cynet

2022 Survey of CISOs with Small Cyber Security Teams

July 2022

Table of Contents

Introduction and Key Findings

Introduction & Methodology

Last year, in our 2021 survey of small security teams, we spoke to 200 CISOs about the challenges of working in a small security team with 5 members or fewer in organizations of between 500-10,000 employees. We saw that these teams had unique challenges, holding a critical role in the company, and yet often working with a lack of budget and skills.

With the market shifting quickly, this year we have revisited our survey to see what has changed within the market. We asked CISOs to share their purchasing decisions, their budget constraints, and how they are facing key industry challenges such as the skills gap, technology overlap, and tools that are built for and focused on larger enterprise security teams.

By comparing this year's results with our 2021 report, we can see a growing cultural shift in the way small security teams are handling their unique challenges. The technologies CISOs rely on have changed dramatically from one year to the next, and the risk of overlapping security tools and a lack of visibility is more prominent than ever. Virtually all respondents admit to pain points in operating their security products and face barriers in maintaining their security posture. One key message shines through the data, more emphasis on consolidating technologies to gain greater visibility and control.

Methodology

To gain this insight, we repeated our survey of 200 CISOs from the United States, Canada and the United Kingdom, all who work for commercial companies with 500-10,000 employees. Uniquely in the research published in the market, they are all the CISO of companies with small security teams of 5 people or fewer. The survey was completed by Global Surveyz, an independent survey company, and took place during Q1 2022.

The respondents were recruited via a B2B research panel and invited via email to complete the survey. The average amount of time spent on the survey was 7 minutes and 10 seconds. The answers to the majority of the non-numerical questions were randomized in order to prevent order bias in the answers.

Key Findings

1 The surge in remote work has accelerated the use of EDR technologies

While in 2021, 52% of CISOs were relying on endpoint detection and response (EDR) tools, this year that number has leapt to 85%. In contrast, in 2021, 45% were using network detection and response (NDR) tools while this year just 6% have NDR in place. EDR is also the number one tool for detecting threats, at 77% with NDR almost non-existent at 3%, despite being 46% in 2021. Organizations are seeing the value of EDR, as well as extended detection and response (XDR) tools which combine EDR with integrated network signals (up from 15% usage to 30% in 2022). In large part this is likely to be because of remote working norms, where employees are working outside of the company network, which is more difficult to secure.

2 90% of CISOs use an MDR solution, up from 53% in 2021

In 2021, 47% of CISOs relied on a Managed Security Services Provider (MSSP), while 53% were using an MDR service. This year, just 21% are using an MSSP, and 90% are using managed detection and response (MDR). There is a huge skills gap in the cybersecurity industry, and CISOs have an increasing amount of pressure on recruiting internally. Especially in small security teams where headcount is not the answer, professionals are looking to outsourced services to fill this gap. MDR services are a way to get extra resources by outsourcing rather than hiring.

3 Overlapping capabilities of threat protection tools is the #1 pain point for small security teams

87% of companies with small security teams have pain points in managing and operating their products for threat protection. For 44%, that's overlapping capabilities, while 42% struggle to visualize the full picture of an attack. These challenges are connected, as it's much harder to get one single view with multiple dashboards and tools. In many ways, having multiple technologies with the same capabilities and features can make security a lot harder, showing the importance of consolidation.

4 Small security teams are paying attention to fewer security alerts than this time last year

There is a dangerous trend in the attention that small security teams are placing on their security alerts. For example, last year 14% of CISOs said they only look at critical alerts, while this year the number has jumped to 21%. In addition, organizations are increasingly letting automation take the wheel. Last year, 16% said they ignore automatically remediated alerts, and this year that is true for 34% of small security teams. Any alert could be part of something larger, so it's essential that security teams don't place over-reliance on automated threat remediation and ignore root cause analysis, as this puts them at greater risk.

5 96% of CISOs are planning to consolidate their security platforms

Consolidating multiple security tools and technologies down to fewer, more robust and comprehensive tools is an essential task, and almost all CISOs have it on their roadmap, up from 61% in 2021. Not only would this process reduce the number of alerts – making it easier to prioritize and view all threats – respondents believe consolidation will stop them from missing threats (57%), reduce the need for specific expertise (56%), and make it easier to correlate findings and visualize the risk landscape (46%). XDR technologies are the preferred method of consolidation, with 63% of CISOs calling it their top choice.

Security Teams and Budgets

Company Size and Cybersecurity Team Size

Our focus for this survey was medium to large companies (500-10,000 employees) with small security teams of 5 employees or fewer. We chose to focus on these, since as we will see, smaller teams face different challenges compared to large cybersecurity teams. On average, survey respondents work in companies with 1,713 employees.

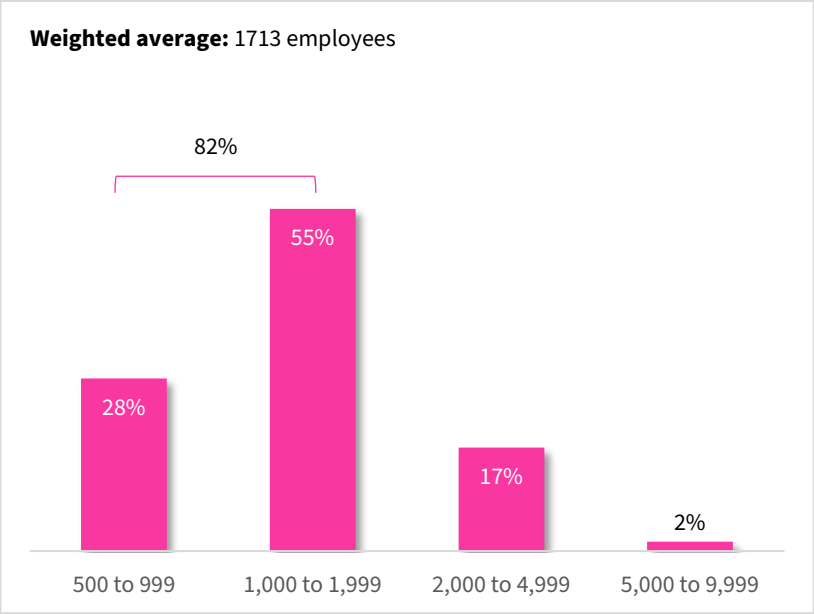

Figure 1 Company Size

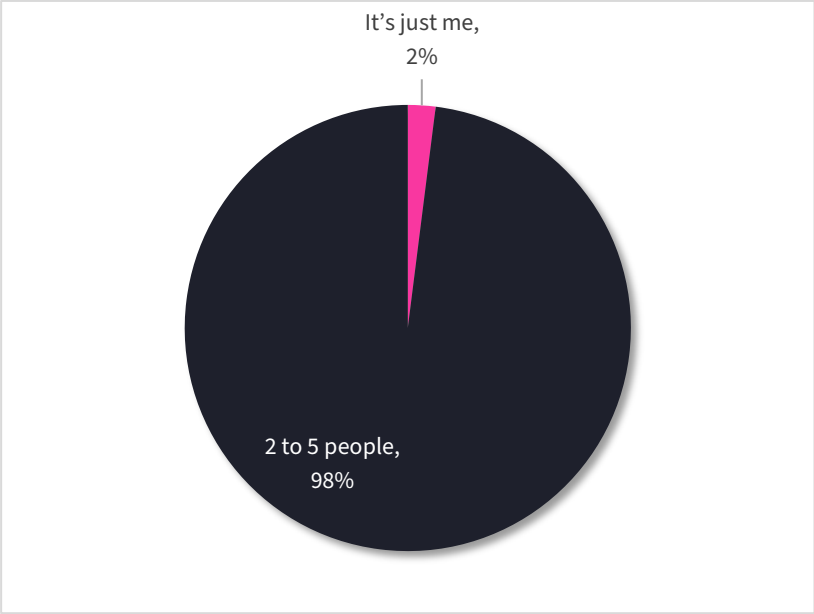

Figure 2 Size of Security Team

*Percentages on figure 1 do not add up to 100% due to rounding up of numbers

Security Budgets in 2021 and Planned Budget for 2022

With small team sizes, comes smaller budgets. 95% of survey respondents have a budget of under $1,000,000. The survey respondents' average security budget in 2021 was $436K.

However, budgets are growing. **73% of survey respondents are planning to increase their budget by 5% or more,** with 11% planning to increase their budget by more than 10% this year. Only 2% plan to decrease their budgets by 5%-10%, and none of the survey respondents will decrease their budget by more than 10%.

