SOPHOS

The State of Cybersecurity 2023: The Business Impact of Adversaries

Findings from an independent study of 3,000 leaders responsible for IT/cybersecurity across 14 countries conducted in January and February 2023.

A Sophos Whitepaper. April 2023

Research Methodology

To explore the real-world business impact of cybersecurity in 2023, Sophos commissioned an independent survey of 3,000 leaders responsible for IT/ cybersecurity across 14 countries. All respondents were from organizations with between 100 and 5,000 employees. The research was conducted in January and February 2023 by Vanson Bourne.

3,000
respondents

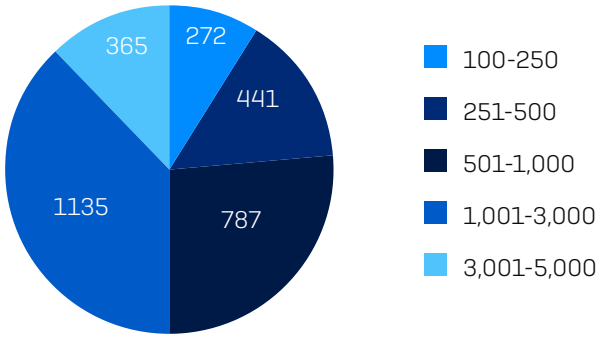
100-5,000
employees

14
countries

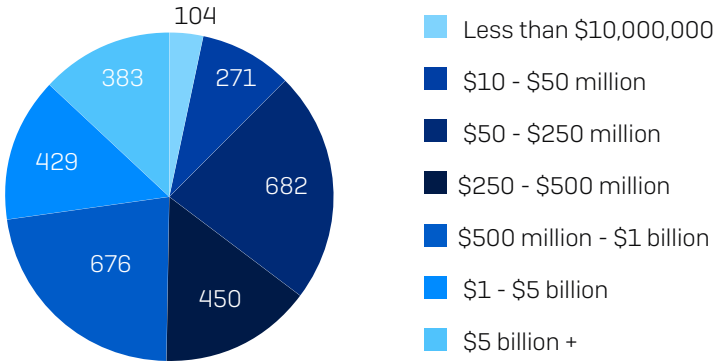
<$10M - $5B+
Annual revenue

Jan/Feb 23
research conducted

Respondents by Organization Size (number of employees)



Respondents by Organization Size (annual revenue)



Respondents by Country

COUNTRY	NUMBER OF RESPONDENTS	COUNTRY	NUMBER OF RESPONDENTS
United States	500	United Kingdom	200
Germany	300	South Africa	200
India	300	France	150
Japan	300	Spain	150
Australia	200	Austria	100
Brazil	200	Singapore	100
Italy	200	Switzerland	100

Executive Summary

Situation: Adversaries Are Accelerating, and Defenders Are Unable to Keep Up

The study revealed that today's reality is a two-speed cybersecurity system with adversaries and defenders moving at different speeds. Through automation, cybercrime "as-a-service" models, stealthy impersonation, and adaptation, adversaries are accelerating and can now execute a wide range of sophisticated attacks at scale. With 94% of organizations experiencing a cyberattack of some form in the last year, all companies – regardless of size or revenue – should assume they will be a target in 2023.

Slowed by a shortage of expertise, an overwhelming volume of alerts, and too much time spent on incident response, defenders are unable to keep up. Operationalizing threat detection and response is difficult for most organizations, with 93% finding the execution of essential security operations tasks challenging.

Investigating security alerts is a widespread issue. On average, just under half (48%) of all alerts are investigated to determine whether they are signs of malicious activity, and most organizations struggle to identify (71%) and prioritize (71%) which alerts/events to investigate. For the alerts that require it, the full detection, investigation and response process takes nine hours on average for organizations with 100-3,000 employees, rising to 15 hours for those with 3,001-5,000 employees.

Operationally, defenders lack confidence in their processes, with security tool misconfiguration identified as the top perceived security risk in 2023. Over half (52%) of IT professionals say that cyberthreats are now too advanced for their organization to deal with on their own, rising to 64% among small businesses (100-250 employees).

Business Impact: The Situation Has Financial, Operational and Resourcing Consequences

This two-speed system has a considerable impact on the wider organization. The direct financial repercussions of a cyber incident are huge and already well-known, with the average cost to a small or mid-sized organization to remediate a ransomware attack coming in at $1.4 million[1]. These incident clean-up costs are, however, just part of the story.

