Cynet

2021 Survey of

CISOs with Small Cyber Security Teams

JANUARY 2021

Table of Contents

Introduction and Key Findings

Size Matters: How are Today's Small Security Teams Taking on Increasingly Big Security Challenges?

While there are many reports out there looking at large enterprise security teams and their challenges, Cynet commissioned this report from 3rd party research firm Global Surveyz to better understand the unique challenges faced by *small* security teams. We wanted to gain insight into how they make their purchasing decisions, what budget these teams will have in 2021, and what their priorities are for tackling issues such as technology overlap, lack of visibility and control, and reliance on external security providers. With the risk landscape growing exponentially year on year, how do small security teams feel that they measure up against larger Enterprise-size teams?

This report therefore focuses on the reality for today's small security teams. **We surveyed 200 CISOs at 200 companies, looking specifically at those with 5 or less team members, in medium-large sized organizations that have between 500 and 10,000 employees**. These teams have unique challenges as they hold an essential role within the company, but do so with a small presence and often a small budget. Uniquely, we chose to *only* interview CISOs, across the USA, Canada and UK, as these 200 CISOs are the true decision-makers of small security teams. The result? A rare insight into the inner workings and dynamics of their organizations, and a spotlight into the challenges of small security teams everywhere.

Key findings

Small security teams have their own unique challenges

We looked at teams with 5 or less security staff, and in 70% of cases, less than $1,000,000 in budget. With less people power, and less budget to play with, we quickly saw that security teams are forced to cut corners. **16% of teams are ignoring alerts that have been automatically mitigated, 14% of teams only look at the alerts that are flagged as 'critical', and 79% of companies take more than 4 months to get up to speed deploying and becoming proficient in top security tools**.

The realities of small security teams are opening companies up to serious risk

63% of CISOs feel that their risk of attack is higher compared to larger Enterprises, who have larger teams, budgets and tools in place. In fact, only 7% feel their risk is smaller, despite the assumption that Enterprises have a larger target on their backs. This sentiment is taking its toll, as a shocking **57% of CISOs admitted that their ability to protect their company is overtly lower than they would like it to be**. Perhaps most critically of all, **47% of companies say that their top challenge is that they don't have adequate skills and experience to protect against cyber-attacks**.

Small security teams are drowning in duplicate processes, and complex controls

When asked how small security teams are trying to reduce the impact of their unique challenges, **80% of CISOs responded that they would like to invest more in automation**, proving that the tide is turning towards smart processes. While budgets are increasing this year, increasing their team sizes ranked at the bottom of the tactics chosen, proving that companies are looking for innovative ways to do more with less heads, and that CISOs realize that onboarding more employees isn't necessarily the smart approach. **62% say that they would be able to speed up threat detection and response**, if only they could consolidate their security tools and processes effectively. 48% of CIOs revealed that they could have avoided some security incidents in 2020 if they had a bigger team.

Virtually all small security teams are outsourcing some level of security services

Outsourcing is one way to handle risk. We can see that this is a common response, split almost equally between companies outsource to an MDR service (53%) and those that or are using an MSSP service (47%). And yet, in many cases this isn't reducing workload, as **39% of CISOs still have a full-time team member on-staff that chases all of their alerts.** An MDR that checks all the boxes is high on CISOs priority lists. **33% prioritize 24/7 critical alerts and monitoring, 21% are looking for remediation capabilities, and 21% would prioritize incident response recommendations.**

Small security teams are looking for smart ways to consolidate, automate, and head into 2021 strongly

Today's small security teams are not short on ideas. They know which breach prevention technologies are essential, with **EDR at 52% adoption**, and **87% of CISOs seeing value from its use.** 15% of CISOs report having an XDR solution in place. XDR adoption makes sense as it supports several tactics indicated by respondents, including the investment in automation solutions and processes (80%), consolidating security tools and platforms (61%) and replacing complex security technologies (52%). With smaller budgets, organizations are looking for ways to innovate using automation, and if possible, to consolidate the cost of essential MDR services into the cost of security products, allowing a single line item to check many boxes.

Cyber Security Team Size and Budgets

Company Size and Cyber Security Team Size

Our focus for this survey was medium to large companies (500-10,000 employees) with small security teams of 5 or less employees. We chose to focus on these, since as we will see, smaller teams face different challenges compared to large cyber-security teams.

