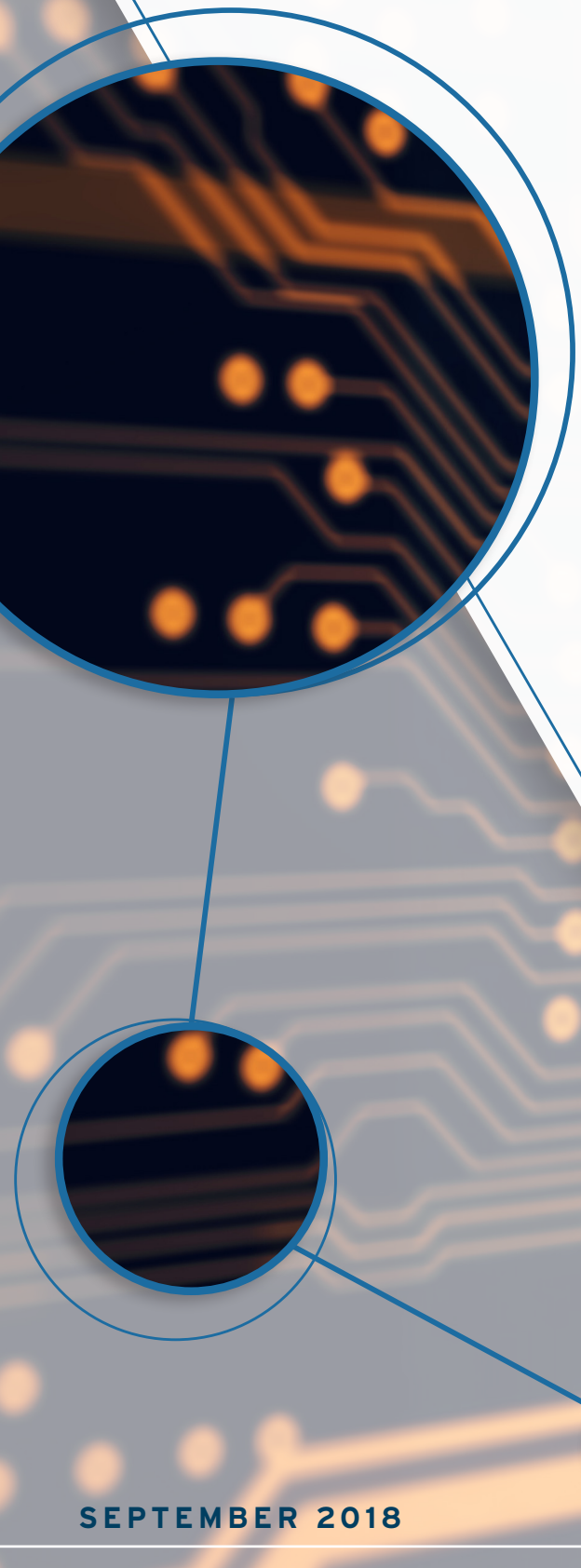
451 Research® | PATHFINDER REPORT



Considerations for EDR Adoption

COMMISSIONED BY

Bitdefender®

SEPTEMBER 2018

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

ABOUT THE AUTHOR

FERNANDO MONTENEGRO

SENIOR ANALYST, INFORMATION SECURITY

Fernando is a Senior Analyst on the Information Security team, based in Toronto. He has broad experience in security architecture, particularly network security for enterprise environments. He currently focuses on covering vendors and industry events in the endpoint security and cloud security spaces.

Executive Summary

The broad trends in the industry – increased adoption of cloud-based resources, increased employee mobility, newer developments in traditional and mobile operating systems, the rise of more capable adversaries, among others – have significantly impacted how organizations should think about endpoint security. Traditional endpoint security strategies included deploying antivirus technology and, if the organization was large enough, additional monitoring capabilities via a host-based intrusion detection system or similar technology. In order to respond to changes to the threat environment, organizations have begun to consider endpoint detection and response (EDR) capabilities. The basic premise behind EDR is that it is prudent to assume attackers may occasionally breach defenses, and the organization needs to be able to detect these incidents, respond to the attacks and restore the environment.

Midsized organizations should take care when selecting EDR tooling because their needs are typically different than those of larger organizations that have been the traditional market for EDR tools. This paper highlights some of these differences and how they may affect the process of choosing EDR tools. It also includes a recommended high-level process for EDR tool selection.

Even though EDR was originally targeted at larger organizations, we recommend that organizations of all sizes consider how they'd be able to address the questions EDR aims to answer: how to detect an attacker that bypasses defenses, and how to remove that attacker from the environment. Ultimately, the functionality provided by EDR will help organizations become more resilient in the face of newer threats, and better support their mission.

Introduction

Much of security boils down to an economics problem: how best to allocate finite resources. While the list of possible vulnerabilities is apparently endless, and the sophistication of adversaries doesn't seem to diminish, the reality is that all organizations have to make trade-offs in terms of security spending versus the benefits – reduced exposure – derived from it. To think otherwise is to ignore the reality of how organizations conduct their affairs, which pushes security practitioners even further from the proverbial 'seat at the table' that is needed to improve security outcomes.

Against the endless stream of attacks – which are often publicized beyond what some consider to be necessary – organizations and vendors have no option but to respond, although they often do so with approaches that end up being suboptimal. Security teams and executives at customer organizations continually spend resources to address the latest attack, often to the detriment of a broad security program. Vendors, on the other hand, see a recent attack as something 'top of mind' with prospects and rush to fill in the space, targeting messaging and sometimes product roadmaps to these newer threats.

Naturally, some threats are significant and present formidable challenges to the entire industry: for example, the rash of disclosures about processor flaws related to hyperthreading and parallel execution that surfaced with Meltdown and Spectre. Still, the majority of organizations deal with a much broader set of threats that, while perhaps not as sophisticated, can overwhelm teams based on volume alone.

The technology environment is also changing dramatically. From the explosion in the number of IoT devices to the broad adoption of cloud-based resources – IaaS, PaaS or SaaS – there have been significant shifts in how organizations deploy and consume resources, with strong implications for security. One of the consequences of this change is the increased importance of the endpoint.