Capacity for IT program delivery is reduced, with 55% of respondents reporting that dealing with cyberthreats has negatively impacted the IT team's work on other projects. The urgent and unpredictable nature of cybersecurity also gets in the way of business-focused efforts: 64% wish the IT team could spend more time on strategic issues and less time on firefighting.

The lengthy time spent on detecting, investigating and remediating security alerts also has a considerable financial impact in terms of the resourcing cost.

The situation also creates a heavy burden on employees. 57% of IT professionals say that worrying about the organization being hit by a cyberattack sometimes keeps them up at night, rising to 65% among those working in organizations with 3,001-5,000 employees. Given the high costs of recruiting, training, and retaining staff in this space, these repercussions create additional challenges and costs for the business.

1 The State of Ransomware 2022, Sophos

Recommendation: Accelerate the Defender Flywheel to Move Ahead of Adversaries

Enabling defenders to overtake attackers in the 2023 cybersecurity race requires a comprehensive, but straightforward approach. Firstly, organizations need to set up an incident response process that can scale, achieved through minimizing the attack surface and the volume of alerts that require attention, and optimizing response time by leveraging specialist services.

Next, they need to implement adaptive defenses that automatically adjust to the situation. This allows them to slow down adversaries and buy defenders time to respond.

Finally, they also need to set up a virtuous cycle that combines technology and human expertise to turbo-charge defenses, enabling an increase in speed, efficacy, and impact. Together they accelerate the defender flywheel, enabling them to pull ahead.

Central to the success of this approach is the use of third-party specialists. The good news is that organizations already have a blended approach to cybersecurity delivery, with 94% of companies working with external specialists in some capacity to scale their operations. As adversaries ramp up their efforts, engaging with dedicated security operations expertise is increasingly essential.

Key findings

94% of organizations experienced a cyberattack of some form in the last year

Data exfiltration is the number one security concern for 2023

93% find the execution of essential security operations tasks challenging

48% of security alerts are investigated

15 hours is the median time to detect, investigate and respond to an alert in 3,001-5,000 employee organizations

Security tool misconfiguration is the top perceived security risk in 2023

52% say that cyberthreats are now too advanced for their organization to deal with on their own

55% say dealing with cyberthreats has negatively impacted the IT team's work on other projects

64% wish the IT team could spend more time on strategic issues and less time on firefighting

57% of IT professionals lose sleep worrying about the organization being hit by a cyberattack

Cyberthreats 2023: Reality from the Front Lines

Top Cyberthreat Concerns for 2023

99% of IT professionals are concerned about cyberthreats affecting their organization in 2023. Data exfiltration (theft by an external attacker) tops the list of threats that IT professionals are most concerned about affecting their organization, closely followed by phishing (including spear phishing). Ransomware rounds out the top three placements.

It's important to remember that these three threats are often interlinked: a phishing email often starts an attack that results in data exfiltration and ransomware.

CYBERTHREAT	PERCENTAGE OF RESPONDENTS SAYING IT IS A TOP CONCERN
Data exfiltration (theft by an external attacker)	41%
Phishing (including spear phishing)	40%
Ransomware	35%
Cyber extortion	33%
Denial of Service attacks (DDoS)	32%
Business email compromise	31%
Active adversaries (human hands-on-keyboard attackers)	30%
Mobile malware	30%
Cryptominers	22%
Wipers	16%
Other	0%
I am not concerned about any cyber threats affecting my organisation in 2023	1%
Don't know	0%