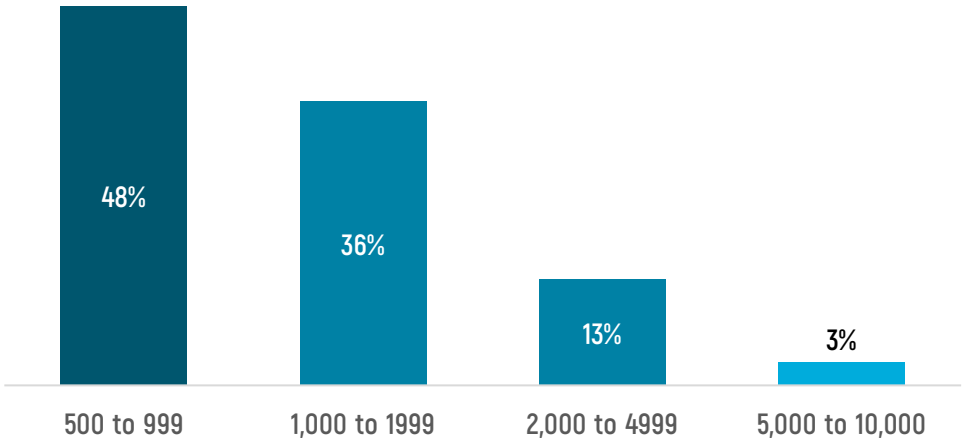

Figure 1 Number of Employees

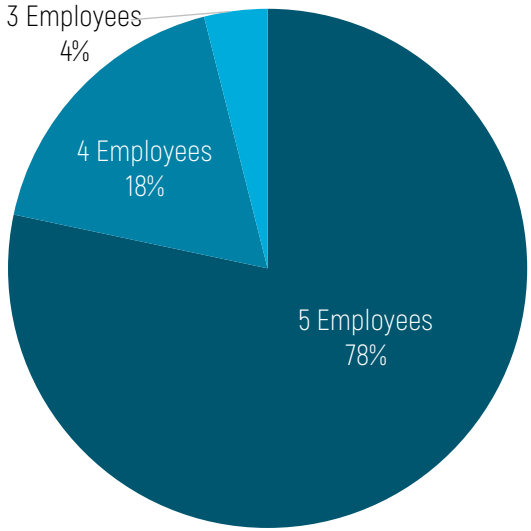

Figure 2 Cyber Security Team Size

Security Budget in 2020 and Planned Budget for 2021

With small team size, comes smaller budgets. More than two thirds (70%) of survey respondents have a budget of under $1,000,000, with 31% owning a budget of $1,000,000 to $2,000,000 and only 4% owning budgets of over $2,000,0000.

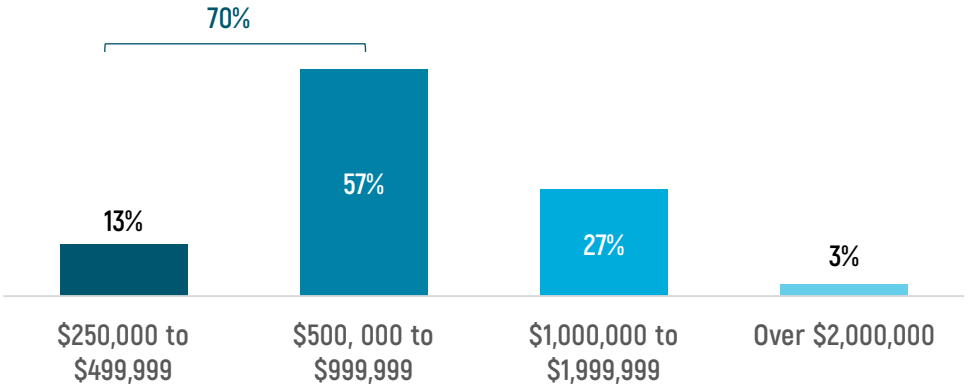

Figure 1 Security Budget in 2020

However, budgets are growing. **85% of survey respondents are planning to increase their budget by 5% or more,** with 23% planning to increase their budget by more than 10% this year. Only 11% plan to keep the same budget as in 2020 and while 5% expect to decrease their budgets by 5%-10%, none of the survey respondents will decrease their budget by more than 10%.

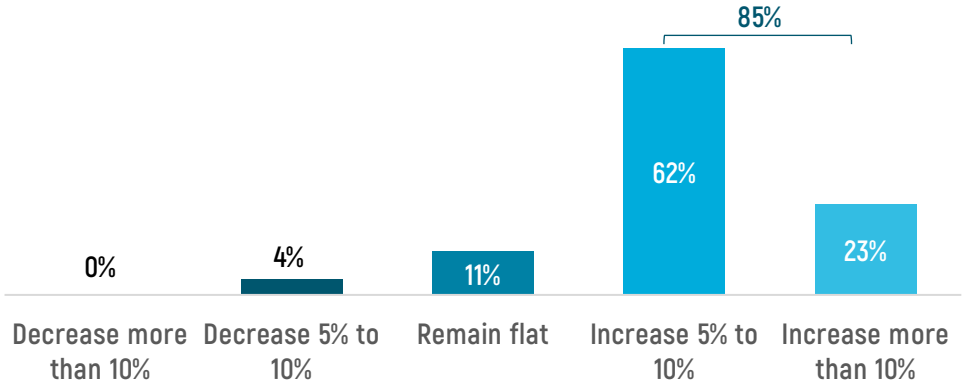

Figure 2 Expected Growth in Security Budget for 2021

Breach Prevention Technology

Top 10 Breach Prevention Technologies in Use / Plans

We asked survey respondents for a wider understanding of their breach prevention technologies. What are their top 10 already in use and what technologies do they have no interest in?

The top two breach prevention technologies used by about almost all respondents were EDR/EPP (52%) and NTA/NDR (45%), followed by CASB (29%), NGAV (18%) and XDR (15%).

The top breach prevention technologies on the CISO roadmap to be purchased are NGAV (64%), Deception (56%) and CASB (42%).

Deception (13%) and UEBA (12%) were the top two breach prevention technologies that companies want but cannot afford due to high costs or lack of people to operate. See a detailed breakdown on page 12.

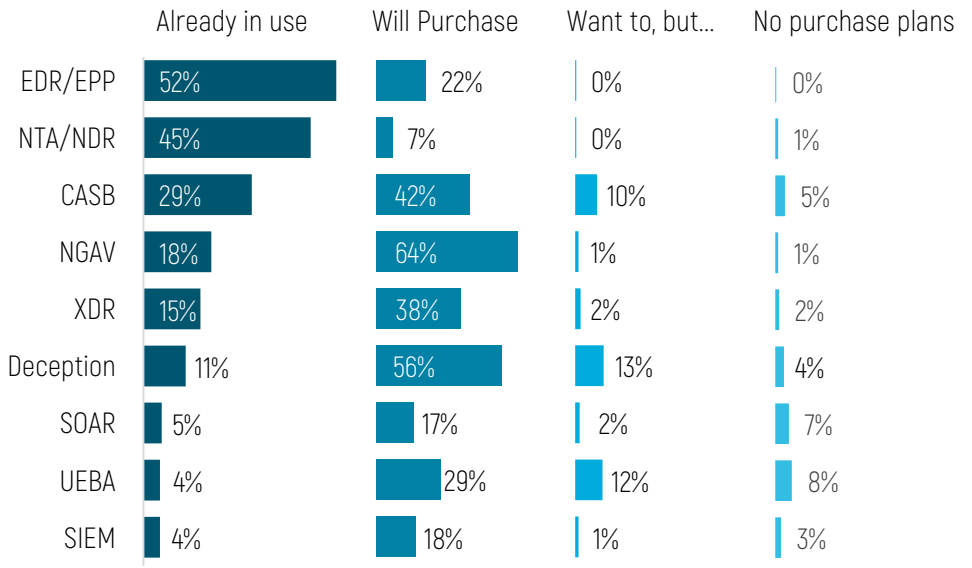

Figure 3 Top Breach Prevention Technologies in Use / Plans

Breach Prevention Technologies Companies Want but Cannot Afford

We asked survey respondents which breach prevention technologies they want but cannot use. The two main reasons stopping them from using these technologies were either due to high costs or lack of people to operate.