There are several aspects behind the rationale for placing increased importance on the endpoint, but two stand out: mobility and encryption. Modern endpoints have become much more mobile; the same notebook or, increasingly, mobile device that sits on a corporate network may shift to a variety of networks that have different security profiles. This means it is no longer prudent for the device to assume the network is wholly responsible for implementing security, or even that the network is safe to begin with. At the same time, there is increased adoption of application-level encryption, which greatly diminishes the visibility of any network-centric security controls.

Endpoint security has been a subsector of the security industry since the popularization of personal computers in the early 1990s, when it established a foothold. Since then, the endpoint security evolved quickly through antivirus, anti-malware, next-gen antivirus and, recently, endpoint protection (EPP) products. The market rushed to fill organizations' need to protect against increasingly sophisticated threats. Although they were initially seen as a nuisance, the onslaught of attacks became a critical concern for most organizations.

The increased importance of the endpoint has not been lost on vendors such as Google, Apple and, significantly, Microsoft. Despite historical criticism of its security record, Microsoft has been constantly improving the baseline security in its operating systems. Windows 10 includes several security features that ultimately raise the cost to attackers. Because of that improvement, alongside the increase in sophistication of attacks, organizations taking a prudent approach to security are looking beyond protection features on their endpoint suites. They are now considering how endpoints can be part of a broader incident response and digital forensics practice, working alongside the rest of the
security architecture.

The industry has broadly adopted the term endpoint detection and response for the capabilities that, when deployed on endpoints, detect evidence of security incidents, investigate these incidents and, when necessary, offer some level of response. Although initially adopted by larger organizations, EDR is becoming more mainstream, and adoption should expand into multiple types of organizations. Vendors have been quick to respond to this demand, proposing offerings that include a variety
of features.

Understanding EDR

At a high level, endpoint detection and response tools require the capability to perform some variation of the following tasks:

- Data/telemetry collection. This means collecting relevant information from the endpoints. This information typically includes details about files, filesystems, processes, memory, network connections, user activity and system configuration. Depending on the product architecture, this collection can be done locally on the endpoint and periodically sent to a centralized location, or it can be done centrally. There are arguments for and against these approaches to data collection.
- Exploratory data analysis. As the system collects information from the endpoint fleet, an analyst should be able to interact with the data that has been gathered to answer questions related to the various use cases for EDR. This interaction between agent and the system will vary, but can include elements of ad hoc queries, data visualization, prerecorded sets of queries and scheduled
  reporting, etc.
- Analytics and enrichment. In addition to interactions with the analyst, the EDR tooling is expected to perform some level of independent analysis with the goal of triggering alerting based on security use cases. This analysis often includes the application of statistical methods including various machine learning techniques to assist with anomaly detection, clustering or predictive modeling. This analysis can be further enhanced by integrating the EDR system with third-party data-enrichment sources such as threat intelligence feeds and malware sandboxes for analyzing
  runtime behavior.
- Response capabilities. Whether triggered by an automatic alert from its analytics engine, an external alert by another system, or invoked manually by an analyst/operator, the EDR system should offer a range of responses that support investigation or containment use cases. These responses normally range from restricting endpoints – either via the EDR agent or in collaboration with the rest of the environment, and may be done at the process, network, file, system or user levels, with optional rollback to previous states – to triggering additional data collection – often for further analysis or, in some cases, interaction with law enforcement. Importantly, some systems support the use of playbooks (predetermined response plans) to be used, either manually or in some
  automated manner.

Considerations for Selection of EDR Tooling

With endpoint detection and response becoming a critical component for many organizations, the focus changes to understanding the steps to take when looking at EDR products. We believe that the proper approach to this includes understanding the organization and its capabilities, in addition to the more technical considerations around EDR.

STEP 1 – WHERE DOES THE ORGANIZATION STAND?

The first step is to understand the organization's needs. This is relevant because EDR was originally targeted at larger companies, and vendors made assumptions about how the organization is structured, what capabilities it has, and what the threat environment looks like. A recent 451 Research Voice of the Enterprise survey asked respondents several questions about their priorities for the next 12 months.

Figure 1: Organizational priorities – top InfoSec projects over the next 12 months

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2018

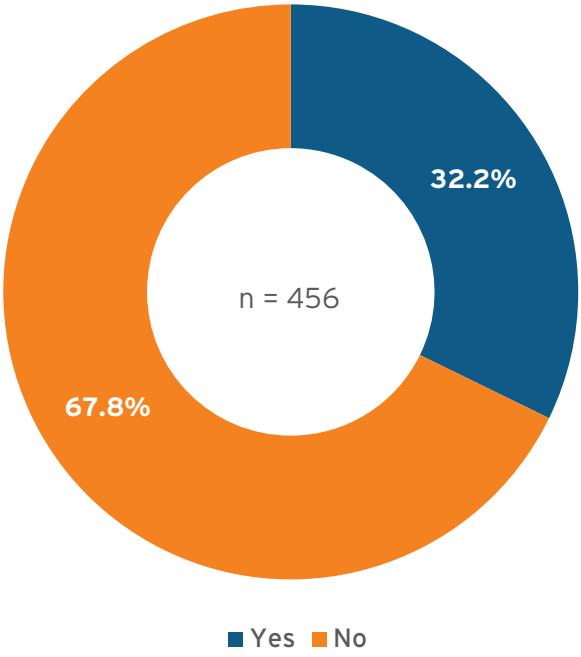
	TOTAL	SIZE					REVENUE				
		1-249 employees	250-999 employees	1,000-9,999 employees	10,000+ employees	Govt/Educ	< $1M	$1M-$9.99M	$10M-$99.99M	$100M-$999.99M	$1BN+
Regulatory compliance (e.g., PCI compliance, GDRP, PSD2, NIST)	34.8%	33.7%	31.9%	38.9%	39.7%	22.4%	31.3%	34.5%	21.8%	35.6%	41.5%
Security awareness initiatives	19.2%	18.4%	22.2%	14.2%	17.2%	27.6%	12.5%	20.7%	23.1%	25.3%	14.3%
Cloud infrastructure security	17.9%	16.6%	16.7%	11.5%	30.2%	12.1%	12.5%	13.8%	16.7%	13.8%	26.5%
Security information and event management (SIEM)/security analytics	17.5%	13.5%	16.7%	24.8%	17.2%	15.5%	8.3%	17.2%	16.7%	18.4%	21.1%
Vulnerability assessment	16.4%	18.4%	18.1%	15.9%	11.2%	17.2%	25.0%	19.0%	23.1%	13.8%	11.6%
Multifactor authentication	16.0%	13.5%	15.3%	20.4%	12.1%	22.4%	8.3%	13.8%	11.5%	19.5%	17.7%
Data loss prevention	15.8%	19.0%	16.7%	16.8%	12.9%	10.3%	20.8%	29.3%	17.9%	13.8%	12.2%
Endpoint security	15.6%	16.6%	22.2%	11.5%	10.3%	24.1%	20.8%	17.2%	21.8%	16.1%	13.6%
Patch management	13.3%	12.3%	20.8%	10.6%	13.8%	10.3%	20.8%	6.9%	14.1%	13.8%	13.6%
Monitoring improvements	12.4%	16.6%	12.5%	14.2%	6.0%	10.3%	10.4%	17.2%	12.8%	16.1%	8.2%