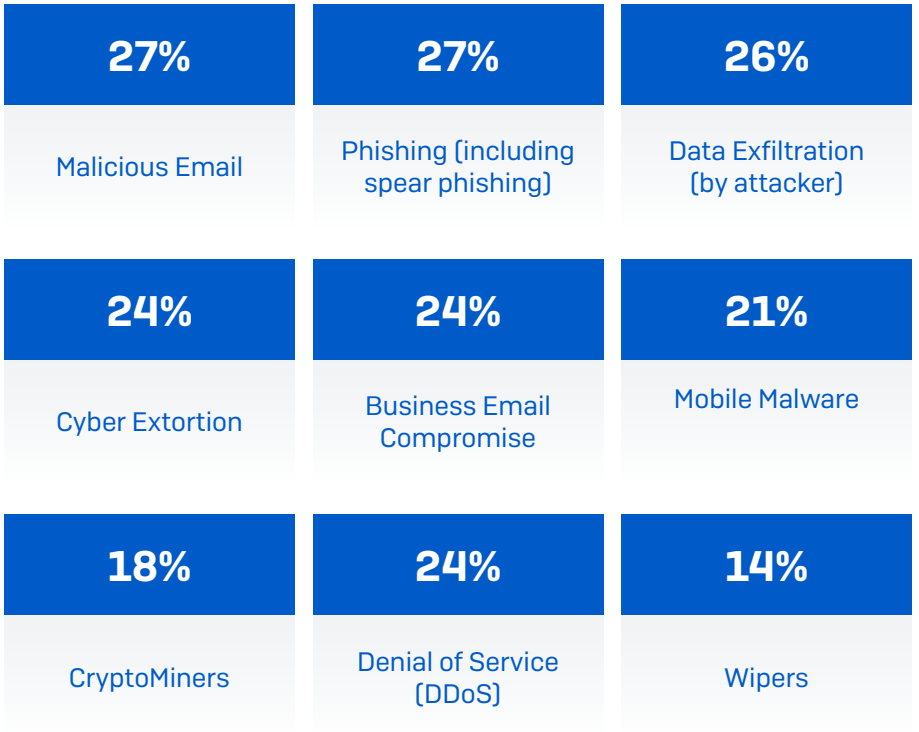
Thinking about 2023, which cyberthreats are you most concerned about affecting your organization? (n=3,000)

Adversaries Now Execute Myriad Attacks at Scale

The concerns of IT professional closely match the reality of what is happening on the front lines with 94% of organizations experienced at least one cyberattack in the last year. While ransomware was the most reported attack, adversaries execute a wide range of attacks at scale. This breadth and depth of attacks creates a considerable and growing challenge for defenders.

Behind these numbers is the increasing professionalization of the cybercriminal economy, including the growth of the 'as a service' model, including 'access-as-a-service', 'phishing-as-a-service', and 'scamming-as-a-service.' This evolution in cybercrime operations has lowered the barriers to entry for would-be cybercriminals. [For more information, read the Sophos 2023 Threat Report.]

Selection of non-ransomware cyberattacks experienced and the percentage of organizations that reported them



Active Adversary Attacks Are Now Commonplace

23%
of organizations experienced an attack involving an Active Adversary in the last year

30%
say Active Adversaries are one of their top cyberthreat concerns for 2023

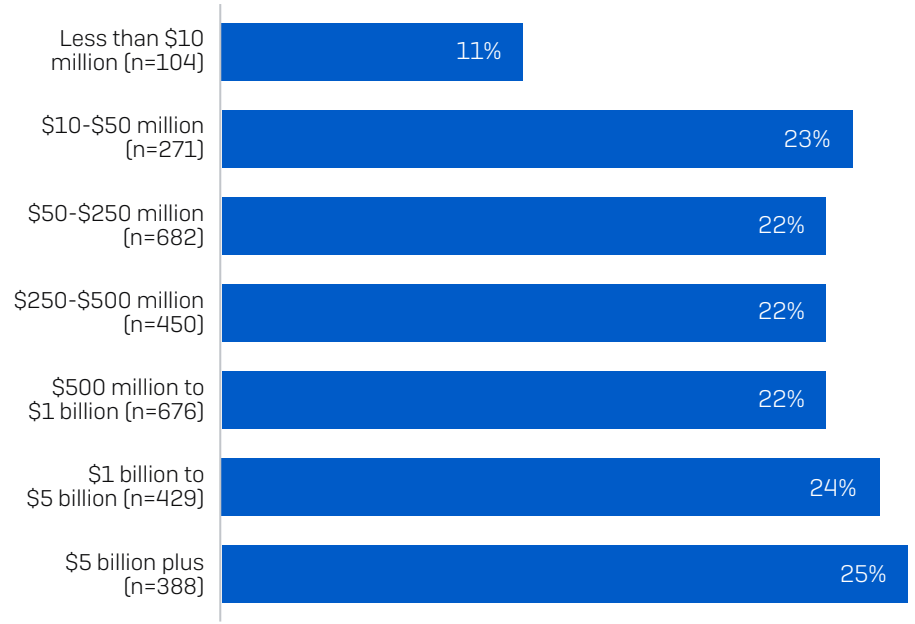
Active adversaries are threat actors who adapt their techniques, tactics, and procedures (TTPs) on the fly using real-time hands-on-keyboard actions in response to actions by security technologies and defenders, and as a tactic to evade detection. These attacks, which often result in devastating ransomware and data breach incidents, are among the hardest to stop.