The top breach prevention technologies companies want but are too expensive are UEBA (9.4%), CASB (6.4%) and Deception (5.9%).

They also selected the ones they want but do not have the people to operate and those include Deception (6.9%),CASB (3.4%) and UEBA (3%).

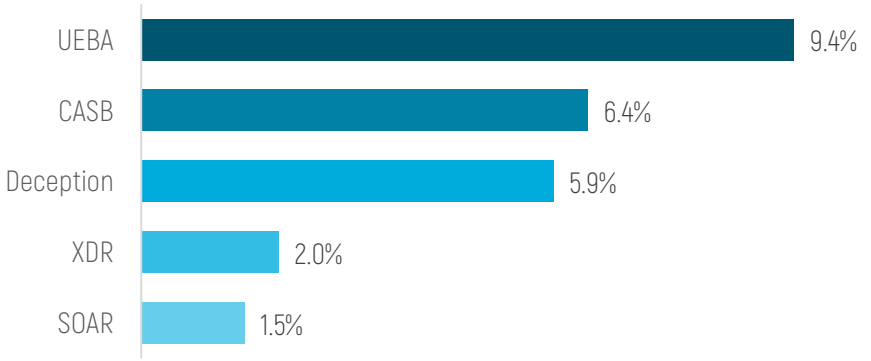

Figure 5 Breach Prevention Technologies that are too Expensive

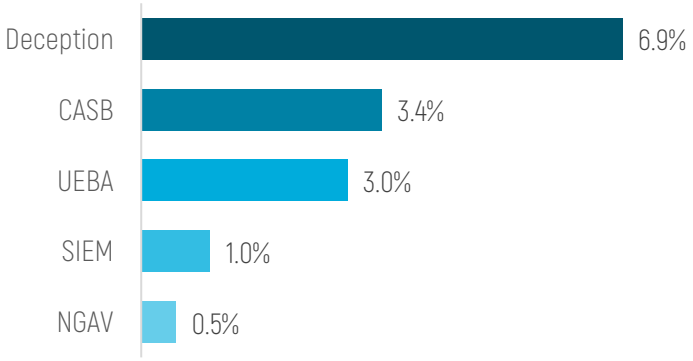

Figure 4 Breach Prevention Technologies that Require More Resources

Usage of External Security Services

All of survey respondents use an external security service, almost split equally between those outsourcing to an MDR service (53%) and using an MSSP service (47%). Note that 3% of companies reported using an MDR Service provide by their endpoint security provider.

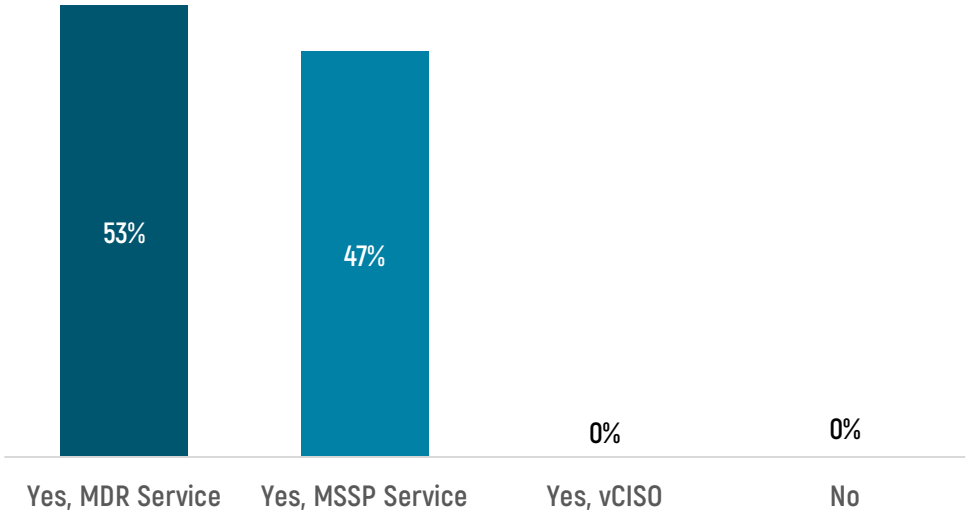

Figure 6 Usage of External Security Services

Most Important Services Provided by MDR

Looking at the most important services provided by MDRs, **the top three are 24x7 critical alerts and monitoring (33%), threat response remediation (21%) and threat response recommendations (21%)**.

Today's small security teams are looking to external companies to take some of the day-to-day toll of managing risk off of their shoulders. The deep experience of a specialized provider also ensures that important signals will not be overlooked and will be addressed properly. Always-on support comes out on top, by a seriously wide margin.