Figure 1 illustrates how responses vary. While there is a preponderance of respondents who indicated a focus on compliance – due, in large part, to the new phase of the EU's GDPR – there are differences between organizations when you take their size or revenue into considering. Clearly, this is an indication that there is no 'one size fits all' when it comes to security.

Furthermore, results from 451 Research's Voice of the Enterprise surveys indicate use of a security operations center (SOC) is not as prevalent as one might imagine:

Figure 2: Existence of a security operations center

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2017



Only about one-third of respondents said that they have a security operations center. This is a sobering message when you consider that many security conferences, publications and products are aimed at optimizing SOC workflows, SOC process improvement and similar topics. Yet even the statement that 'one-third of respondents have a SOC' can be further refined by segmenting responses based on organizational size and on revenue.

Figure 3: SOC adoption by organization size and revenue

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2017

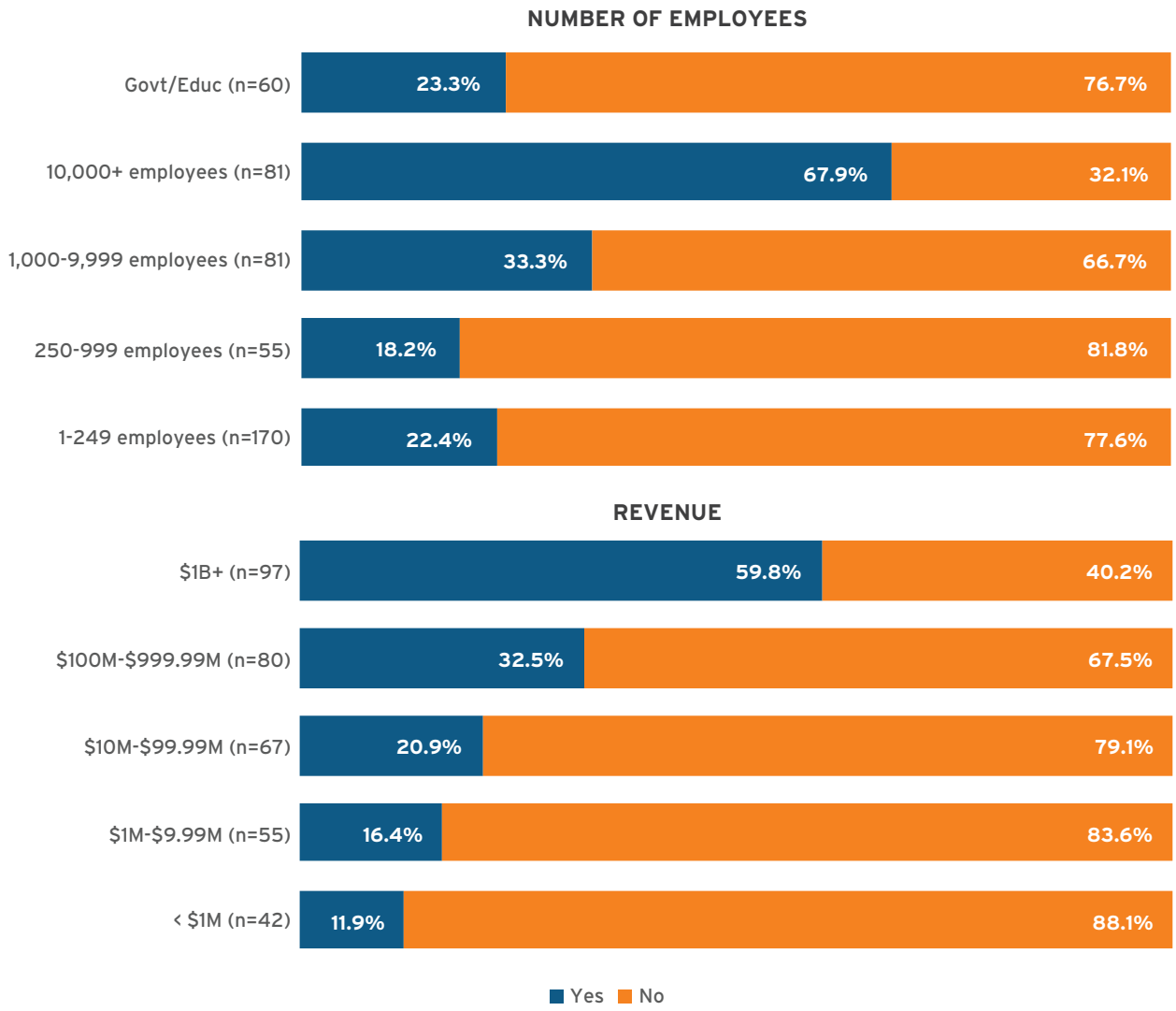


Figure 3 shows that larger organizations – 10,000+ employees or more or more than $1bn in revenue – are more likely to have SOCs, but there are still many companies in that category that have don't have an SOC. The picture is more telling for smaller organizations. In their case, the responses fall off significantly, indicating that SOC-centered approaches and products may not be a good fit. This is critically relevant for endpoint detection and response because vendors that assume customers have SOCs in which to deploy EDR products will create features that may not be easily applicable outside
a SOC.