23% of respondents reported that their organization experienced an attack involving an active adversary last year. The attack rate was consistent regardless of organization size, varying by only two percentage points across all organization size segment splits.

Interestingly, for organizations with less than $10 million in annual revenue, the rate of reported active adversary attacks dropped to just 11%, which may indicate that attackers are deliberately focusing on targets with deeper pockets. Detecting active adversaries requires a high level of skill and it is likely that the actual rate of incidents is higher.

Reflecting the potential devastation of these attacks, 30% of respondents reported that active adversaries are one of their top cyberthreat concerns for 2023.

Active Adversary Attack Experience by Revenue

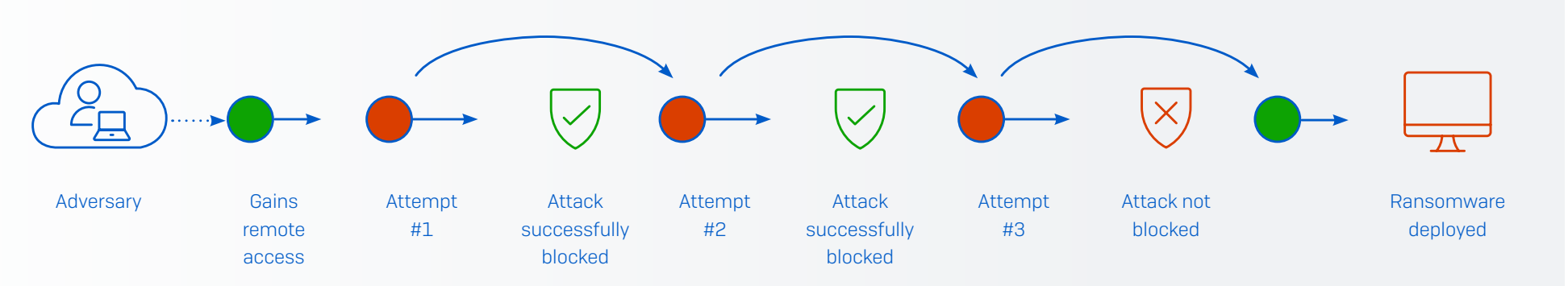


Have you experienced any cyberattack(s) in the last year? Yes - Active adversaries (human hands-on-keyboard attackers)

Understanding Active Adversaries

To appreciate the challenge facing defenders, it's essential to understand that blocking active adversaries is not enough to thwart them. These skilled and persistent threat actors deploy multiple techniques, tactics, and procedures (TTPs) to achieve their goals, including:

- Exploiting security weaknesses to penetrate organizations and move laterally once inside the network, including stolen credentials, unpatched vulnerabilities, and security tool misconfigurations,
- Abusing legitimate IT tools used by defenders to avoid triggering detections,
- Modifying their attacks in real-time in response to security controls, by continuing to pivot to new techniques until they find a way to achieve their goals.



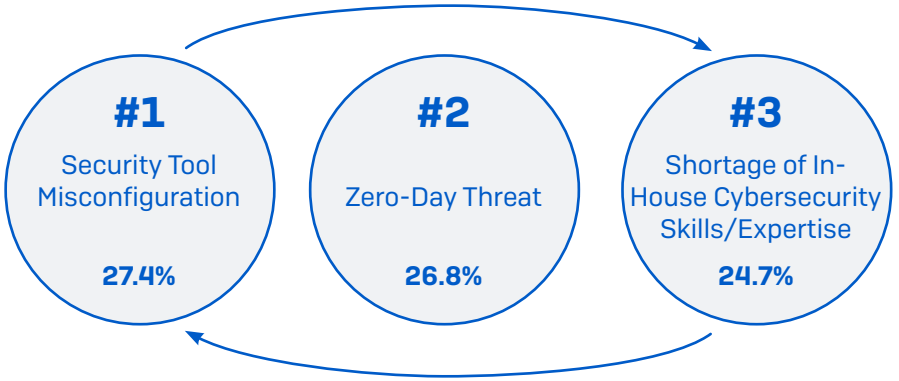
Cybersecurity 2023: The State of the Defenders

Top Cyber Risk Concerns

Security control misconfigurations (e.g., of an endpoint or firewall solution) are the most widely reported perceived security risk, with 27.4% of respondents including it in their top three cyber vulnerabilities. This top ranking illustrates the challenges IT teams face in ensuring that their security controls remain correctly configured and deployed at all times, and the readiness with which adversaries exploit any gap in an organization's defenses.