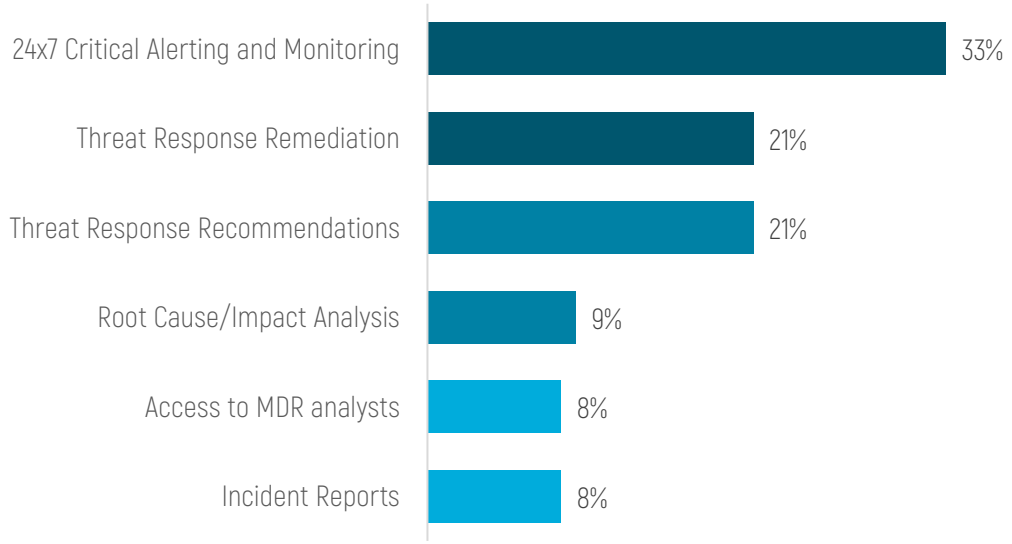

Figure 7 Most Important Services Provided by MDR

Perceived Value from EDR Solutions

It should come as little surprise to find that EDR was one of the top breach prevention technologies used by 70% of surveyed companies (see Top 10 Breach Prevention Technologies in Use / Plans, page 11). We've asked survey respondents who are using EDR, what is their perceived value from using EDR solutions. 87% saw value and 13% saw partial value.

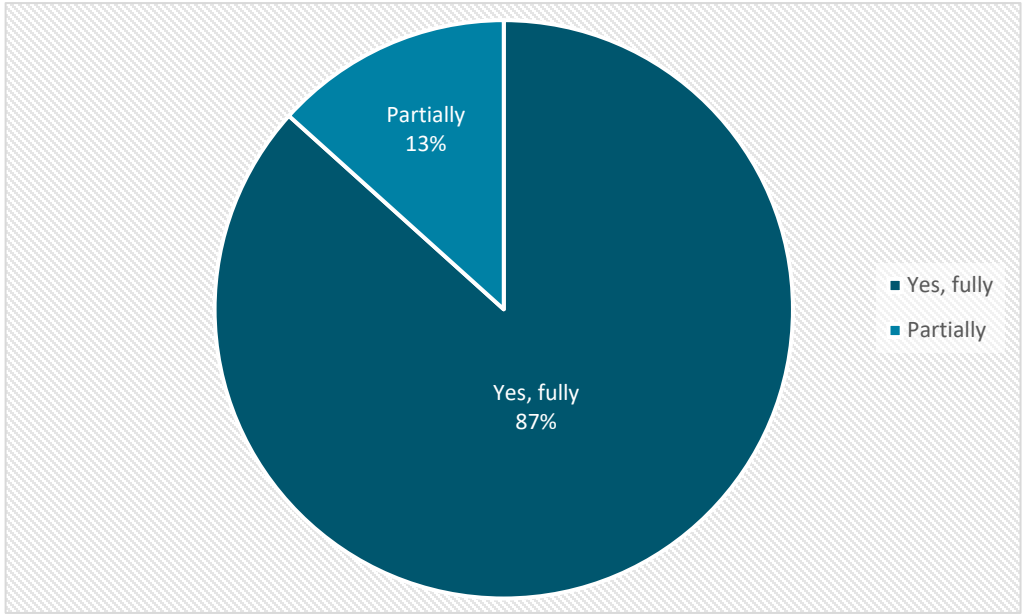

Figure 8 Perceived Value from EDR Solutions

Time to Implement and Become Proficient in EDR

We asked the companies using EDR, how long did it take them to implement and become proficient in EDR? For **79% of companies, it took their teams more than 4 months to finish their EDR deployment and become proficient in its use. Only 19% finished their EDR deployment and became proficient in 3 months or less**.

The time to proficiency is particularly important for smaller security teams that cannot afford their staff to be caught up in lengthy learning curves.

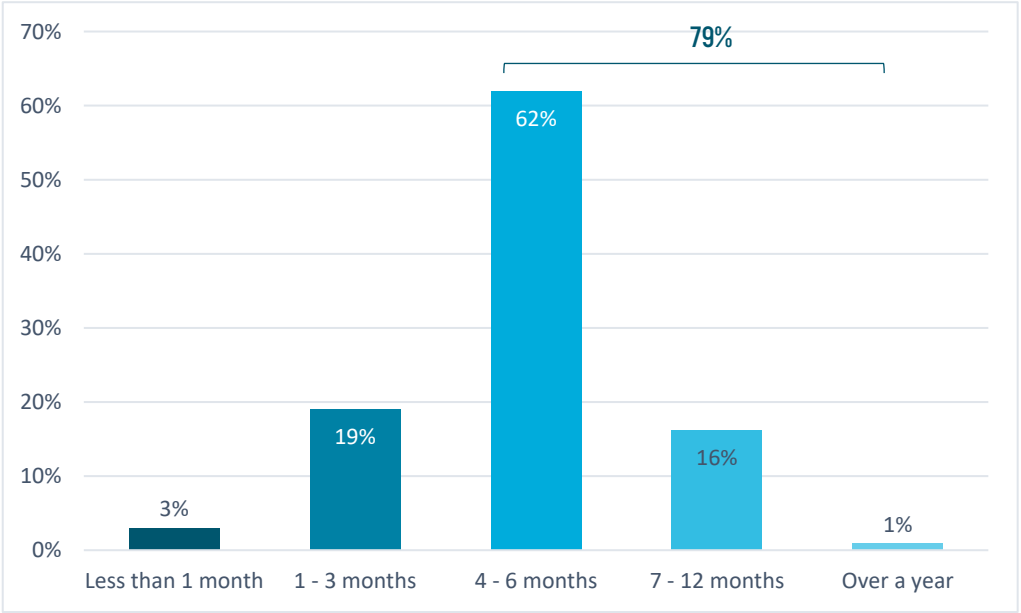

Figure 9 Time to Implement and Become Proficient in EDR

Preferred Deployment Methods for Security Technology

Public cloud is by far the #1 preferred deployment method for security technologies (57%), followed by on-premises (21%), Hybrid (13%) and virtual private cloud (9%).