STEP 2 - WHAT IS THE TEAM SIZE AND MAKEUP?

The increased importance of cybersecurity over the past few years has given rise to a widely held view in the industry that there is a shortage of security skills. Just as IT infrastructure becomes even more embedded within organizations, organizations seem to be struggling with maintaining the necessary staffing levels, at the right levels of expertise, to properly address security concerns with that infrastructure. The cybersecurity skills shortage manifests itself in multiple ways. There's increased difficulty in hiring professionals with the necessary skill sets to address security needs, just as there's difficulty in updating the skill sets of existing staff. Furthermore, given a certain level of expertise, it becomes more difficult for organizations to retain those professionals. Data from 451 Research's Voice of the Enterprise confirms this and provides some nuances.

Figure 4: InfoSec skills shortage by organization size and revenue

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2017

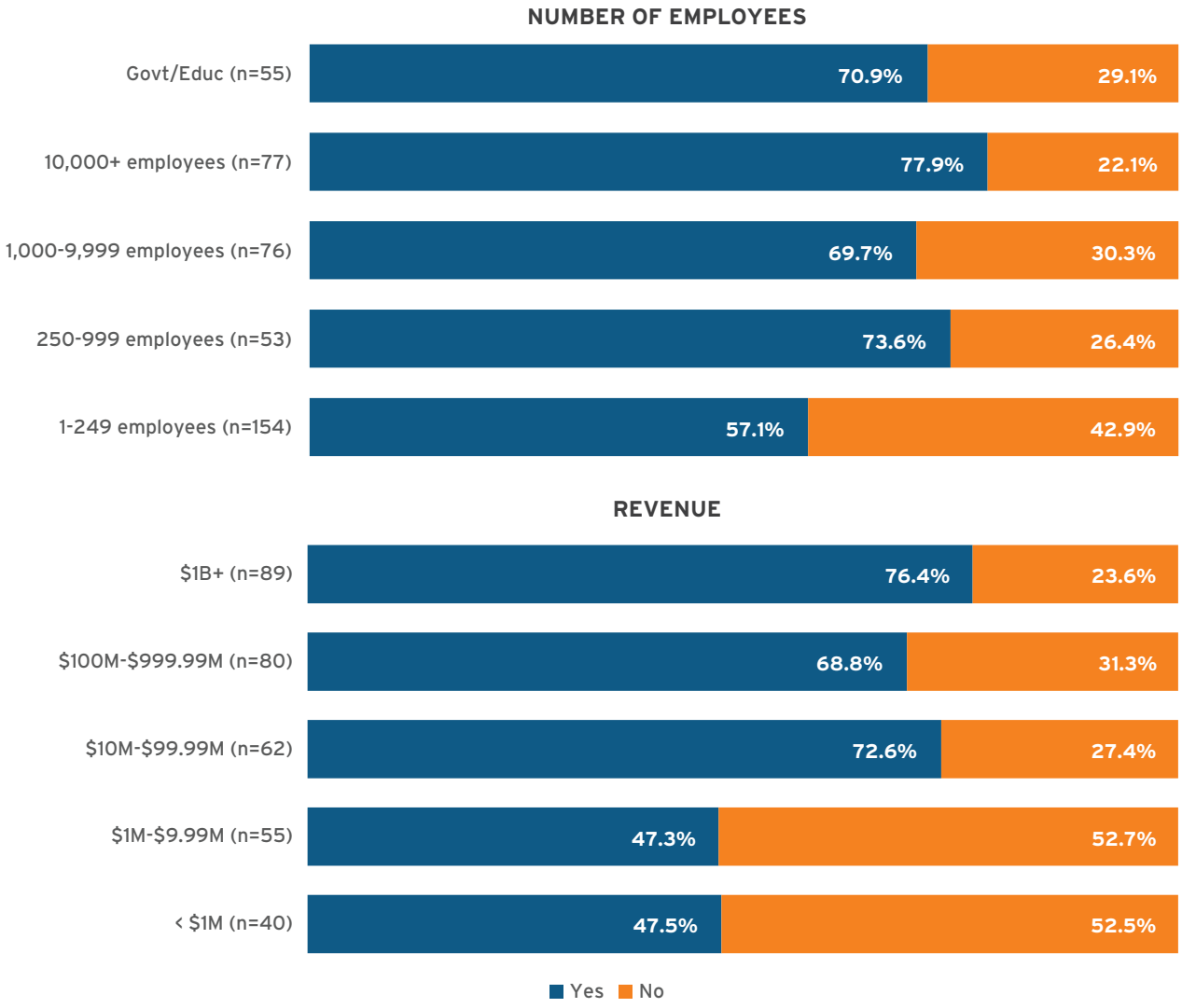
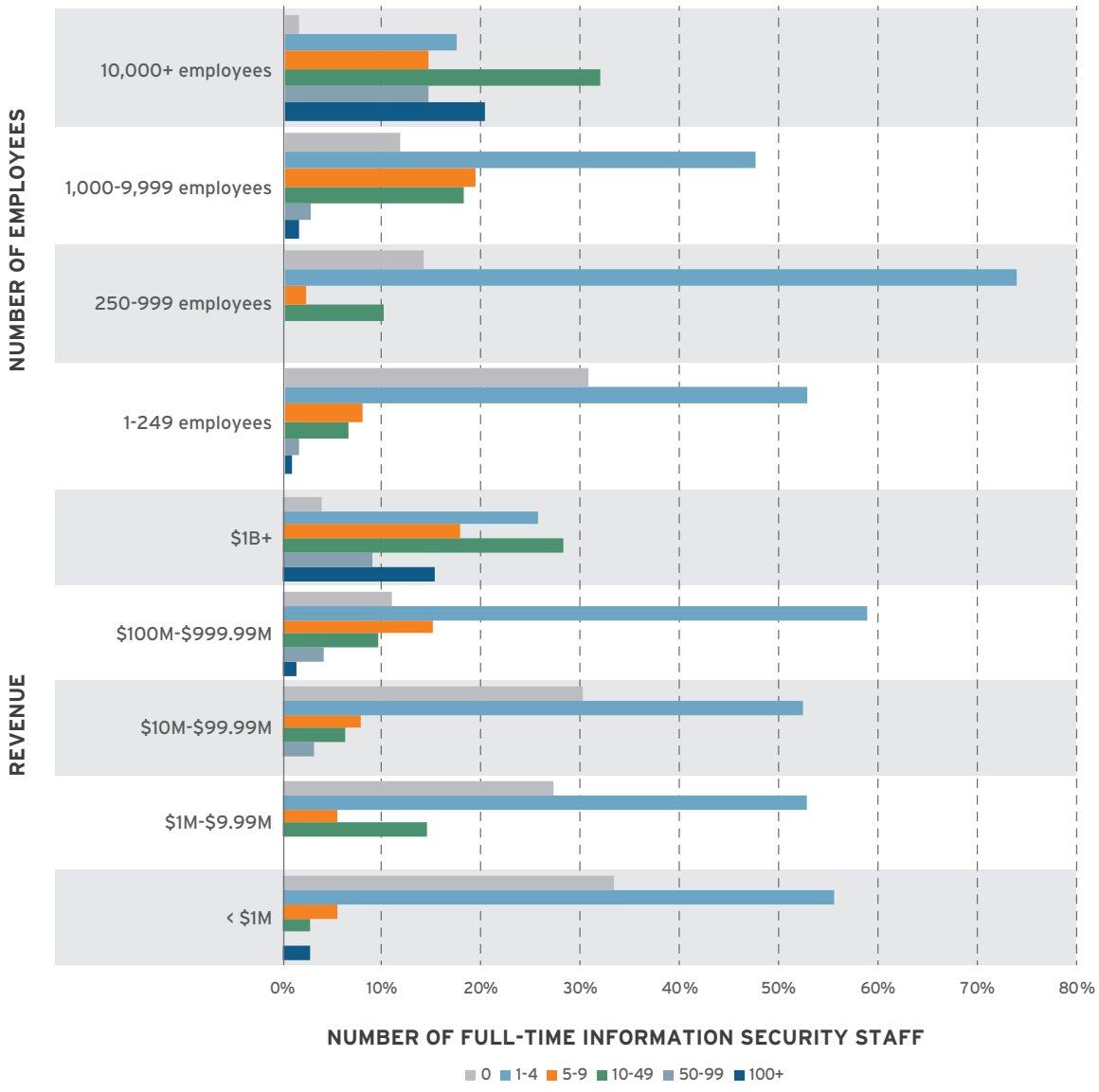