*Percentages on both figures do not add up to 100% due to rounding up of numbers

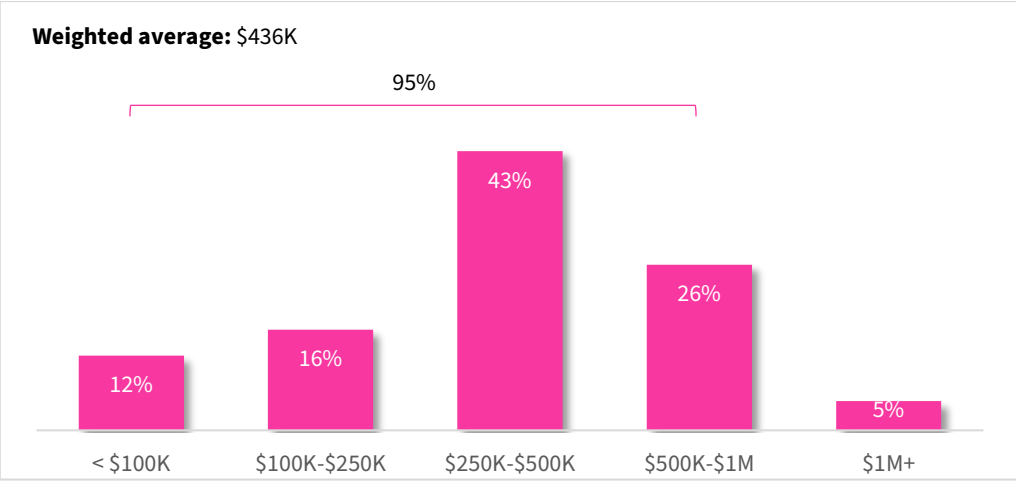

Figure 3 Security Budget for 2021

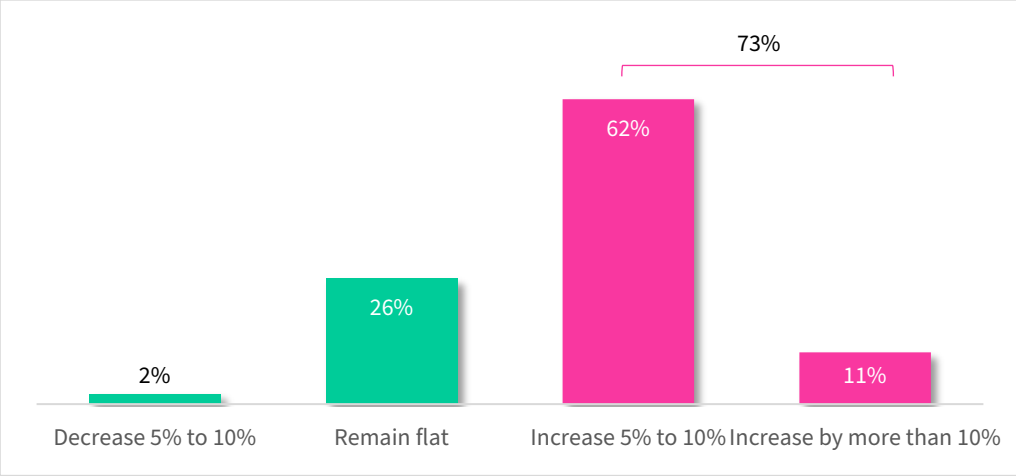

Figure 4 Budget Growth for 2022

Breach Prevention Technology

Top Breach Prevention Technologies in Use and Plans

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

The top breach prevention technology used by almost all respondents is EDR/EPP (85%), followed by XDR (30%). **This is a huge rise from 2021 adoption rates, which were 52% for EDR, and 15% for XDR.** In contrast, while NTA/NDR was second place in 2021 at 45% adoption, this year just 6% are using this technology.

It's clear that CISOs are seeing the value in robust EDR/XDR solutions, especially in a remote working landscapes where employees are often not on the company network.

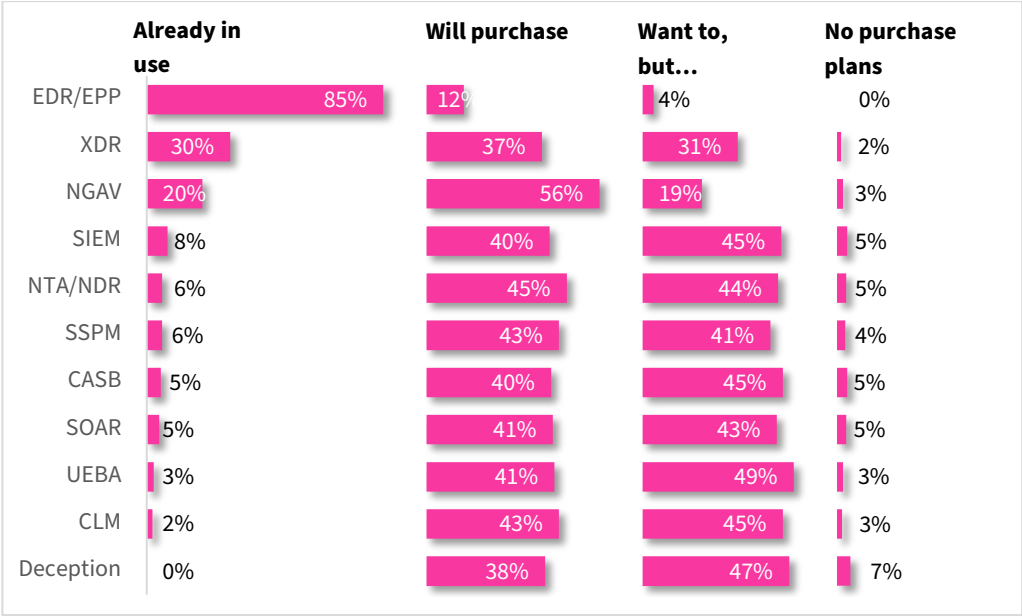

Figure 5 Top Breach Prevention Technologies in Use and Plans

Breach Prevention Technologies Companies Want but Cannot Afford

Using column three from figure 5, we looked into the companies who would like to be using certain breach prevention technologies but feel they cannot. The two main reasons preventing CISOs from purchase are high costs and lack of people to operate.

The top breach prevention technologies companies feel are prohibitively expensive are Deception (35%], UEBA (34%), and CASB (33%).

They also selected the ones they want but do not have the people to operate and those include SOAR (18%), CLM (17.5%) and UEBA (15%).

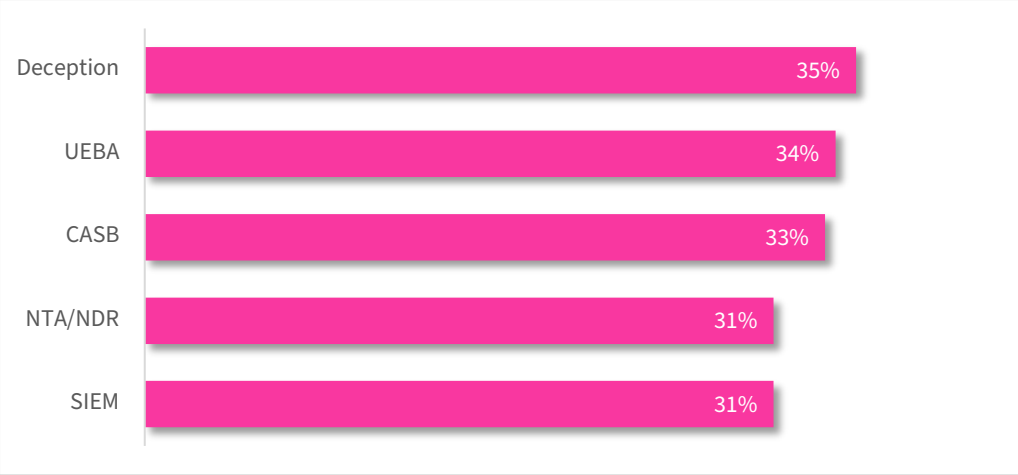

Figure 6 Breach Prevention Technologies that are too Expensive

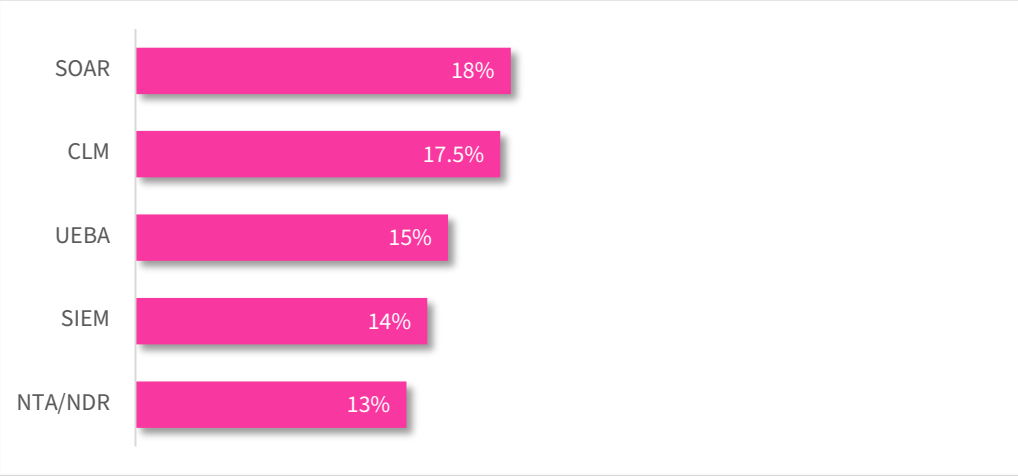

Figure 7 Breach Prevention Technologies that Require More Resources

Usage of External Security Services

90% of surveyed CISOs use an external security service, and all of those respondents use an MDR service. Additionally, some also use MSSP (21%) and vCISO (15%).