Companies are looking for cost-effective, quick ways to implement security technologies, and lean toward approaches that allow them to outsource resource-intensive elements of security, such as infrastructure. As many security providers shift to cloud-only delivery models, note that 1 in 5 users continue to prefer on-premises deployment.

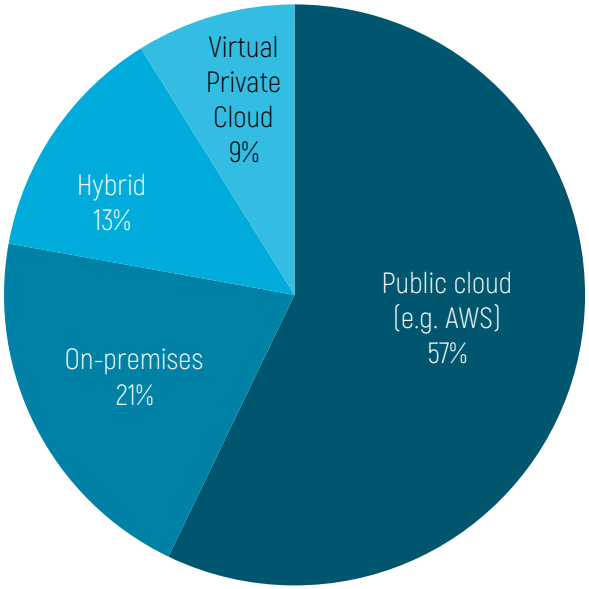

Figure 10 Preferred Deployment Methods for Security Technology

Primary Tool for Detecting Threats

NTA (Network Traffic Analysis) and NDR (Network Detection & Response) are the #1 tools for detecting threats (46%), followed by a combination of EDR & NTA (31%) and EDR (23%).

As more organizations see the value in leveraging both NDR and EDR tools for detecting threats, interoperability of network and endpoint security will become increasingly important. Some XDR solutions natively combine NDR and EDR out of the box, which is one of the key adoption drivers.

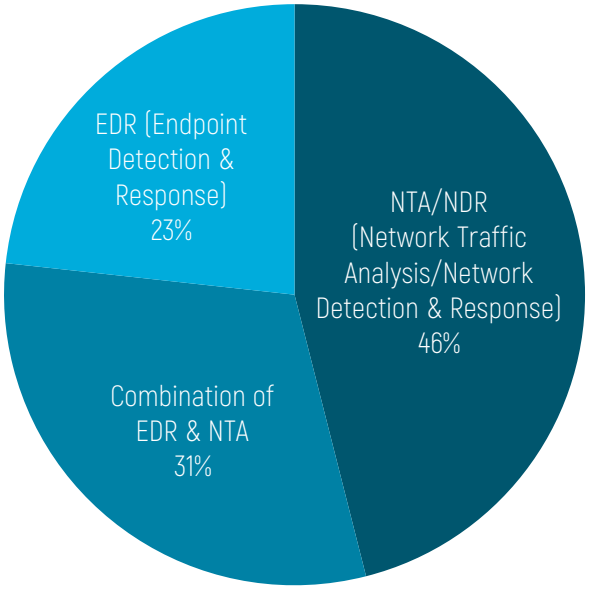

Figure 11 Primary Tool for Detecting Threats

Top 10 Considerations for Choosing a New Security Technology

We asked survey respondents for their top 10 considerations when choosing a new security technology. When dealing with smaller cyber security teams, we found that **at the top, 27% of CISOs, felt it was essential to have an existing team member who is familiar with the solutions.** This would potentially save companies the time it takes to become proficient with the new tool.

Other top considerations include how the tool complements existing security tools (26%). Industry and peer recommendations also had large percentages of the vote, at 23%, and 19% respectively.

It's clear than companies are looking for peace of mind, as early on in the cycle as the pre-sale process.

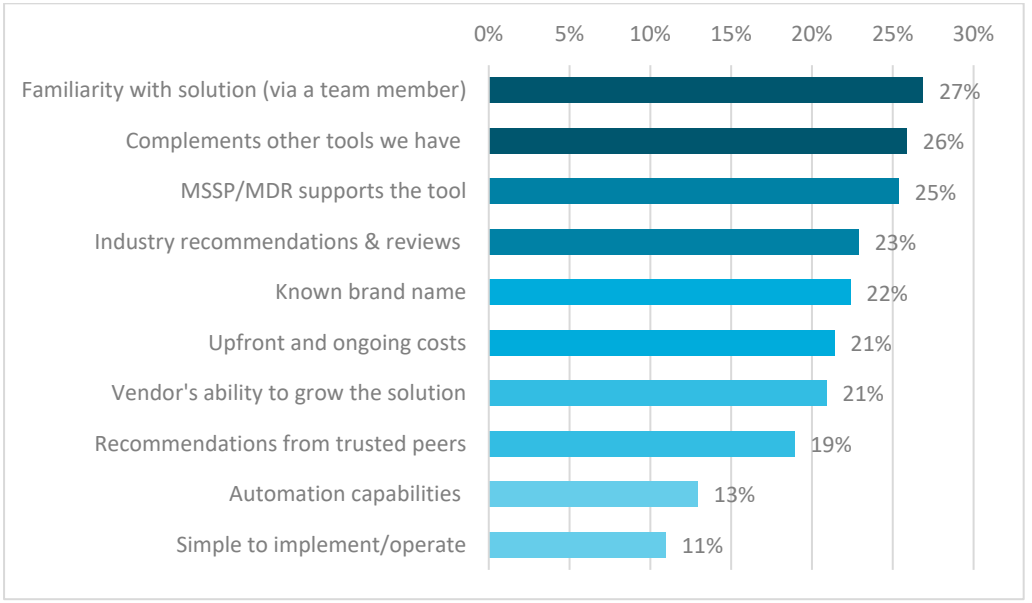

Figure 12 Top 10 Considerations for Choosing a New Security Technology

Challenges for Small Cyber Security Teams

Top Challenges Protecting Against Cyber Threats

When we looked at the 4 top challenges in protecting against cyber threats, 47% of respondents believe that their main **challenge is not enough skills or experience to protect against cyber-attacks, followed by rising threats outpacing investments in cybersecurity staff and tools (43%)**.