Figure 4 shows that there is some difficulty in hiring across organizations of all sizes when measured by employee count. Smaller organizations are impacted less, although there is some distinction when company size is based on revenue. This is an important data point that offers some rationale and justification for vendors adding more sophisticated automation capabilities to their offerings, particularly when targeting larger organizations. This drive for automation, though, may come at the expense of a steeper learning curve.

Team size and composition are also important. The following charts illustrate differences among organizations. When asked about how many staff were dedicated full time to information security, organizations responded as follows:

Figure 5: Size of information security team by organization size and revenue

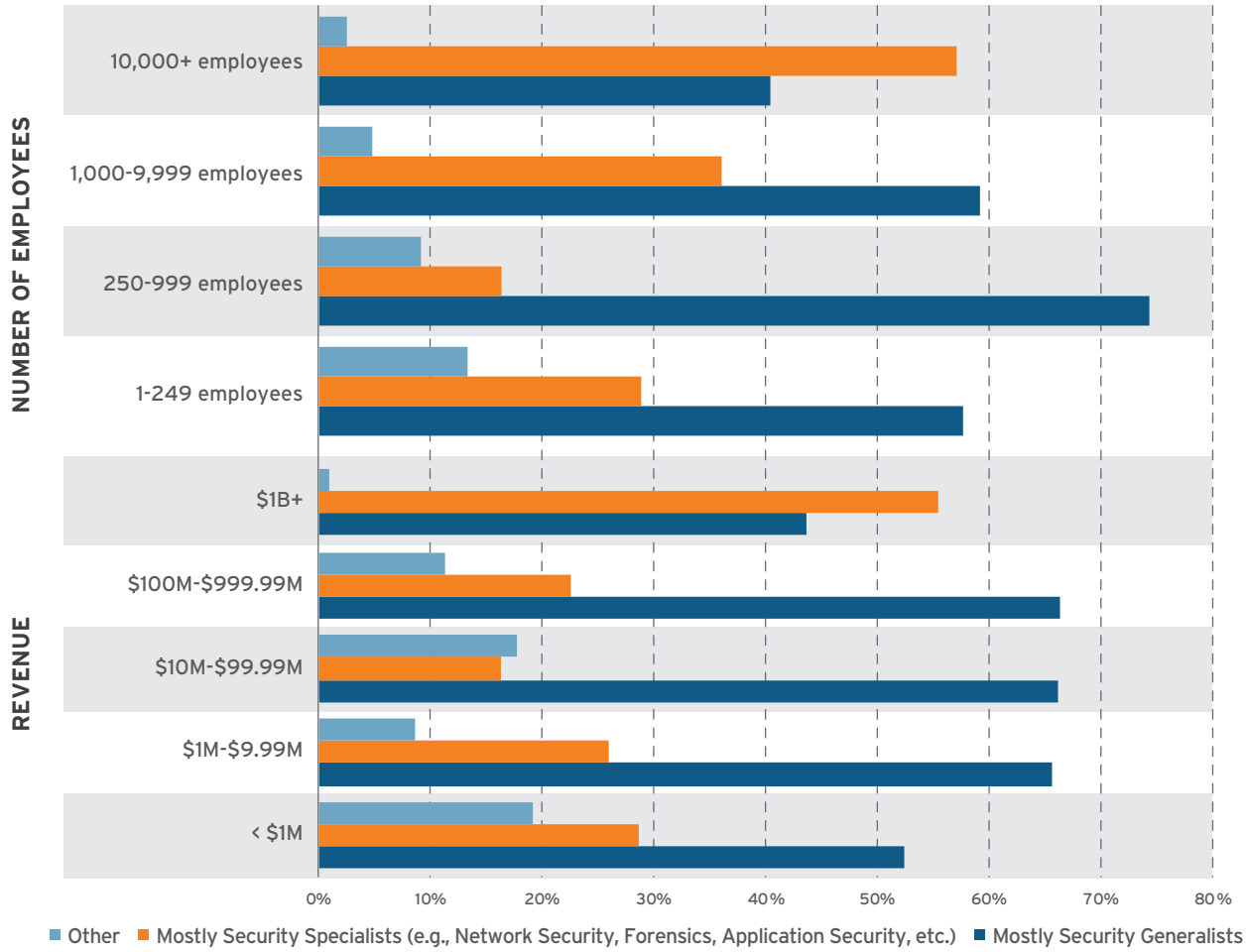
Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2017



