are able to investigate and remediate confirmed threats in less than six hours. This is notable because low incident response time is key to minimizing the effect and severity of a compromise, and although 37% of organizations are taking 1-24 hours to initially review alerts, this still is a significant improvement for these organizations.

SMEs are also shifting from believing 'we are too small to be targeted' or 'we don't have anything of value to hackers' to recognizing they will be breached – it's just a matter of when. SMEs are beginning to realize that with the rapid increase in complex, multi-vector attacks, a breach is no longer a direct indicator of a poor security program. This change in posture is key as SMEs invest in the capabilities and knowledge required to address compromises quickly and efficiently to minimize impact.

The overall improvements in the cybersecurity posture for SMEs have largely been a result of a growing sense of urgency regarding cybersecurity. This awareness is being fueled by new industry and federal regulations, customer demands, partner mandates and board expectations. SMEs are also recognizing (or have experienced) the consequences of cybercrime – operational disruption, reputational damage, financial losses, regulatory penalties and brand damage. With cybersecurity issues on the rise, SMEs are looking to implement a comprehensive security strategy to stay ahead of potentially devastating threats and significantly reduce the ongoing risks they face from cyberattacks.

Challenges

SMEs have made great strides toward increasing the security posture of their organizations, but security is a journey, not a destination, and there are more challenges ahead. SMEs reported that they are now focused on addressing more complex security challenges that require new tools, controls and specialized security expertise.

Securing the Cloud

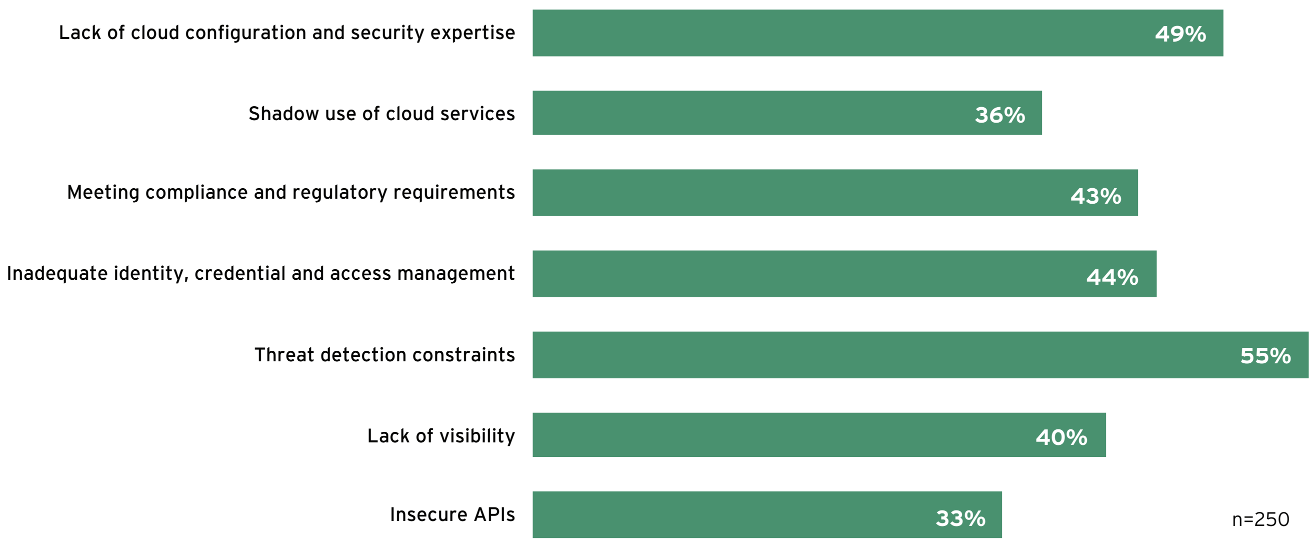
While SMEs are not shifting all of their workloads to the public cloud anytime soon, they are increasingly adopting a hybrid infrastructure model that spans public and private clouds, hosted environments and on-premises infrastructure. The traditional, on-premises IT infrastructure footprint is shrinking as SMEs consume more cloud services. And while cloud services can provide enterprises with the speed, agility and scale needed to propel the business forward, they also create an environment that is increasingly difficult to protect.