Other challenges include not enough budget for required tools (30%) and not enough personnel to address cyber risks (27%).

Companies need to turn towards out-of-the-box tools such as automation-led technology. These will take away some of the pressure to constantly upskill against the latest threats and relieve the burden on small security teams by automating otherwise manual, time consuming processes. However, it's clear that these tools need to be cost-effective enough so that acquiring them doesn't become just the next stumbling block.

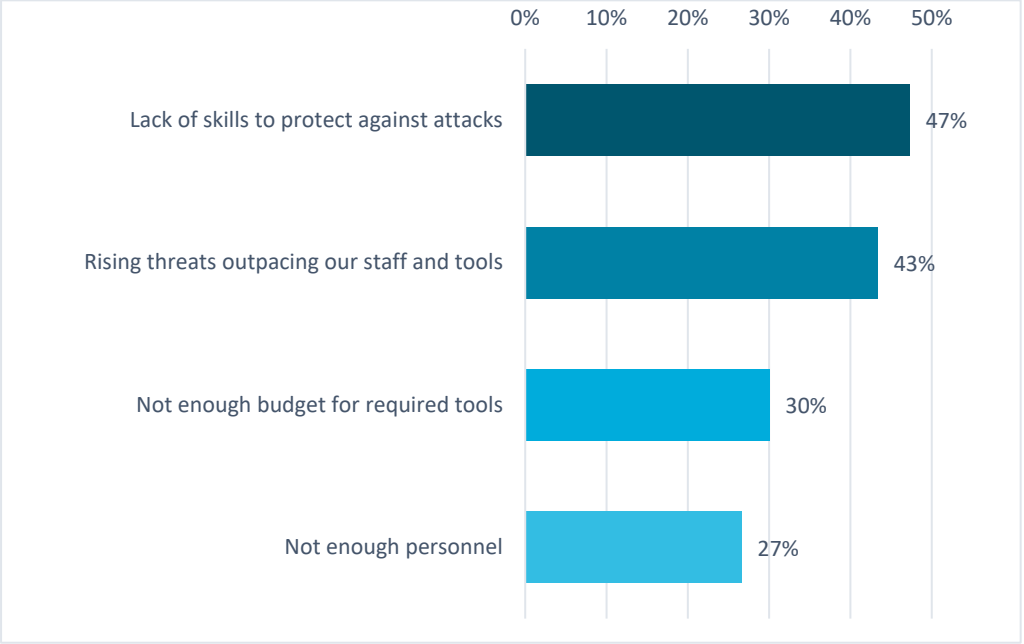

Figure 13 Top Challenges Protecting Against Cyber Threats

Risk of Attacks Compared to Large Enterprises

When we asked respondents about the challenges of smaller cyber security teams in protecting their organization from cyber-attacks, we found that **63% of companies feel their risk of attack is higher compared to larger Enterprises.** Enterprises have larger teams, budgets and tools in place, and survey respondents feel they are better placed to protect themselves as a result. In fact, only 7% feel their risk is smaller compared to large Enterprises.

This should come as no surprise, as we'll see in Methods for Handling Threat Alerts with Small Cyber Teams (page 27), 16% of companies ignore alerts that have been remediated automatically, and also ignore non-critical alerts. This may come down to a lack of resources, as we have seen through previous answers.

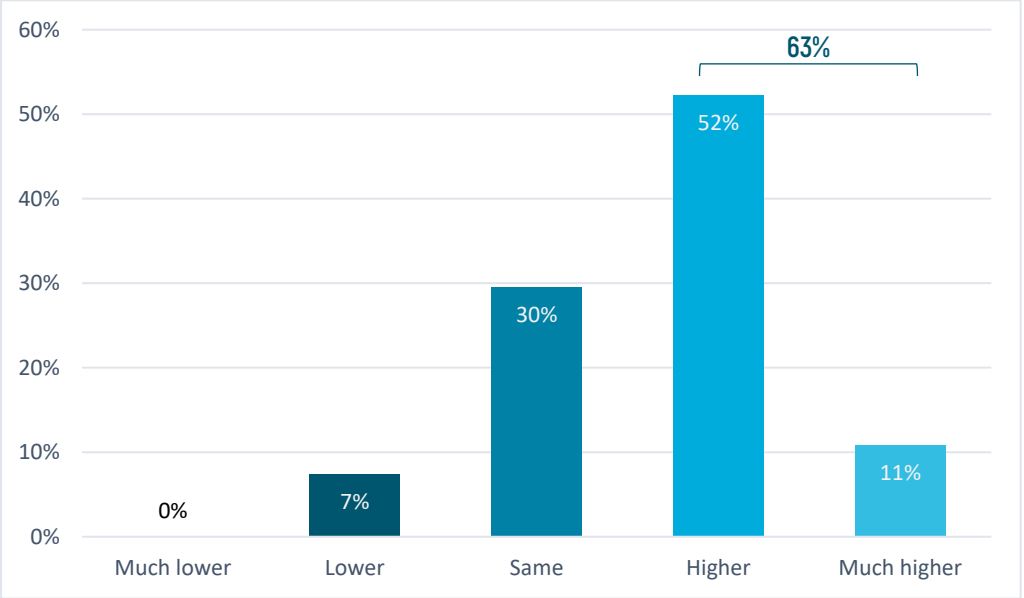

Figure 14 Risk of Attacks Compared to Large Enterprises

Implications of Small Security Teams

After understanding the challenges from smaller security teams (page 21), we asked survey respondents what the implications are of having smaller teams.