Zero-day attacks, i.e., attacks that take advantage of a previously unknown security vulnerability or software flaw, are in second position, rated a top three security risk at 26.8%. A shortage of in-house cybersecurity skills/expertise is third on the list, rated a top three security risk by 25% of respondents.

There is a direct relationship between skills shortage and security tool misconfiguration: without the time, knowledge, and experience to configure controls correctly, you create gaps in your defenses.



CYBERSECURITY RISK	PERCENTAGE RANKING AS TOP THREE CONCERN
Zero-day threats (a threat that takes advantage of a previously-unknown attack technique).	27%
Shortage of in-house cybersecurity skills/expertise	25%
Stolen access data and credentials	24%
Unprotected devices (including unknown devices)	24%
Shortage of cybersecurity tools	23%
Unpatched vulnerabilities	22%
Enabling access for remote users	20%
Insecure wireless networking	20%
Internal users (accidental)	18%
Partners/supply chain	18%
Remote access tools	18%
Internal users (deliberate)	17%
IoT devices	17%
Other	0%
None of these are cybersecurity risks to my organization	0%
Don't know	0%

Who/ what do you consider to be your organization's top three cybersecurity risks? Combination of responses ranked first, second and third (n=3,000)

Differing Approaches to Alert Investigation

Organizations investigate **48% of their security alerts** to identify if they are signs of malicious activity

One of the challenges for defenders is identifying which alerts to investigate and how to use their limited resources to best effect.

On average, just under half (48%) of all security alerts are investigated to identify whether they are signs of malicious activity, rising to 54% in organizations with 3,001-5,000 employees. However, approaches differ greatly: 16% of organizations investigate more than three quarters of their alerts (including 5% who report they investigate all alerts) while 18% investigate a quarter or fewer.

From a sector perspective, central/federal government investigates the lowest percentage of alerts (39%) (n=89) while energy, oil/gas and utilities investigates the highest (55%) (n=69).

Detection, Investigation and Response Overhead

The median time to detect, investigate, and respond to an alert is nine hours for organizations with 100-3,000 employees, rising to 15 hours for organizations with 3,001-5,000 employees, likely reflecting the increased complexity of their operating environments.

The survey revealed considerable variation by industry, with organizations in the manufacturing and production (15 hours) and energy, oil/gas and utilities (18 hours) sectors taking more than twice as long as those in IT, technology and telecoms (6.75 hours).

It's important to note that the majority of alerts will not reach the response stage. Most attacks will be blocked proactively by security technologies with a subset of alerts triaged and brought forward for investigation. Response actions will also vary considerably due to the nature of the event that requires remediation, from deleting a phishing email from users' inboxes to rebuilding an entire server farm.

Median time to detect, investigate, and respond to an alert

ACTIVITY	100-3,000 EMPLOYEES (n=2,460)	3,001-5,000 EMPLOYEES (n=350)	IT, TECHNOLOGY AND TELECOMS (n=98)	MANUFACTURING AND PRODUCTION (n=331)	ENERGY, OIL/GAS AND UTILITIES (n=66)
Detection	3 hours	3 hours	1.5 hours	3 hours	6 hours
Investigation	3 hours	6 hours	2.25 hours	6 hours	6 hours
Response	3 hours	6 hours	3 hours	6 hours	6 hours
Total	**9 hours**	**15 hours**	**6.75 hours**	**15 hours**	**18 hours**

How long does it take for your organization to detect, investigate and, when necessary, remediate a potential incident? (n=2,812 respondents that investigate alerts in-house)

Organizations Lack Essential Security Operations Skills

As already seen, IT professionals consider the shortage of in-house cybersecurity skills/expertise to be one of their biggest security risks for 2023. Diving deeper, the survey reveals that the majority of organizations struggle with the day-to-day delivery of core security operations tasks, with 93% rating at least one of the following activities as 'challenging':

- Identifying signals from noise (71% find challenging)
- Prioritizing which signals/alerts to investigate (71% find challenging)
- Getting sufficient data to identify if a signal is malicious or benign (71% find challenging)
- Remediating malicious alerts or incidents in a timely way (71% find challenging)
- Identifying the root cause of the incident (75% find challenging)
- Keeping accurate records of investigations (68% find challenging)

Identifying the root cause of the incident is the most widespread issue, with 75% of respondents reporting that they find it challenging.