This is a huge leap from 2021 numbers, where the numbers were split almost evenly, 53% using MDR and 47% using MSSP.

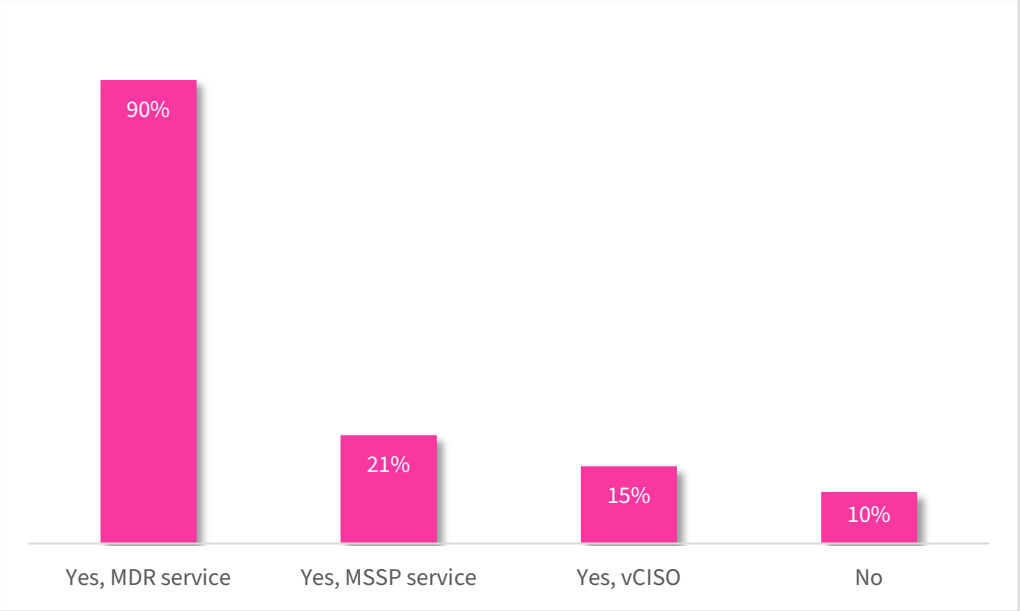

Figure 8 Usage of External Security Services

*This question allowed more than one answer and as result, percentages will add up to more than 100%

Most Important Services Provided by MDR

The most important MDR services are threat response remediation and 24/7 critical alerting and monitoring.

Looking at the most important services provided by MDRs, we can see **threat response remediation (38%), 24x7 critical alerts and monitoring (32%), and incident reports (14%)**.

Today's small security teams are looking to external companies to take some of the day-to-day toll of managing risk from their shoulders. The deep experience of a specialized provider also ensures that important signals will not be overlooked and will be addressed properly. While in 2021, always-on support was the #1 service provided by MDRs, this year it has been knocked off the top spot by threat response remediation.

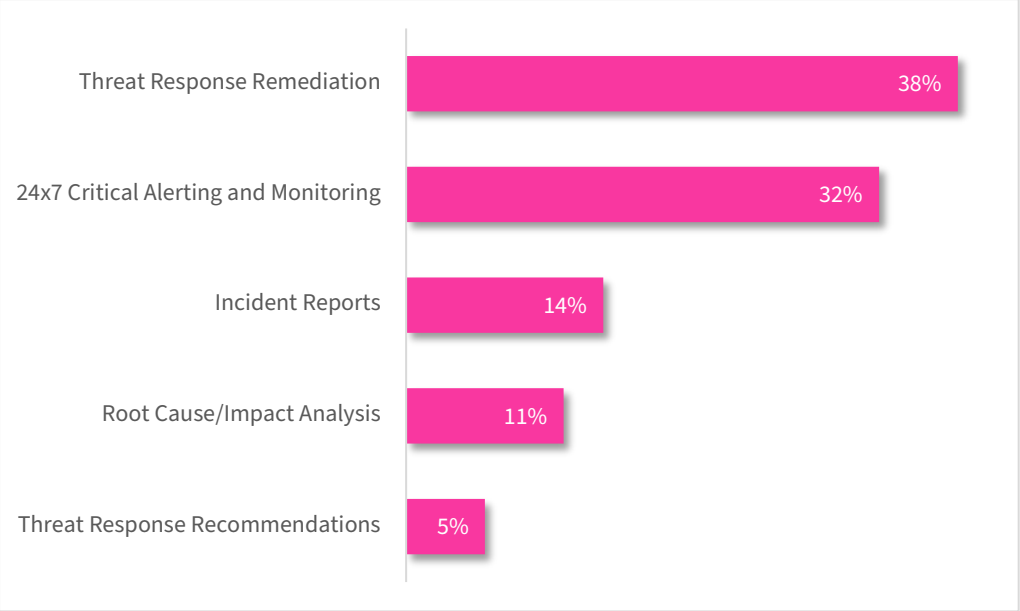

Figure 9 Most Important Services Provided by MDR

Security Products in Use & Integration Required Security Products

On average, companies use 19 security products, and 89% of them (17 out of 19) require integration with other security products. Despite these companies having smaller security teams, the challenges are still the same as in large organizations, which means all organizations rely on multiple tools for protection. As many of these require integrations, this workload can push small security teams to their limit.

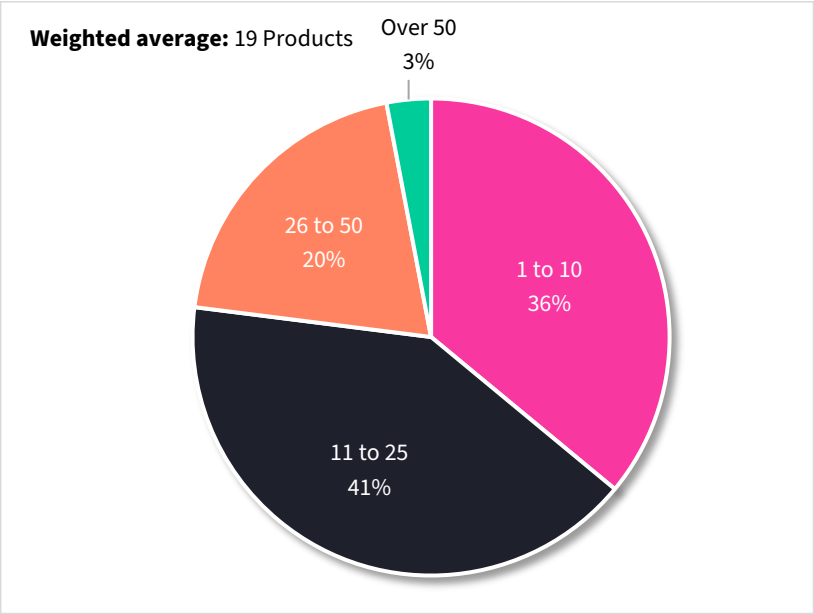

Figure 10 Number of Security Products in Use

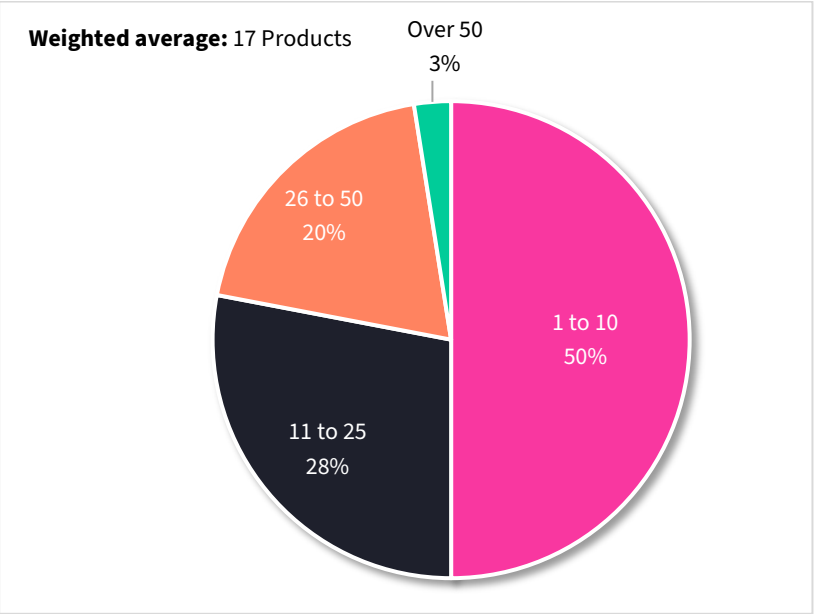

Figure 11 Number of Security Products that Require Integration with Other Security Products