Until an organization reaches 10,000+ employees or $1bn in revenue, the size of the security team is not at all large. This concentration of activities into such a small group of professionals all but dictates that the team makeup leans toward generalists rather than specialists. This is precisely what the Voice of the Enterprise survey indicated as shown in Figure 6 below:

Figure 6: InfoSec team composition by organization size and revenue

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2017



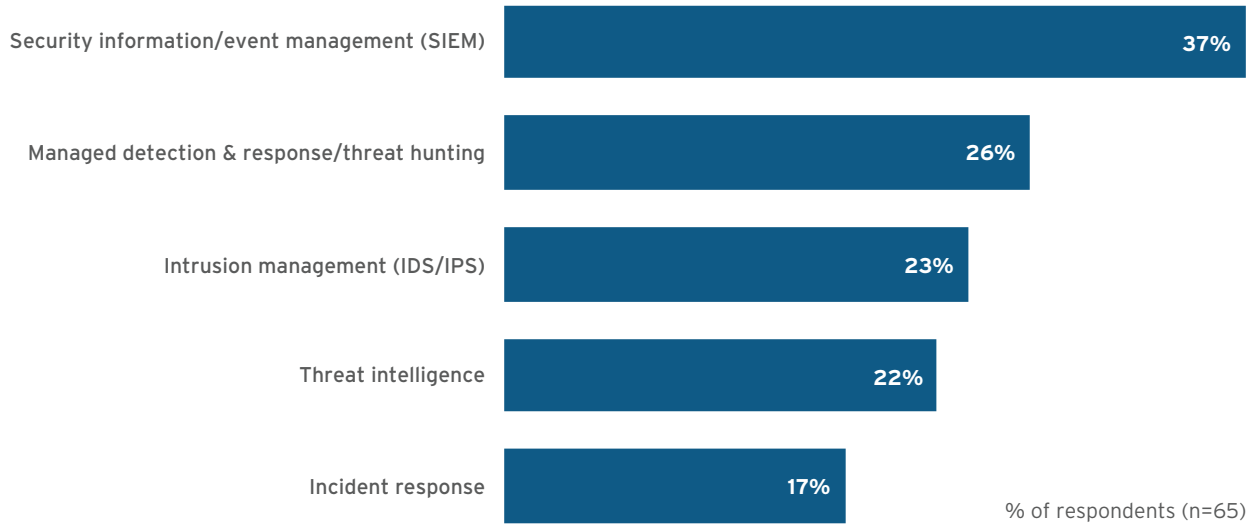
According to these two data points, the size and makeup of security teams varies based on the size of the organization. This is an important factor to consider when selecting security tooling in general – and EDR in particular – because the products are created based on assumptions about the customers that will be using them. These assumptions may include how the products will be deployed on a regular basis, the experience of the team operating them, and what the expected usage will be.

STEP 3 - IS THERE A ROLE FOR MANAGED SERVICES?

The considerations about hiring also invite an investigation into a possible role for external organizations to perform managed security services related to EDR. 451 Research survey data indicates that managed detection and response and incident response are among the top five use cases for organizations considering managed security services.

Figure 7: Top five use cases for managed security service providers

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2018



The market currently offers several options of managed security service providers. Some offerings can work with a customer's existing technology options, while others offer specific choices.

STEP 4 - UNDERSTANDING WHICH ENDPOINT DETECTION AND RESPONSE FEATURES MATTER THE MOST

Once organizations understand their goals and what capabilities are available, the next step is to understand what they require from the EDR tooling. In some cases, EDR's main use may be to track the spread of an outbreak across the organization. In others, it may be to extract artifacts that could reveal more about an attacker's tactics, techniques and procedures. Some organizations also want to conduct proactive threat hunting – look for indications that the network may have already been compromised by a skilled adversary but not yet detected by existing monitoring systems.

The truth is that typical EDR products' functionality and maturity are often tied to the assumptions the vendors have made about client capabilities. While one vendor might favor a more optimized approach for threat hunting, the product may have a steeper learning curve. Conversely, another vendor's product may be optimized for ease of use by non-dedicated teams but lack features for deeper analysis and forensics. This notion of 'easy to use EDR' may be attractive to organizations looking to perform some, maybe even the bulk of, investigations.

There is also the potential to integrate EDR with endpoint protection. The benefits of doing so normally include a reduced agent footprint (see below) and operational effort, as well as a potential reduction in the number of alerts the security team has to review. There's also the benefit of enriching alert information with policy data from the EPP component or accelerating the response by pre-population of EPP policies in response to incidents.