At the top of the list, **77% of companies indicated that their threat detection and response times are longer as a result of having a small security team**.

This was followed by 65% of companies indicating they would have acquired additional security tools if they had a larger security team and as result 58% indicated they only buy security technologies that are easy to implement and maintain.

In the fifth place, **57% of CISOs admitted that their ability to protect their company is lower than ideal**.

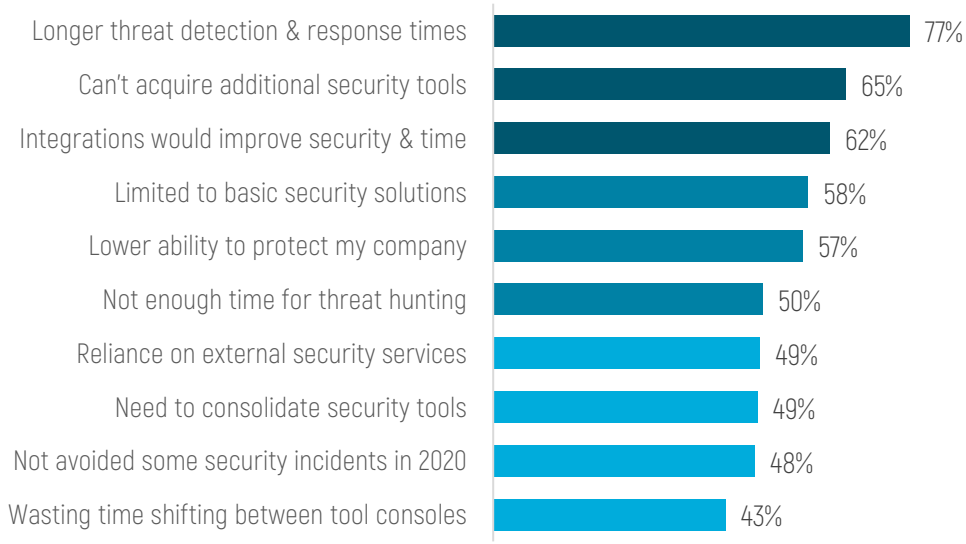

Figure 15 Implications of Small Security Teams

Top Tactics to Compensate for Lack of Large Security Teams

We've seen how smaller cyber security teams leads to challenges (page 21) and the implications this has for the companies. (page 23). So, how are companies managing this reality?

The top tactic chosen by 80% of companies was to invest more in automation solutions and processes.

In second place, 75% of companies plan to add one or more cybersecurity resources, 61% of companies plan to invest in security training and certifications and 56% plan to consolidate their security tools into a smaller number of platforms. Organizations want to achieve more with what they have, cutting down on unnecessary security tools to add visibility and control, along with adding and upskilling employees.

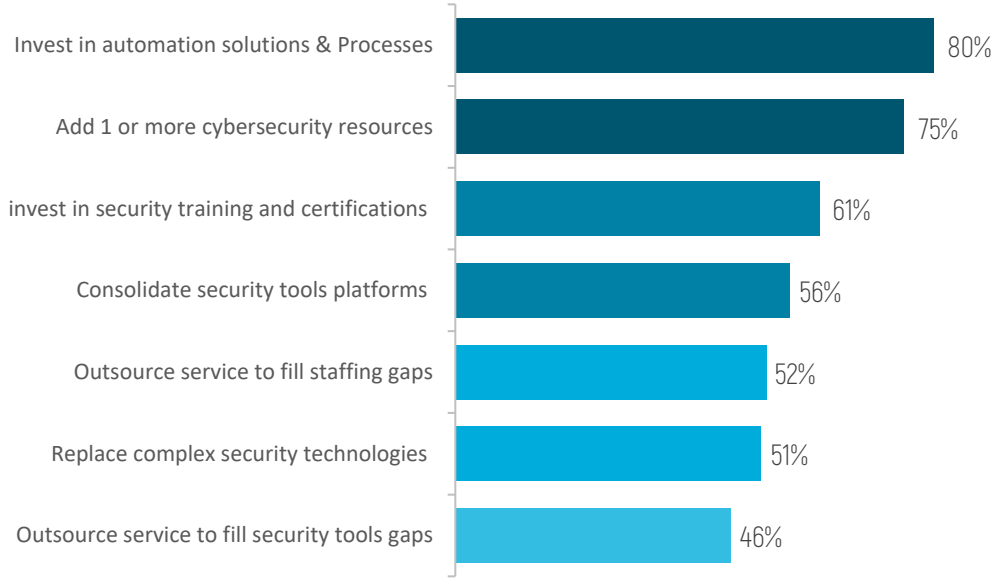

Figure 16 Top Tactics to Compensate for Lack of Large Security Teams

Operating and Investigating Using Threat Protection Products

Biggest Pain Points in Operating Threat Protection Products

We asked survey respondents, what are their biggest pain points when it comes to the operation of threat protection products.

The biggest pain selected by 51% of companies, and with a significant gap of 38% from the 2nd place, is the overlapping capabilities of disparate technologies.

Following that response, at 2nd and 3rd place, companies suffer from operational challenges. These are having too many dashboards (37%) and computing lag on deployed devices. (36%)

Organizations are looking for quick and straightforward tools that offer more 'bang for your buck', covering multiple challenges in one technology, and deployed without adding complexity to business operations.