Time to Implement and Become Proficient in EDR

On average, it took approximately 18 months for small security teams to implement, become operational, reach steady state, and become proficient in their EDR technology. The time to implement and reach proficiency is particularly important for smaller security teams that cannot afford their staff to be caught up in lengthy learning curves.

As shown in Figure 13, 26% of the companies with over 2000 employees surveyed take over a year just to become proficient using their EDR system. This could reflect less time available because these companies also tend to have more security technologies to operate and learn. It could also reflect these larger companies purchasing EDR systems that are more suited to large enterprises, requiring a very steep learning curve, extensive configuration, and continual modification.

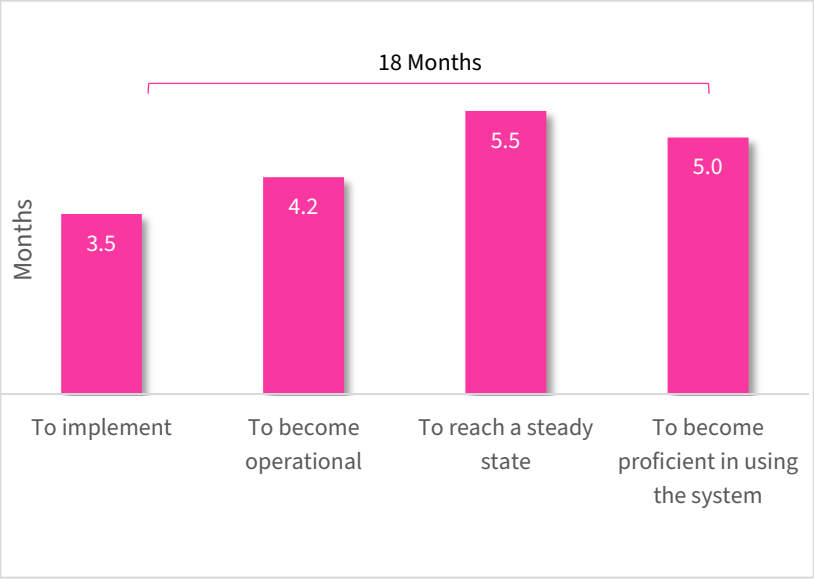

Figure 12 Months to Implement and Become Proficient in EDR (Weighted Average)

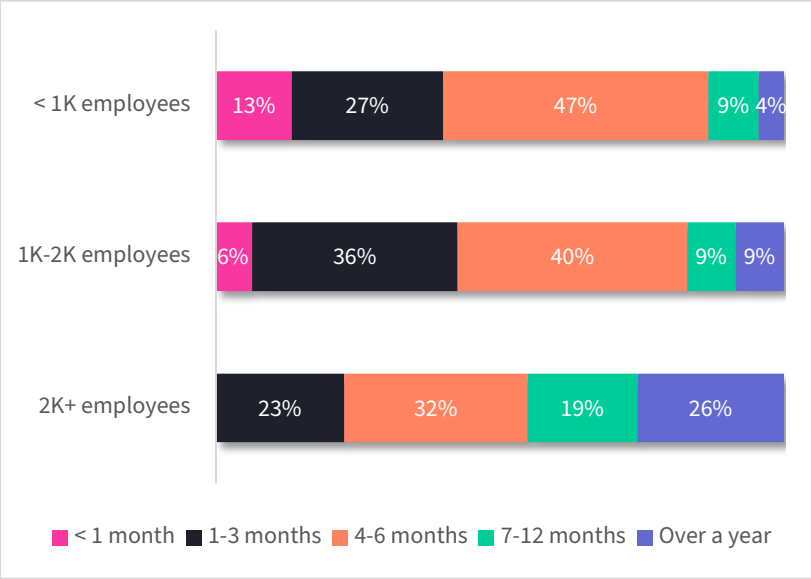

Figure 13 Time to Become Proficient by Company Size

Top Reasons for Delay in Deploying EDR Systems

The top reasons for delay in deploying EDR systems are not having infrastructure ready (32%), and lack of human resources (30%).

When looking at these reasons by company size, 23% of larger companies blamed their EDR implementation delay on their vendor not being responsive (compared to 7-11% in smaller companies). This supports the likelihood that these companies acquire EDR systems provided by vendors that target larger enterprises, and therefore don't pay sufficient attention to the needs of these relatively smaller companies.

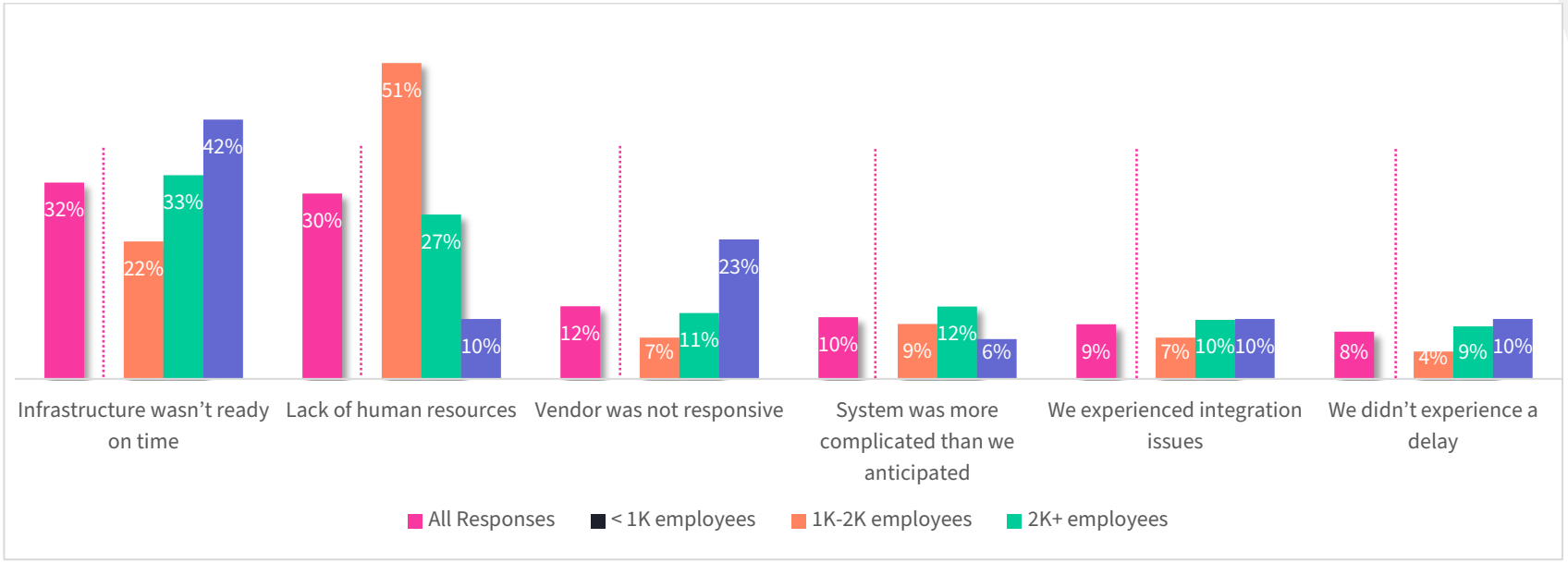

Figure 14 Top Reasons for Delay in Deploying EDR Systems

Preferred Deployment Methods for Security Technologies

Public cloud is by far the #1 preferred deployment method for security technologies (64%), followed by on-premises (17%), virtual private cloud (12%), and hybrid (8%). Public cloud has continued to grow as the industry sees a steady migration from on-premises, and adoption has risen from 57% in 2021.