Ultimately, when selecting an EDR product, organizations need to understand the full suite of capabilities that each EDR offering provides, as well as the features that are necessary to support their incident response and forensics goals. If this is not done properly and a mismatch occurs between organizational capabilities/needs and the tooling capabilities/requirements, the result can be diminished returns on the EDR investment – an EDR system that is not capable of addressing the needs of the organization, or an EDR deployment that is too onerous to yield the desired results.

STEP 5 - DETERMINE AGENT FOOTPRINT

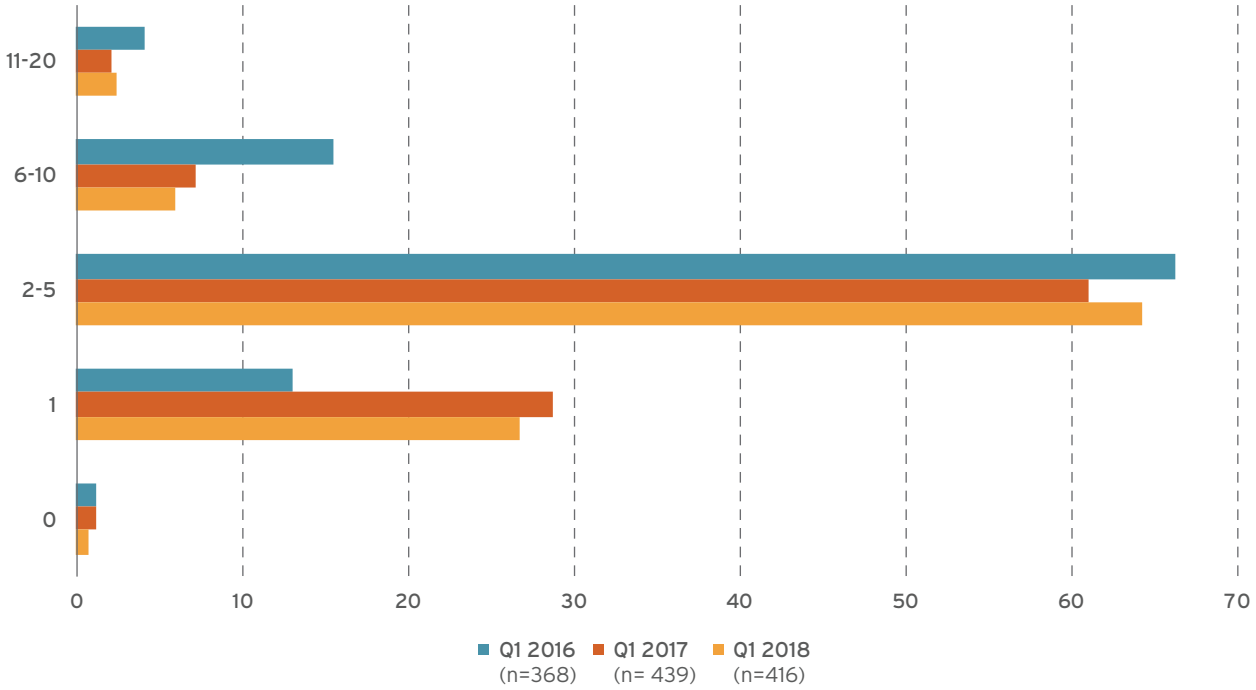
Organizations also need to consider how they want to deploy EDR functionality, either embedded into an existing endpoint product or as a stand-alone EDR tool. Deciding whether to deploy yet another agent on an existing environment is not trivial. While individually, each agent doesn't represent a specifically onerous load on a system, it still consumes organizational resources, and in aggregate, agents can become a burden on the organization.

Endpoint security vendors often indicate that their agents have small footprints – usually low single-digit percentage of CPU and a few MB of memory. However, focusing just on this resource consumption overlooks the operational burden of procuring, deploying and maintaining those agents on an increasingly distributed and diverse endpoint fleet.

That said, there are valid points to be made that implementing endpoint security functionality via separate agents, possibly from distinct vendors, allows for greater granularity, use of more specialized products, and resiliency when faced with the loss of an agent. Ultimately, each organization should consider how it plans this footprint.

Figure 8: Number of endpoint security solutions currently employed

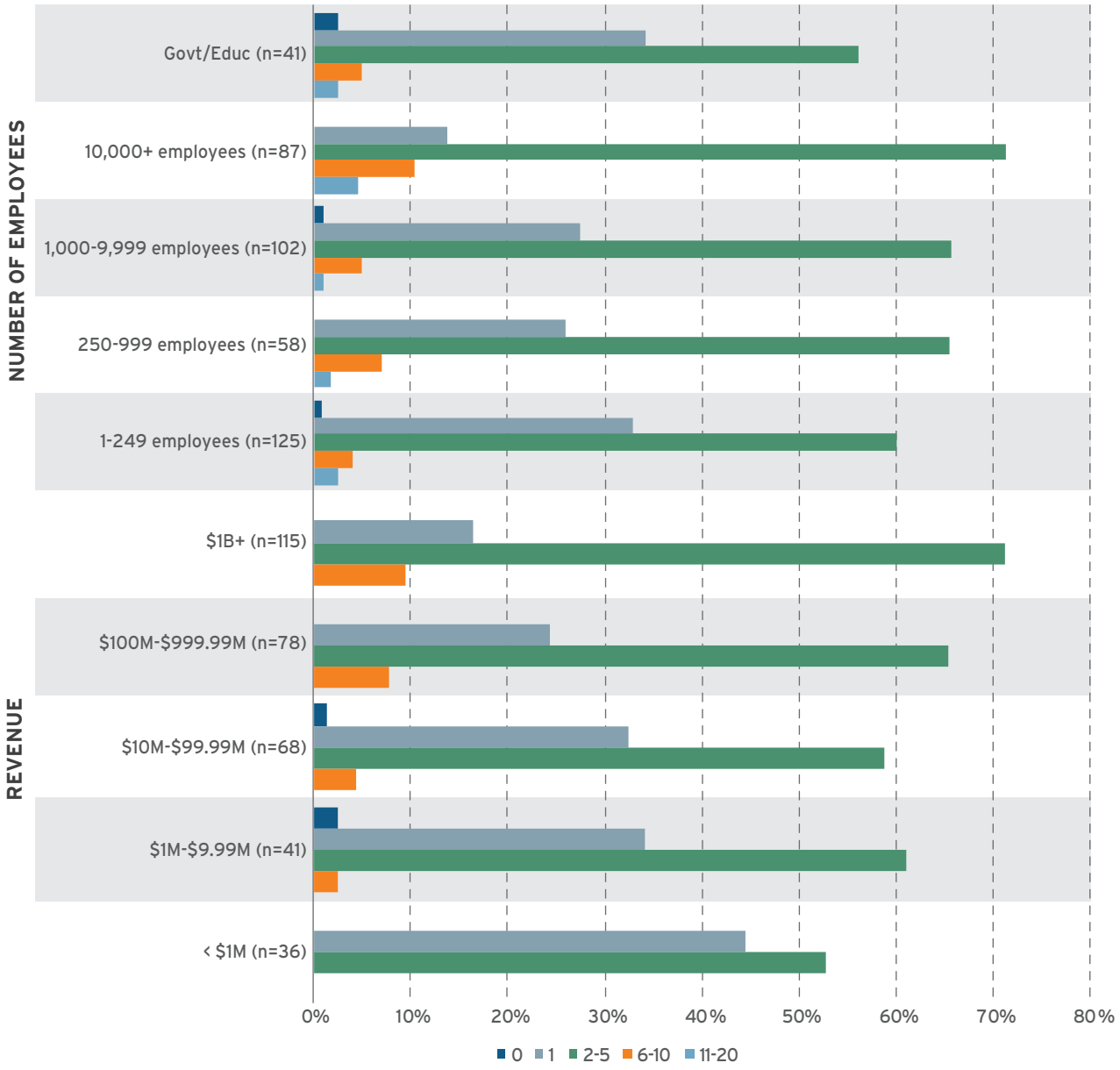
Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2016-18