Sixty-four percent of SMEs reported that they are handling cloud security on their own, but SMEs also indicated that cloud security is one of the top security challenges for their organizations. The shared responsibility model has helped define SMEs' responsibilities in the cloud, but the demarcation point varies greatly from provider to provider, resulting in misunderstandings, security gaps and complexity.

The survey respondents indicated that threat detection is their biggest challenge in securing the cloud, but they are also concerned about a lack of cloud configuration and security expertise, inadequate identity, credential, and access management capabilities, and meeting compliance requirements. Respondents also indicated that a lack of visibility across cloud services is another challenge because different clouds often require different tools to manage and monitor.

Figure 2: Top security concerns for cloud-based services

Source: 451 Research
Q. What are your top security concerns for cloud-based services?



These concerns become more challenging as the business consumes more disparate cloud services and the traditional corporate network perimeter disappears. Although cloud providers are increasingly adding security controls and capabilities to their platforms, SMEs recognize that they need to overhaul their processes, policies, skills and tools to adapt to this new paradigm.

SMEs have good reason to be concerned because improper configuration of cloud deployments was one of the top root causes of security breaches over the last two years. In addition, most SMEs believe they could have prevented those security breaches if the proper cloud security controls and tools had been in place.

Legacy IT

Although SMEs are increasing their consumption of cloud services, most will continue to maintain a sizable portion of on-premises, traditional IT infrastructure. Much of this on-premises infrastructure is the consequence of legacy applications and systems that are not cloud-ready. Legacy technologies are one of the top security challenges for SMEs.

Legacy applications and systems are often no longer supported by the vendors, which results in security vulnerabilities that go unaddressed, leaving systems vulnerable to attack and exploits. These unpatched systems can provide cybercriminals with a pivot point to attack other, more valuable systems or even partners and customers. Resolving these vulnerabilities and securing legacy technologies is a complex, time-consuming and expensive practice.

Legacy technologies tend to lack the built-in security controls and safeguards that their modern counterparts typically possess. It is not uncommon for legacy systems to lack basic security mechanisms such as individual logins and audit trail logging, as well as more advanced capabilities such as encryption. Legacy applications can be difficult to update in response to emerging security and compliance requirements. Combined with manual processes and the inability to adapt to regulatory requirements, legacy systems and applications are creating a compliance nightmare for SMEs.

Regardless of the security posture of these environments, traditional on-premises infrastructure, legacy environments and cloud infrastructures have different security challenges. SMEs struggle with providing a unified security model for these disparate environments and architectures. The result is a variety of redundant, single-purpose tools that lack integration, which creates inefficiencies, management complexity and unnecessary costs.