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 6 users continue to prefer on-premises deployment.

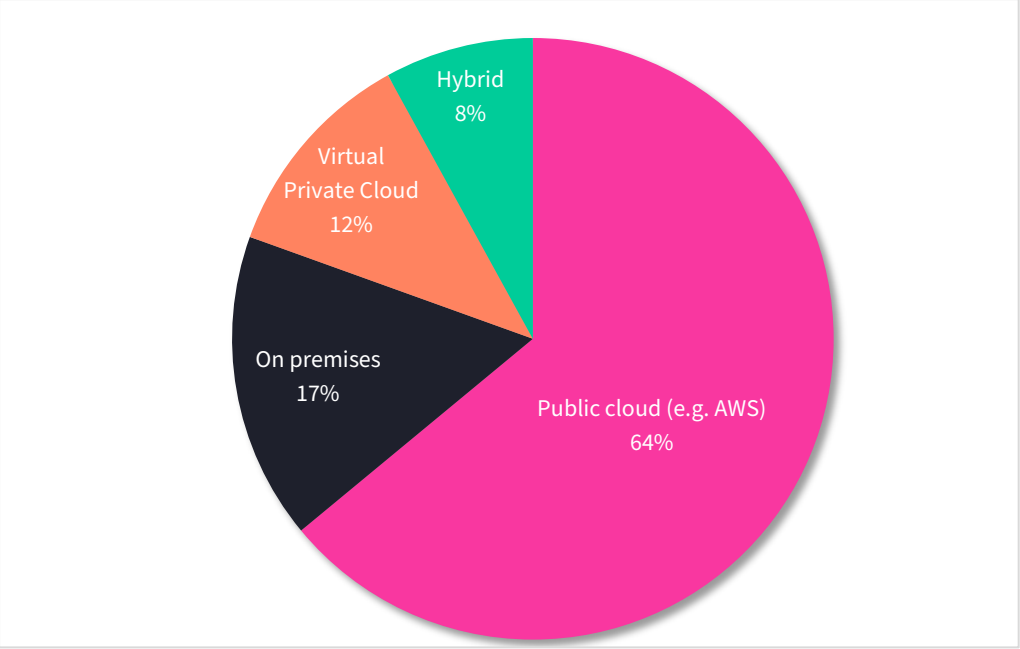

Figure 15 Preferred Deployment Methods for Security Technologies

Primary Tools for Detecting Threats

EDR is the #1 tool for detecting threats (77%), followed by XDR (21%) and NTA/NDR dropping significantly from 46% in 2021 to just 3% this year.

More organizations are seeing the value in leveraging EDR and XDR tools for endpoint security and detecting and mitigating threats. Some XDR solutions natively combine NDR and EDR out of the box, which is one of the key adoption drivers. NDR tools are dropping out of favor, perhaps because of the operational complexity and/or because of the rise in remote working.

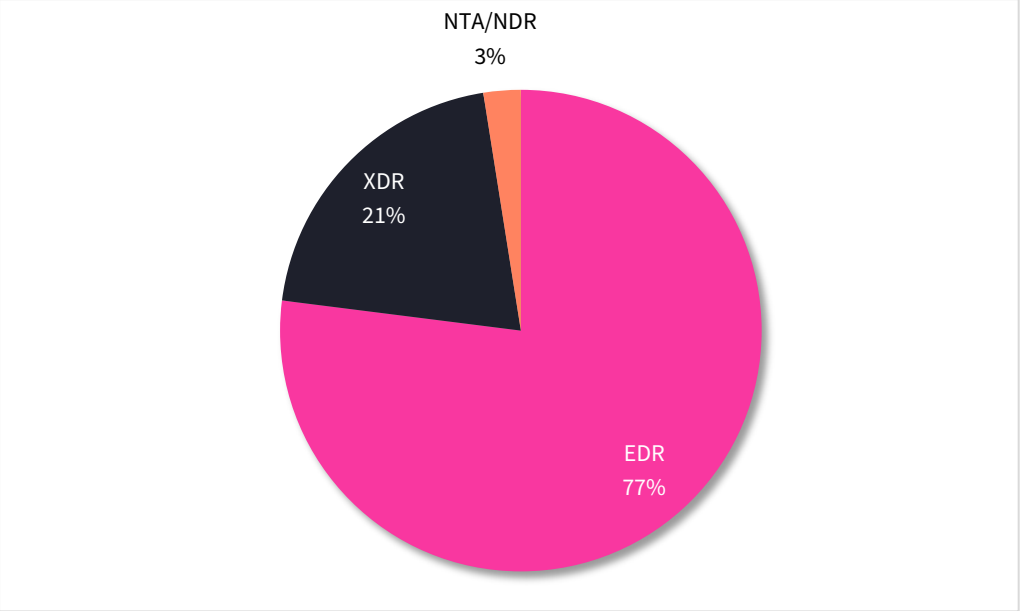

Figure 16 Primary Tools for Detecting Threats

*Percentages do not add up to 100% due to rounding up of number

Top Considerations for Choosing New Security Technologies

The top features taken into consideration when choosing new security technologies are the feature set (45%), scalability and future growth (39%), and the technology's automation capabilities (39%). With limited budgets and staff, feature-full technology platforms continue to be important for small security teams

From a commercial perspective, implementation costs are the top consideration (50%), followed by training cost (39%) and purchase price (38%). Security teams are looking for short, straightforward implementation cycles that don't break the bank.

Peer recommendation also plays a pivotal role, with 49% ranking brand name as very important. With hundreds of vendors, a known brand name can feel like a safer bet, tried and tested in the market.

It's clear than companies are looking for better information early in the purchase process. Initiatives like the MITRE ATT&CK Evaluation can help companies make a smart decision with the budget they have.

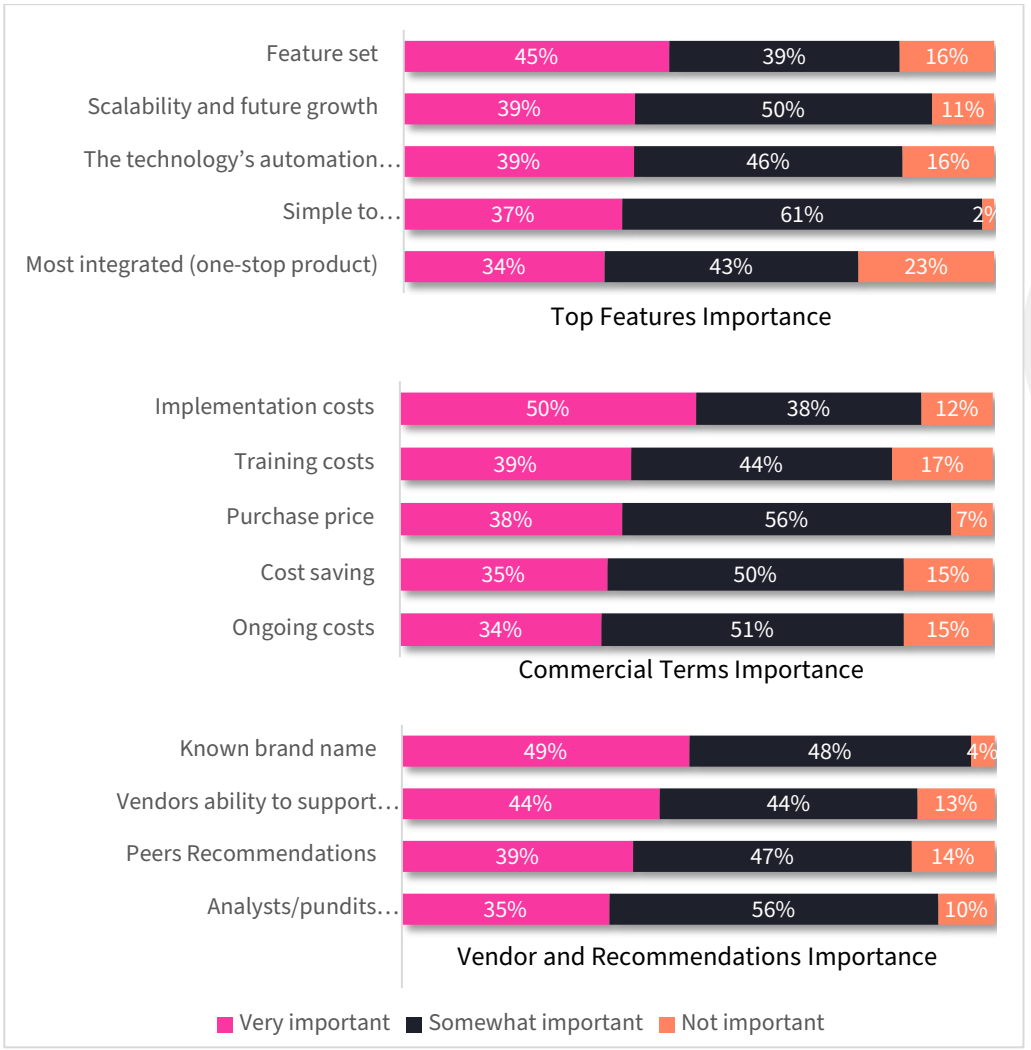

Figure 17 Top Considerations for New Security Technologies

Challenges for Small Cyber Security Teams

Top Pain Points in Operating Threat Protection Products

87% of companies with small security teams admit they have pain points in operating threat protection products, the biggest ones include having overlapping capabilities of disparate technologies (44%), viewing the full picture of an attack (42%), and deployment and maintenance of disparate technologies on one machine (41%).