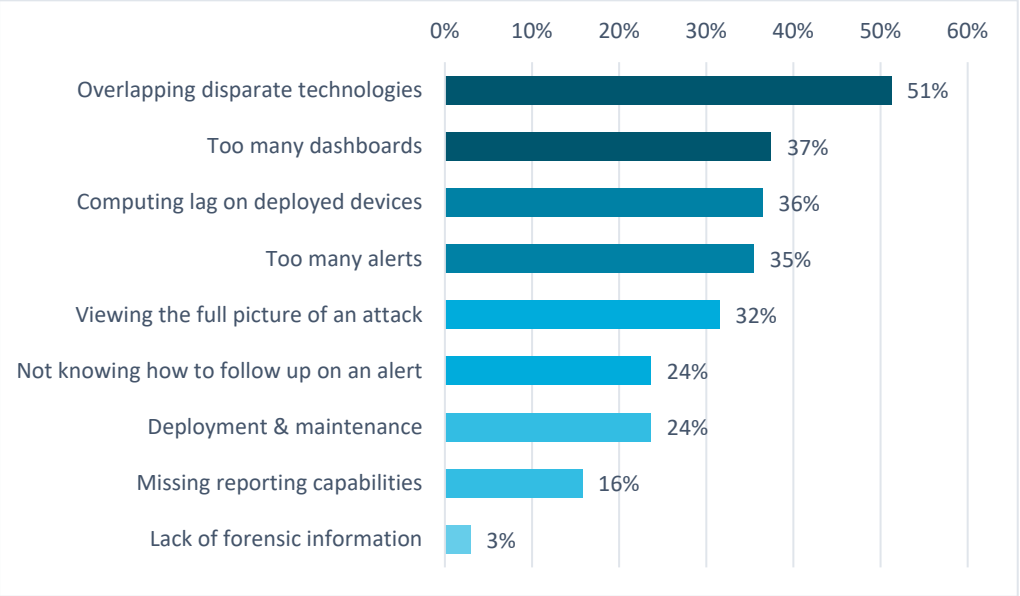

Figure 17 Biggest Pain Points in Operating Threat Protection Products

Methods for Handling Threat Alerts with Small Cyber Security Teams

When asked how companies are handling threat alerts with small cyber teams, **39% of survey respondents have a full-time team member that chases all the alerts**.

Other methods include ignoring alerts that have been automatically remediated (16%), only looking at critical alerts (14%) and outsourcing to external services such as vCISO, MDR or MSSP (28%).

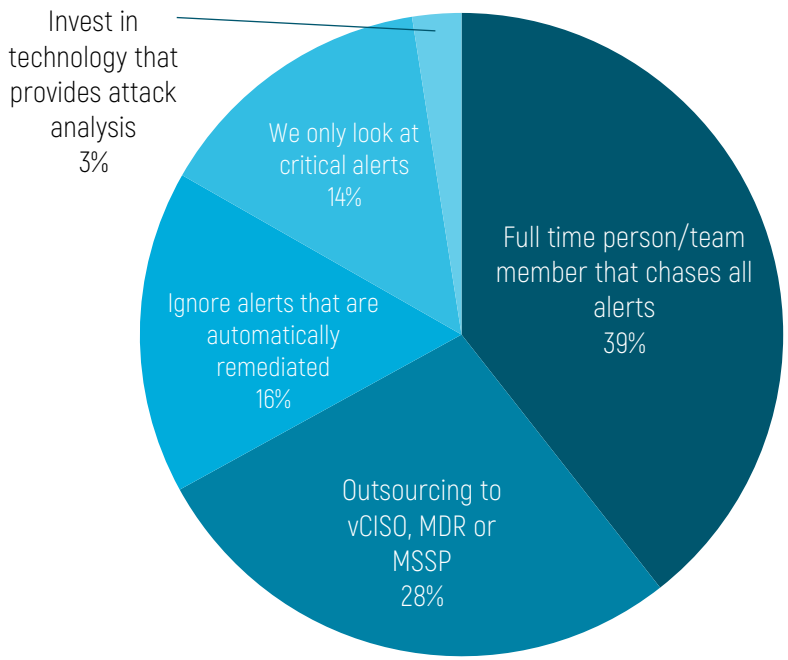

Figure 18 Methods for Handling Threat Alerts with Small Cyber Security Teams

Methods for Investigation and Remediation of High-Severity Security Incidents

Over half (55%) of survey respondents analyze and bring in an external service for remediation. 24% will analyze but only bring in an external service if needed, and 21% will immediately bring in external services.

Only 1 respondent said that they never bring in external services for mitigating security incidents. This 3rd party expertise is clearly an expected cost of managing security today.

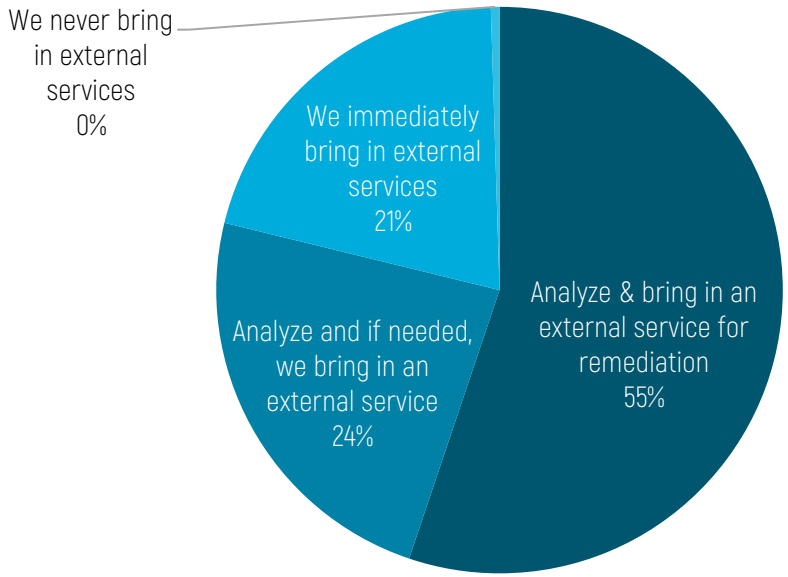

Figure 19 Methods for Investigation and Remediation of High-Severity Security Incidents

Demographics

Country of Residence

Figure 20 Country of Residence

About Cynet

Cynet 360 is the world's first Autonomous Breach Protection platform that natively integrates XDR endpoint, user and network attack prevention and detection capabilities with an incident engine that fully automates investigation and remediation actions, backed by a 24/7 world-class MDR service at no extra cost.

End to end, fully automated breach protection is now within reach of any organization, even with the smallest security teams.

LEARN MORE