Organizations with the lowest annual revenue (below $10 million) are most likely to find security operations tasks challenging, followed by those with the largest revenue ($5 billion +). Both ends of the spectrum will face different obstacles, with organizational and system complexity likely to play a greater role in larger organizations.

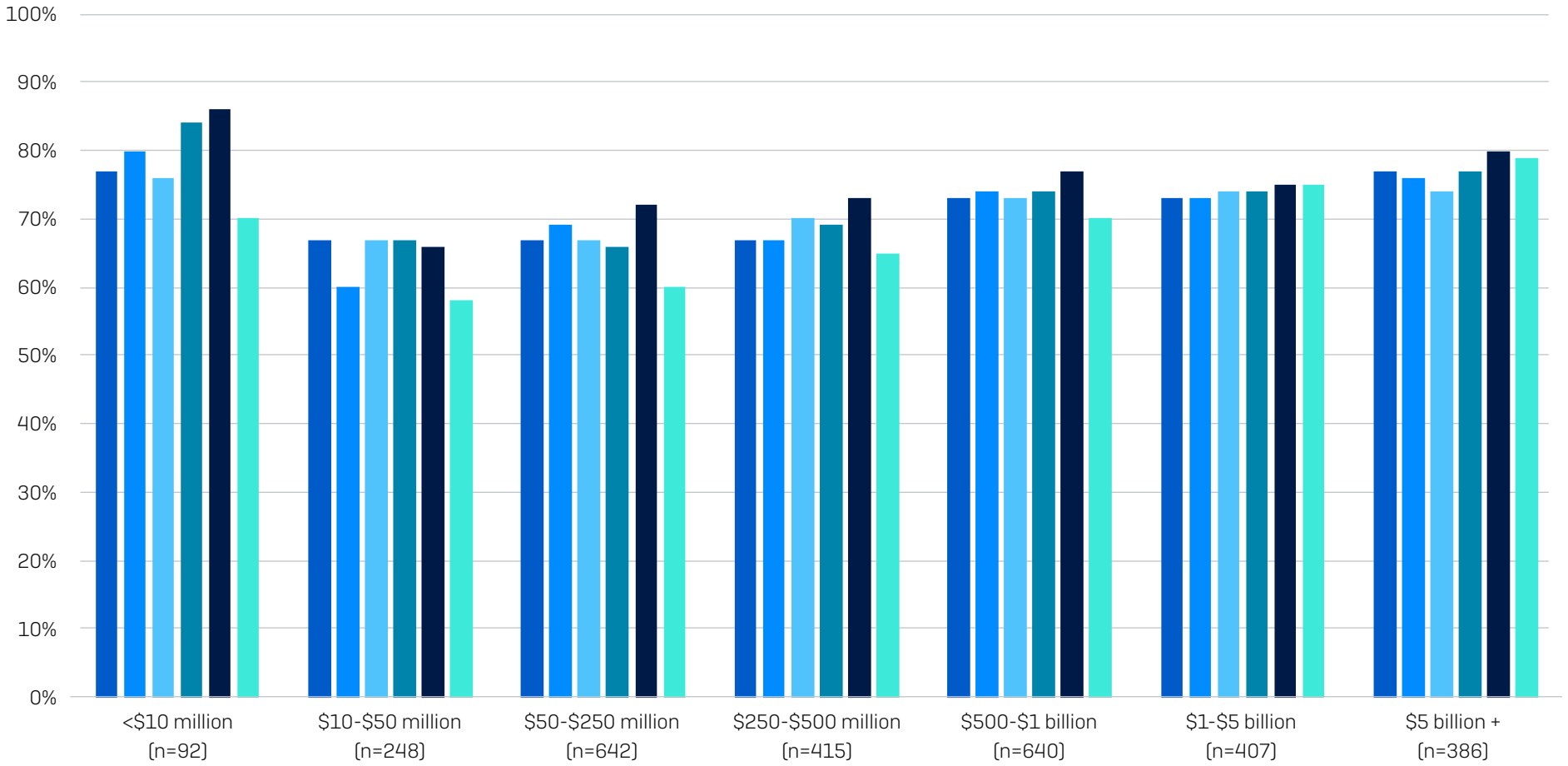
This skills shortage creates a domino effect: investigating alerts takes longer, which, in turn, reduces the capacity of the team and increases risk exposure.