These challenges impact one another. For example, overlapping capabilities of disparate technologies inhibit the ability to view the full picture of an attack.

In many ways, having multiple technologies with the same capabilities can make security harder – showing the importance of consolidation.

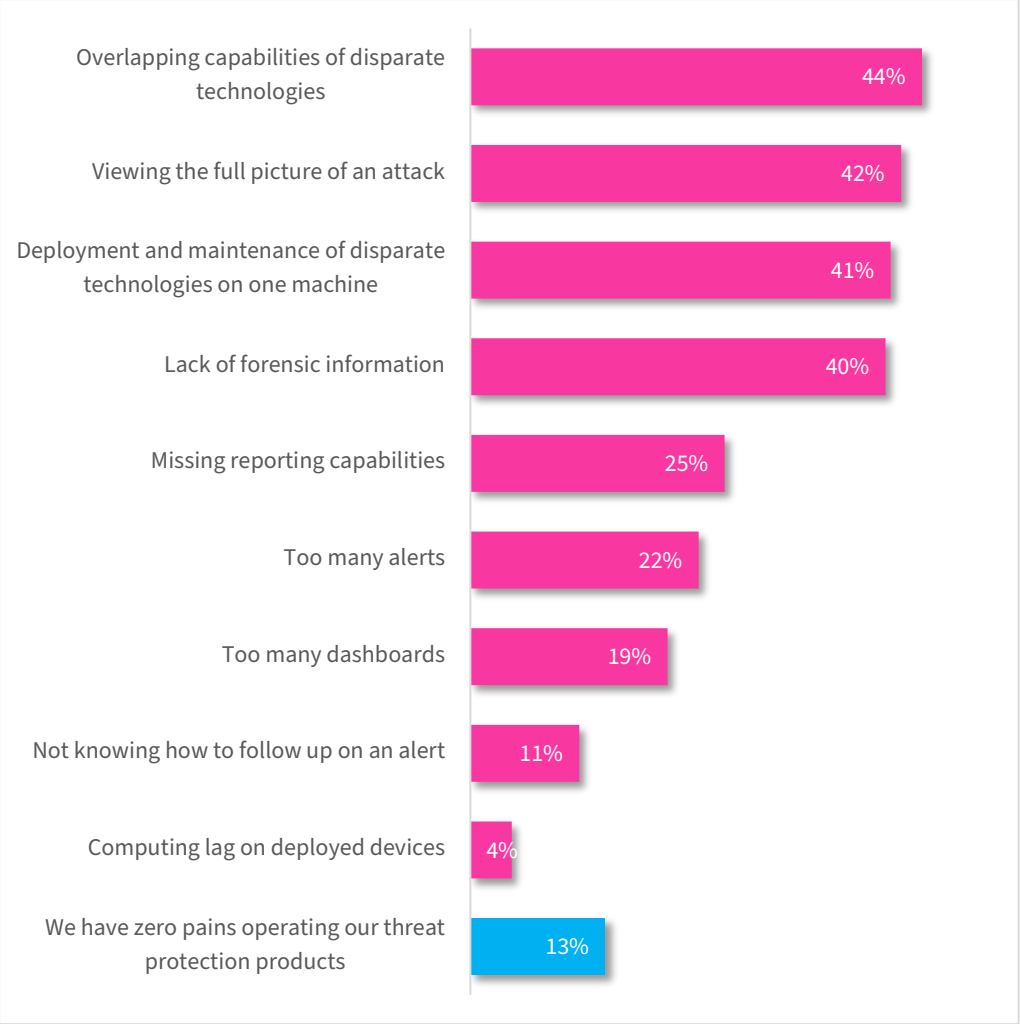

Figure 18 Top Pain Points in Operating Threat Protection Products

*This question allowed more than one answer and as result, percentages will add up to more than 100%

Top Barriers in Maintaining Security Posture

94% of respondents have barriers in maintaining their security posture. The top barriers are lack of skilled security personnel (40%), excessive manual data analysis (37%), and remote work force and many locations (37%).

As smaller organizations have less oversight, they can't afford the mistakes that come from skills gaps and the effort of manual data analysis.

The skills shortage is an industry-wide challenge, which we can be alleviated with the help of outsourcing MDR to more automated technologies such as XDR.

Figure 19 Top Barriers in Maintaining Security Posture

*This question allowed more than one answer and as result, percentages will add up to more than 100%

Risk of Attack in Comparison to Large Enterprises

58% of companies feel that their threat of attack is higher than large enterprises.

Those with higher security budgets of over $500K feel that their threat of attack is even higher (62% indicated their risk of attack is higher).

Smaller companies face the same threats as larger organizations, but with smaller budgets, as well as smaller and often less-experienced teams.

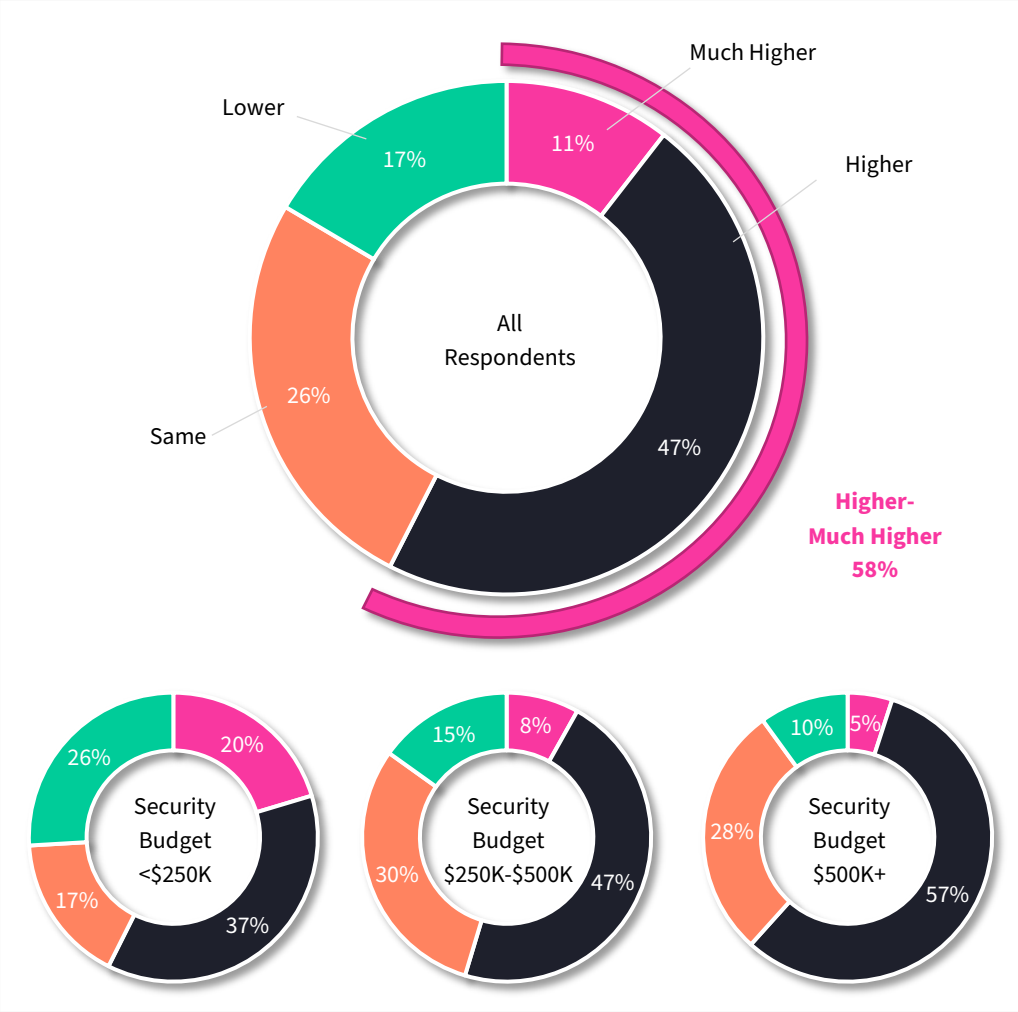

Figure 20 Risk of Attack in Comparison to Large Enterprises

Responding to Alerts with Limited Personnel

35% of survey respondents have a full-time team member that chases all the alerts, down slightly from 39% in 2021.