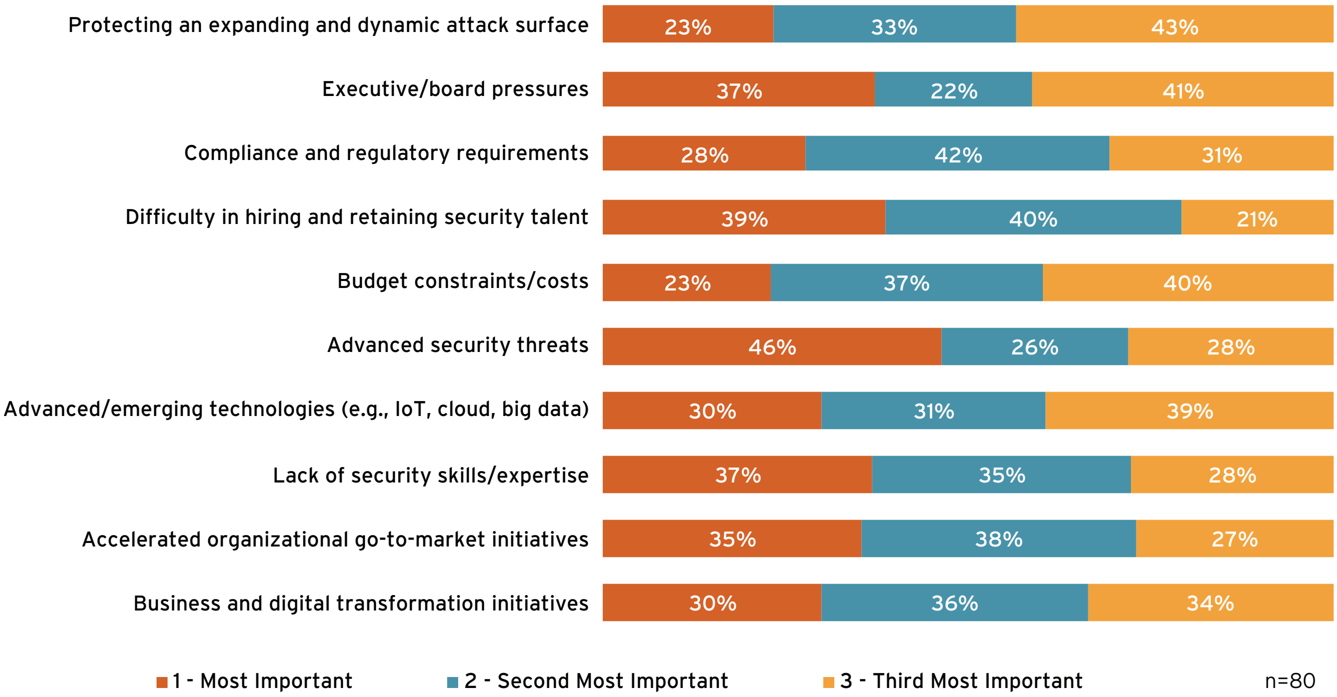
Detecting and Responding to Advanced Threats

Respondents reported that detecting and stopping advanced and emerging threats is the biggest challenge facing their organizations. Advanced threats are growing at an increasing rate and are continually changing in form, function and sophistication. Traditional, single-vector defenses and legacy security controls provide limited protection against these modern, adaptive threats.

Figure 3: Drivers influencing security decisions

Source: 451 Research

Q. What drivers or pressures in your organization have the most influence on security decisions and direction? Please select the top three in order of importance.



At the same time, cybercrime is becoming easier to conduct at scale, leveraging some of the same technology that enterprises are adopting for digital transformation initiatives – automation, orchestration and artificial intelligence capabilities such as machine learning. Attackers are leveraging clouds and containers to launch distributed, scalable strikes against enterprises, enabling attacks at an unprecedented rate and magnitude.

Just like their larger enterprise counterparts, SMEs are facing attacks from every direction. They must protect against attacks targeting multiple vectors, targeted attacks, attacks against operational technology, and attacks targeting suppliers and supply chains. SMEs must also fight attacks spreading fake news and disinformation, as well as attacks targeting IoT, applications and business processes. Simple business-email-compromise attacks are wreaking havoc while cryptoware and mobile malware continue to surge.

As a result, SMEs are shifting cybersecurity tactics, moving from an emphasis on protection and prevention to detection and response. They are focusing on attacks that cannot be prevented and detecting them as quickly as possible. But this shift often results in a greater number of events and alerts that must be interpreted and evaluated. As the amount of data grows, these tasks become overwhelming for security teams, thus hindering the detection capabilities and putting their organizations at risk.