Responses from 451 Research's Voice of the Enterprise indicate that, in aggregate, a lot of companies use one to five endpoint security agents. When considering more specific breakdowns by organization size, the picture is different. In this scenario, only numbers from the 2018 Voice of the Enterprise survey were used.

Figure 9: Number of endpoints by organization size and revenue

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2018



The number of respondents with more than five agents only starts to rise for larger organizations. This is consistent with the constraints that smaller and midsized organizations have.

STEP 6 - BRING IT ALL TOGETHER

After the organization has reviewed the key areas as defined in this paper, the adoption process should follow these general guidelines:

1. First, define the organizational aspects that will drive the EDR adoption process. What are the organizational goals and constraints as they relate to EDR? Does the organization intend to operate the EDR solution itself, or will it involve a third-party MSSP to do so? If selecting an external service provider, this becomes a different conversation that is not covered in this guide.
2. Leverage the organization's security management program to define the list of threats that the organization wants to consider within the scope of the EDR evaluation. This can be done by looking at past incident data, or in cooperation with internal stakeholders and external partners. What kind of threats/incidents are to be considered? Ransomware outbreaks? Targeted phishing campaigns? Malicious insiders looking to exfiltrate data?
3. Clearly define how the organization intends to use the EDR tooling it chooses. This includes considerations around current and future usage; it should cover both functional and non-functional aspects.

ASPECTS	KEY CONSIDERATIONS
FUNCTIONAL: DETECTION	Do the analytics functions of the EDR product – whether based on rules, heuristics, machine learning or some combination – detect the threats that the organization is considering in its threat models? Can these detection functions be augmented with additional information provided by the security team, such as indicators of compromise or other enrichment data?
FUNCTIONAL: INVESTIGATION	How well does the EDR tooling support the investigative tasks and methodologies that are used? Does it collect the right kind of artifacts, from runtime processes and network information to file hashes and operating system objects? Does it support broad search for the right kind of artifacts across the organization?
FUNCTIONAL: RESPONSE	Does the EDR tooling support the range of responses – from additional data collection to quarantine to triggering workflows in incident response playbooks? For responses that integrate with the rest of the environment, how easy is it to integrate EDR with protection components?
NON-FUNCTIONAL: FOOTPRINT	How does the deployment of the EDR tooling affect the existing security footprint? Is it a newer module on an existing agent or a separate agent? What back-end resources are required?
NON-FUNCTIONAL: LEARNING CURVE AND USER EXPERIENCE	What are the steps and ongoing experience for enabling the team to use the tooling? Is the level of information provided by the user interface consistent with the capabilities of the team that will be using the product?

These elements should be incorporated into a specific test plan, independent of any one vendor.

4. Based on existing information sources – product reviews, industry analyses, existing relationships and technology choices, among others – select a subset of vendors that provide EDR capabilities. This is an area where organizations have had some success engaging with value-added resellers or other external parties to help with the selection and testing process.
5. Finally, execute the testing process and score each candidate's product against the predefined criteria.

A selection process like the one described above should help organizations select the EDR tooling most appropriate to their specific needs.

Conclusions

In our opinion, organizations are rightfully placing increased importance on the selection of their endpoint security tooling. This reflects that endpoints are truly becoming a critical component in modern architecture as workforces become more mobile, and application-level security places increased importance on the endpoint as a control point.

Endpoint security should not consist solely of preventive controls, but rather support a broader set of security activities including detection of sophisticated attacks and data collection. This is the essence of endpoint detection and response. As base operating systems improve and attacks become more sophisticated, EDR becomes increasingly important.

We have looked at various topics that could impact the selection of EDR tooling by organizations. Notably, we consider that because the needs of organizations vary significantly based on their size, those variances should also be reflected in EDR choices. This should flow down to the types of activities that customers will be more likely to conduct, their relationship with managed service providers, and the footprint they'll have.

Ultimately, our recommendation is to look beyond the common industry narrative and select processes and tooling that meet the organizational needs. It is well understood that endpoint security is growing in importance and must be maintained constantly. Organizations that can deliver security across their endpoint fleet in an efficient manner will be able to support the agility that their business and the modern threat environment demand.

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.

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) 207 426 1050

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

451 Research®