More companies are using automation than in 2021, as last year just 16% said they rely on ignoring automatically remediated alerts, and this year that number has jumped to 34%. This could pose a risk if organizations ignore alerts which could be part of a larger attack.

In addition, 21% say they only look at critical alerts (21%) and 7% outsource to external services such as vCSO, MDR or MSSP (7%).

Figure 21 Responding to Alerts with Limited Personnel

*Percentages do not add up to 100% due to rounding up of numbers

Approach Toward Selecting Security Tools

Most of the respondents agreed that when selecting security tools for their organization they look to external security services to extend their capabilities (63%). This is likely another direct consequence of the skills gap.

Ease of implementation (55%) is clearly an essential element of onboarding new tools. For smaller security teams, onboarding a technology which is meant for large enterprises is a sure-fire route to implementation problems.

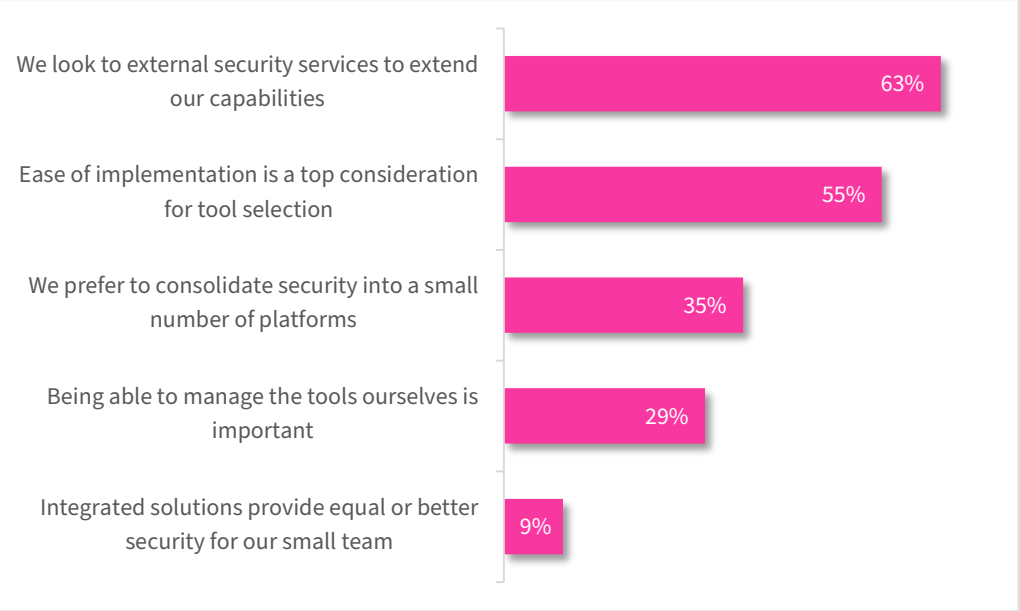

Figure 22 Approach towards Selecting Security Tools

*This question allowed more than one answer and as result, percentages will add up to more than 100%

2022 Top Tactics to Compensate for Lack of Large Security Teams

Rather than increasing the number of security staff, organizations want to achieve more with what they have, cutting down on unnecessary security tools (35%), and investing more in training and certifications (34%).

Investing in automation was indicated as a “very necessary” tactic by 28% of CISOs (figure 23). When further comparing this by the size of their security budgets (figure 24), we see this is becoming increasingly important as budgets grow. The larger the budget, the more importance is placed on automation.

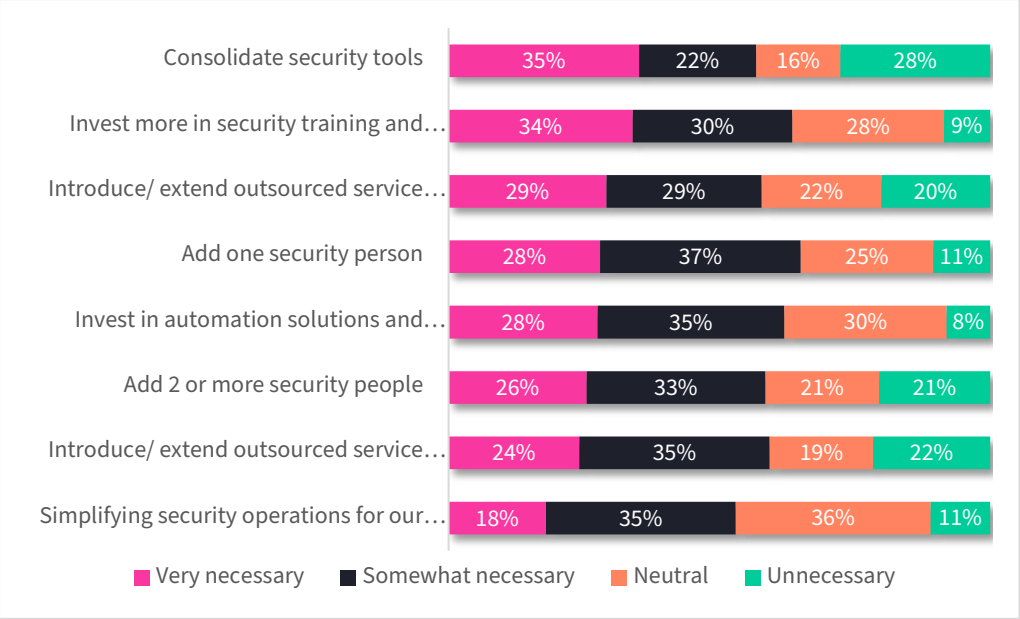

Figure 23 2022 Top Tactics to Compensate for Lack of Large Security Teams

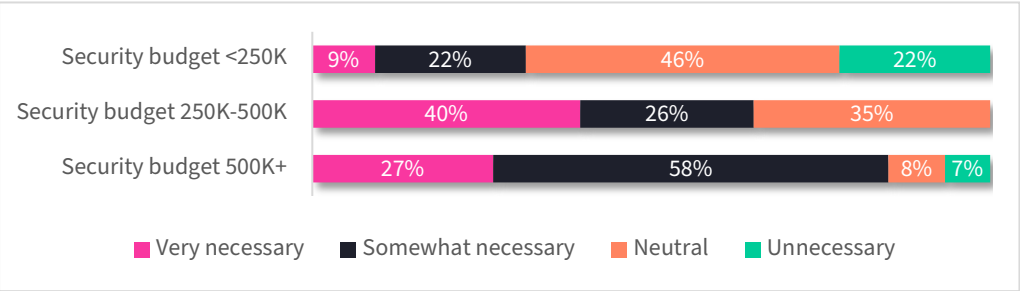

Figure 24 Invest More in Automation Solutions & Processes by Security Budget

Consolidating Security Platforms

Nearly all respondents (96%) plan to consolidate their security platforms (figure 25). Most of them plan to use XDR for their security platforms (figure 26), which is specifically designed to solve for the challenge of consolidation.

The top reasons for consolidating are missing threats because of gaps between products (57%), lack of expertise in some of the systems (56%), and difficulties in correlating findings across various products (46%).