Scale and Complexity

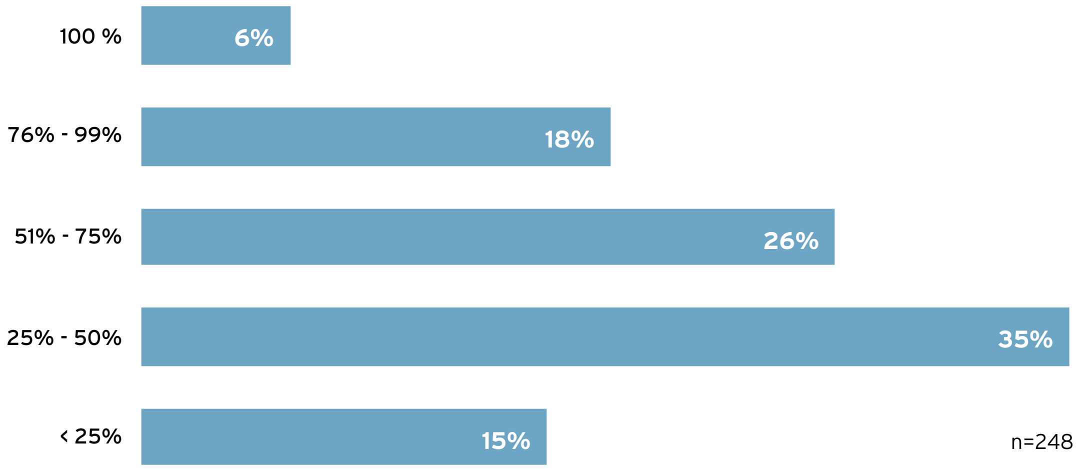
There is an underlying theme to many of the challenges facing SMEs today that centers on their ability to scale security operations and their ability to manage the complexity of protecting an expanding and dynamic attack surface. In each of the top security challenges facing SMEs – securing the cloud, legacy IT, and threat detection and response – scale and complexity are outpacing the capabilities of most SME security teams.

Although SMEs have made great strides in their ability to gather security data from logs and have lowered the average time to respond to alerts, few are able to investigate more than 75% of the alerts their organization generates each day. As they continue to adopt newer technologies and platforms such as cloud, IoT and containers, the number of alerts will continue to grow as will the number of alerts that are ignored.

Figure 4: Percentage of alerts investigated

Source: 451 Research

Q. Approximately what percentage of alerts does your team or service provider investigate each day?

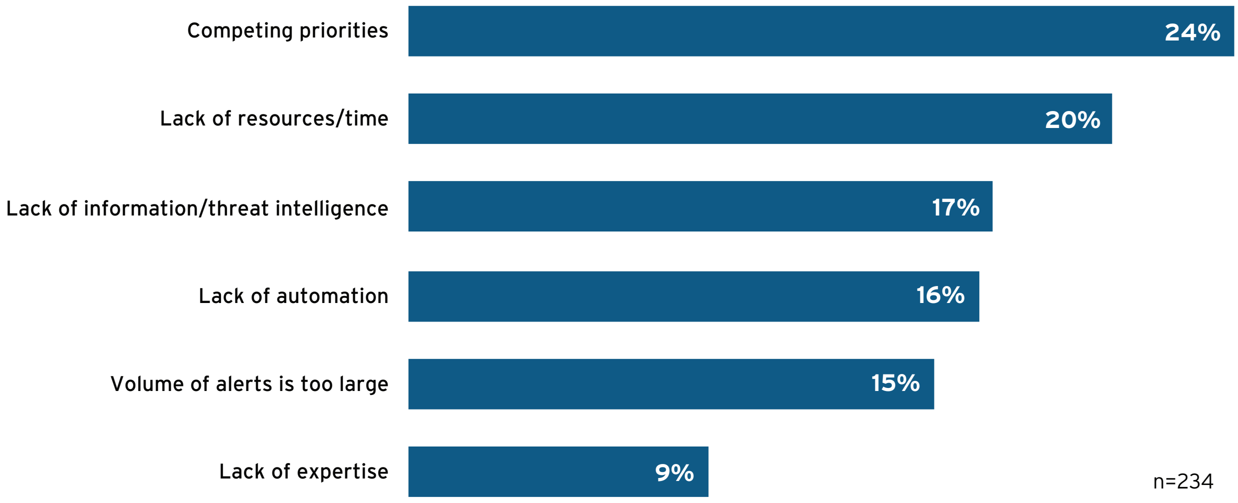


Respondents reported that competing priorities, lack of resources, a lack of threat intelligence and a lack of automation are hindering their ability to investigate all security alerts. They also indicated that security tool silos make it difficult to correlate and analyze events and that their ability to scale is hindered by the high degree of human interaction required for remediation and response activities. Security vendors and providers should take note that SMEs need tools and services that go further to prioritize alerts, provide prescriptive analysis, reduce false positives and engage in response with the organization.