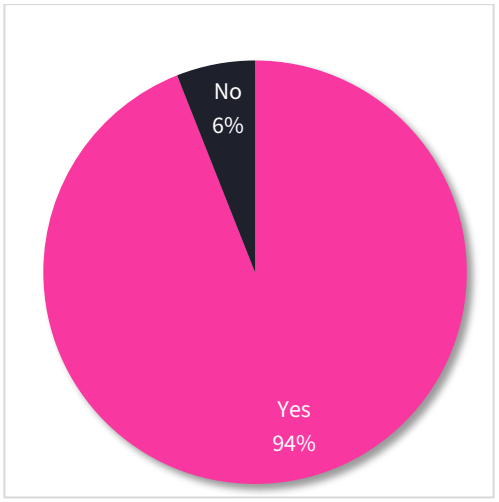

Figure 25 Plans for Consolidating Security Platforms

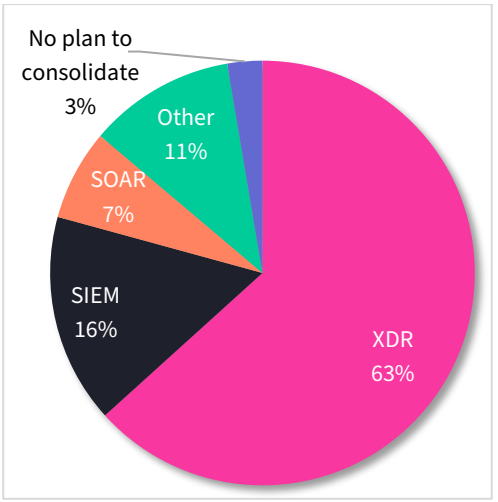

Figure 26 Preferred Type of Consolidation

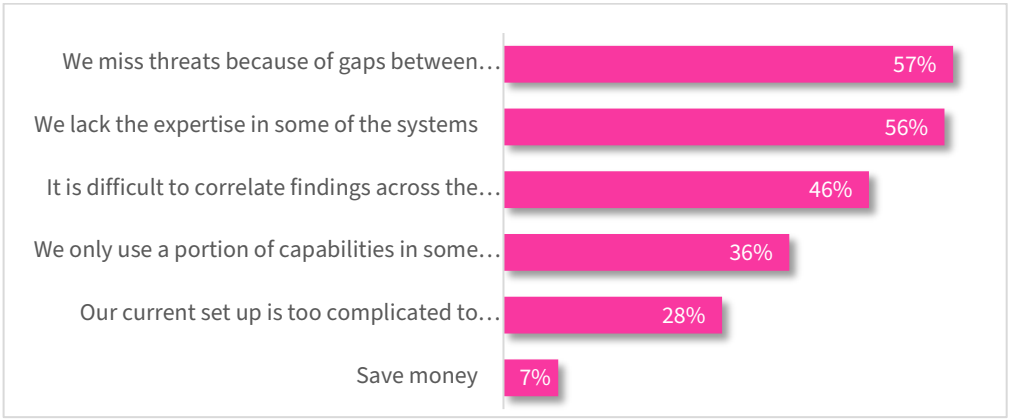

Figure 27 Top Reasons for Consolidating

*Percentages on figure 27 add up to more than 100% as this question allowed more than one answer

Demographics

Country, Department & Industry

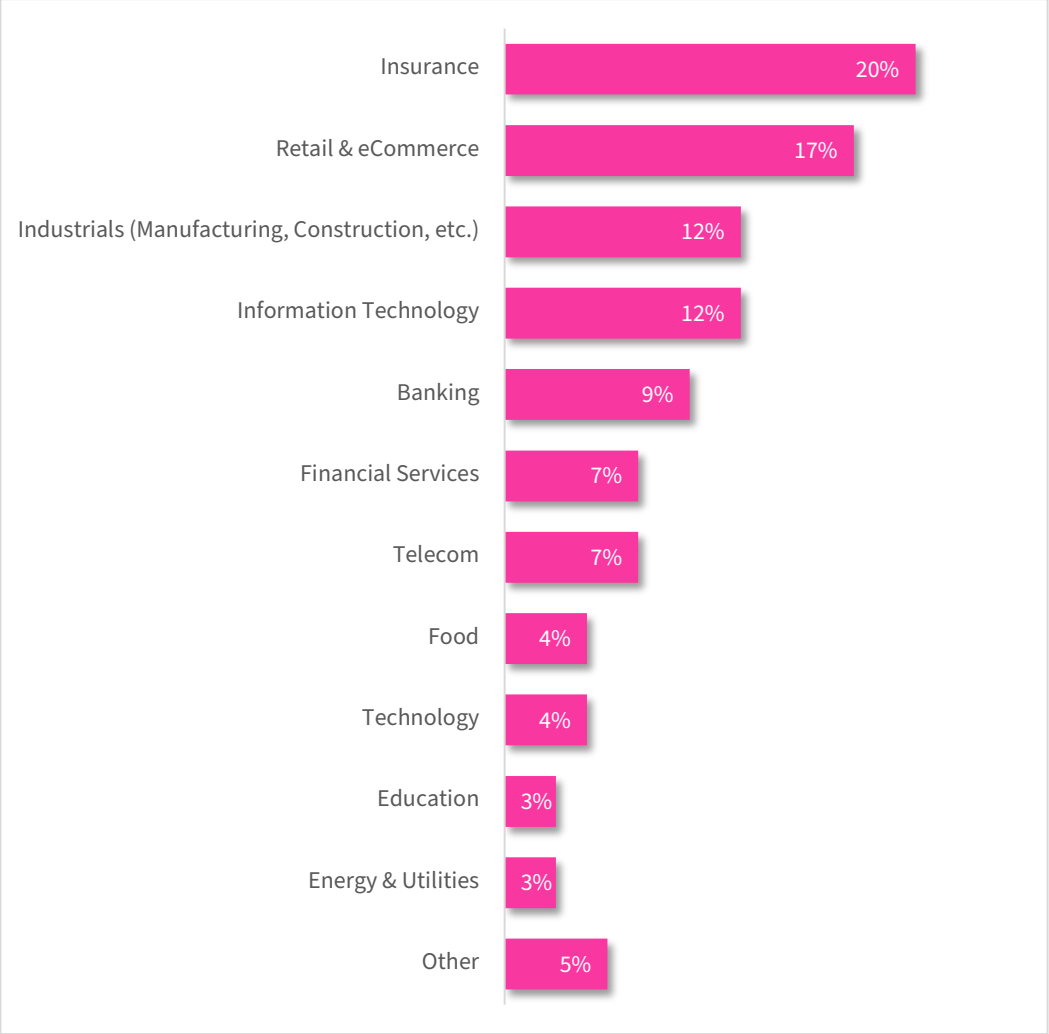

Figure 28 Industry

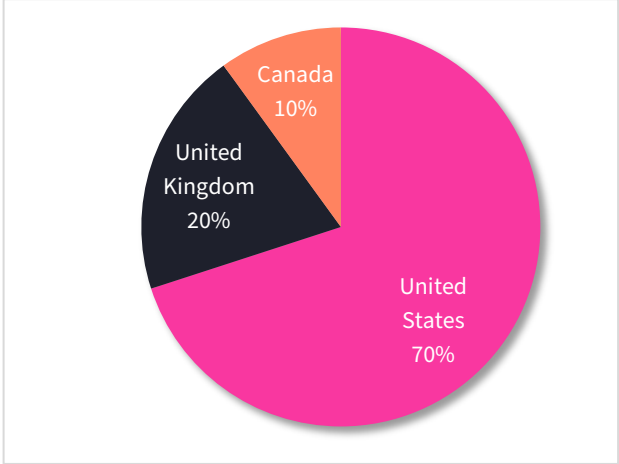

Figure 29 Country

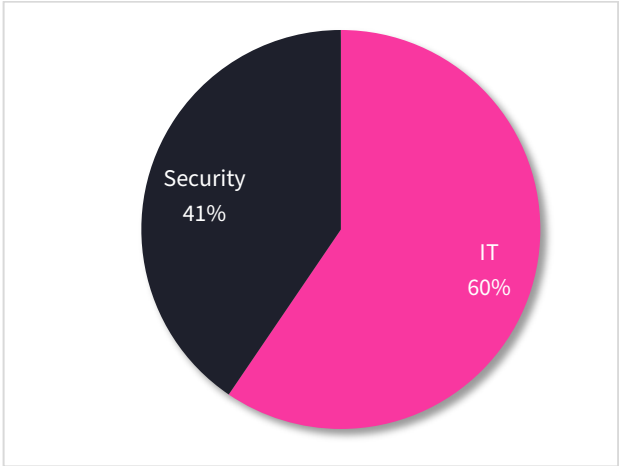

Figure 30 Department

About Cynet

Cynet is a provider of the world's first end-to-end, natively automated XDR platform – Cynet 360 AutoXDR™ – backed by a 24/7 MDR service. The platform was purpose-built to enable small security teams to achieve comprehensive and effective protection regardless of their resources, team size, or skills. It does this by managing day-to-day security operations so teams can focus on managing security rather than operating it.

Request a Demo

For more information, please visit us:

Phone: 1 (212) 634-9358 | Email: info@cynet.com