Figure 5: Top challenges to investigating all alerts

Source: 451 Research

Q. What is the top reason your security team or service provider is unable to investigate all security alerts?



The Move to Security Services

In response to these challenges, respondents said they are preparing for several improvements over the next 12 months. These advancements focus on investing in additional or improved security tools, investing in threat intelligence, and improving visibility into threat and vulnerabilities across clouds and on-premises infrastructure. To fund these improvements, respondents indicated that they expect to spend a greater percentage of their budgets on security tools delivered from the cloud.

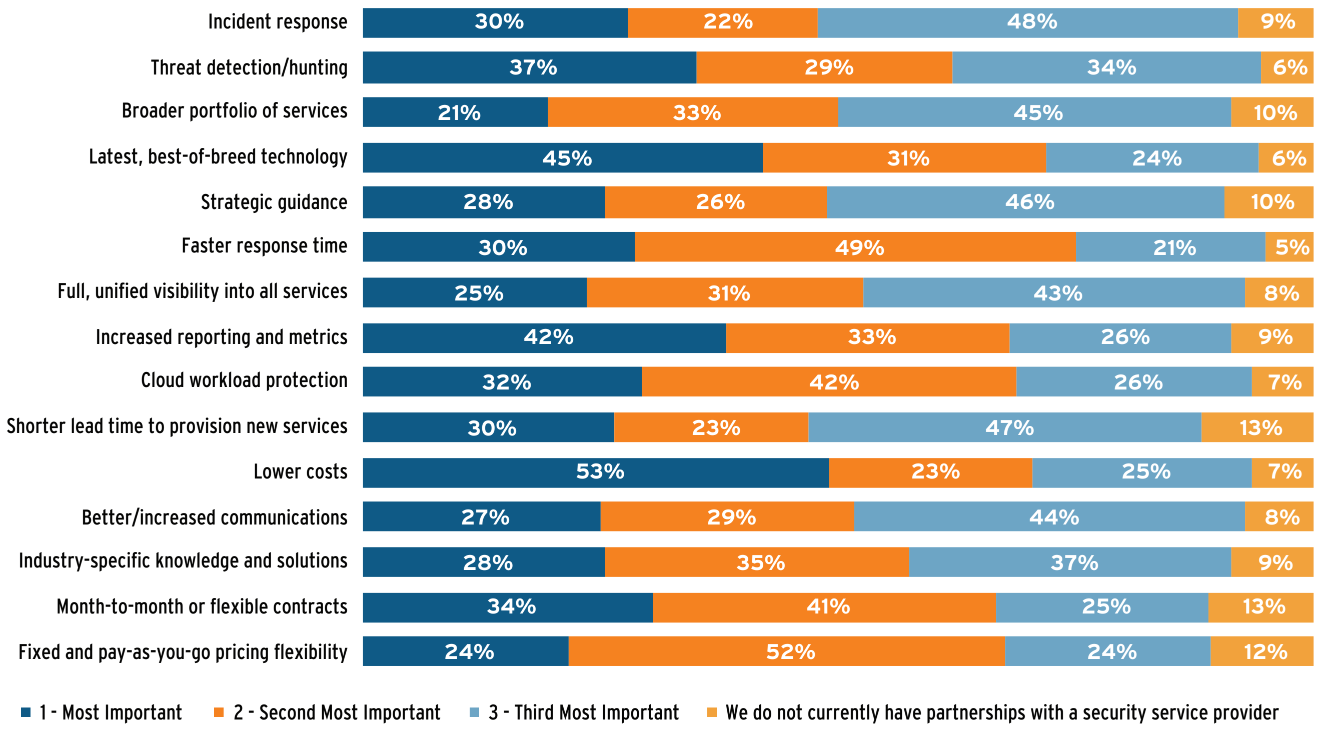
In addition, SMEs are finding that security service providers can help them address many of the challenges they face and provide the tools and services to support and augment their improvement efforts. As they look to partner with a security service provider for tools or to outsource discrete security functions, SMEs are looking for providers that can integrate their services with other security tools and platforms. They expect providers to offer a broad range of security services and protect both on-premises and cloud infrastructure and data through a single, unified platform.

Respondents to the survey said it is important that security service providers deliver services that can be provisioned on demand, with no up-front investment or hardware to install, combined with flexible, consumption-based pricing. While SMEs are looking to deploy the latest, best-of-breed security technology, they are also looking to offload the back-end management and maintenance of security tools, stating they want security services that deliver automatic and transparent patching and upgrades and lower the total cost of ownership. SMEs want a unified platform that can enable management and visibility across the entire hybrid infrastructure. They are also looking for security services that include threat hunting, remediation assistance and SLAs specifying response-time requirements.

Figure 6: Features missing from current security provider offerings

Source: 451 Research

Q. What would you like your existing security provider to offer that is missing today? Please select the top three in order of importance.



n=250

SMEs typically lack the extensive resources of large enterprises to confront cybersecurity threats and are looking for partners that can fill in those gaps. They are pushing back on traditional vendors, manufacturers and service providers as they look to partner with modern providers whose businesses embrace the cloud, capitalize on its advantages and, most important, deliver real value back to their customers. Many SMEs have turned to traditional providers, such as managed security service providers (MSSPs) but have found that these providers often fail to deliver in several key areas.

SMEs report that most traditional security service providers fail to deliver fast response times, lack threat detection and hunting capabilities, and are unable to provide cloud workload protection. According to SMEs, most MSSPs lack ownership and follow-through regarding alerts. They offer little more than a monitoring service, throwing alerts 'over the fence' and leaving SMEs to fend for themselves.

Traditional security service providers tend to have fixed pricing based on multi-year contracts with minimum usage agreements for the term of the contract. While this arrangement is great for the service provider, it fails to deliver the flexibility SMEs require to protect a dynamic and hybrid environment.

SMEs are finding that modern security-as-a-service (SECaaS) providers are in a prime position to help them with the challenges of protecting a growing attack surface and securing hybrid workloads. With modular solutions that minimize the cost and burden of provisioning, managing, and scaling security tools and controls, SECaaS delivers on-demand security that monitors and protects disparate infrastructure and compute environments.

Conclusion

After decades of taking a back seat, cybersecurity is now on the agenda for most SMEs. This new emphasis is resulting in a significant shift in the cybersecurity posture for SMEs, and many have made great strides in securing their organizations and improving their ability to investigate and respond to alerts and incidents. However, as their organizations undergo digital transformation initiatives and move to a hybrid infrastructure, SMEs are feeling the strain of dealing with an increasing volume of security events and alerts, evolving and advanced security threats, and a growing portfolio of security tools and services.

The key pain points that survey respondents highlighted have to do with their inability to scale security operations and protect an increasingly diverse and complex infrastructure. The lack of unified control and visibility across clouds and on-premises infrastructure is at the core of many SME cybersecurity challenges. These pain points and limitations are pushing SMEs to rethink their cybersecurity strategies and partnerships with existing security service providers.

SMEs are increasingly turning to security as a service for many of the same benefits that other cloud-based services provide: reduced capital costs, flexible and on-demand consumption, scalability, and reliability. SECaaS is also enabling SMEs to automate manual tasks, reduce complexity, protect against new and advanced threats, unify protection across disparate environments, and leverage modern security tools geared for protecting a modern infrastructure.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such.

451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200