93%
find security operations challenging

75%
find it hard to identify the root cause of the incident

71%
struggle to identify which alerts to investigate

Organizations That Find Security Operations Tasks 'Challenging' By Revenue



Respondents whose organization finds security operations tasks 'very challenging' or 'somewhat challenging' when investigating suspicious alerts (n=2,812 respondents that investigate security alerts in-house)

- Identifying signals from noise i.e. understanding which signals/ alerts to investigate
- Prioritizing which signals/ alerts to investigate
- Getting sufficient data to identify if a signal is malicious or benign
- Identifying the root cause of the incident i.e., how the adversary entered the organization
- Remediating malicious alerts or incidents in a timely way
- Keeping accurate records of the investigation

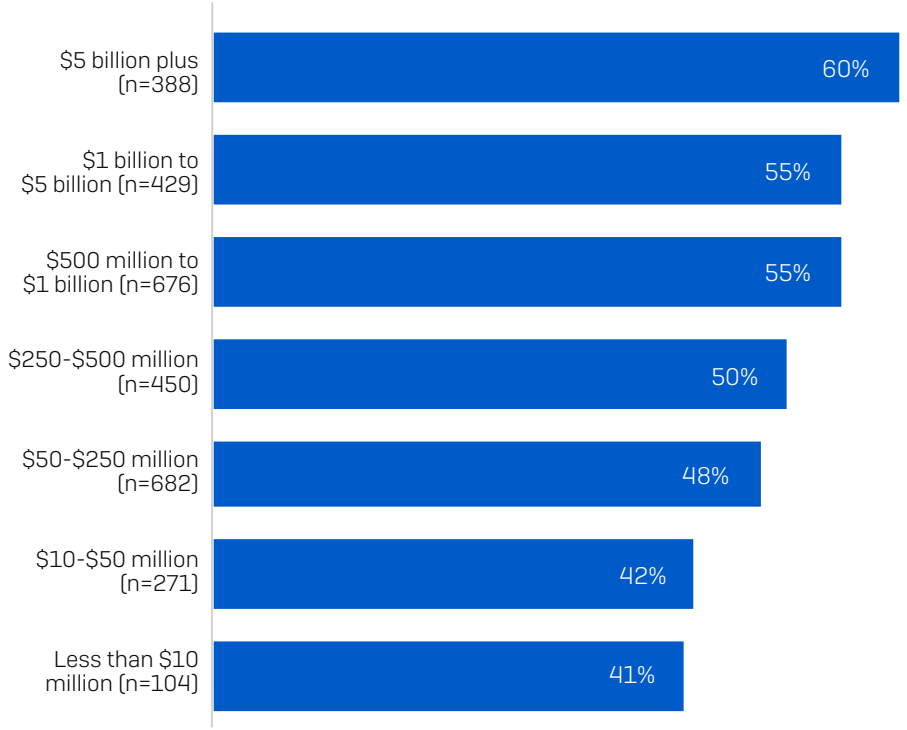
Adversaries Have Outpaced Defenders

52%
say cyberthreats are now too advanced for their organization to deal with on their own

Over half (52%) of IT professionals say that cyberthreats are now too advanced for their organization to deal with on their own, rising to 64% among small businesses (100-250 employees).

As organizational revenue increases, so does the likelihood that in-house teams cannot keep up. This likely reflects the greater complexity of the internal cybersecurity environment in larger revenue organizations and a greater propensity to engage specialist security services. It may also reflect a greater understanding of the threat environment and the challenges in defending against advanced threats.

Cyberthreats are now too advanced for the organization to deal with on their own



To what extent do you agree or disagree with the statement: cyberthreats are too advanced for our organization to deal with on their own? Strongly agree, somewhat agree (base numbers in chart)

The Business Impact

Program Delivery Impact

64%
wish the IT team could spend more time on strategic issues and less time on firefighting

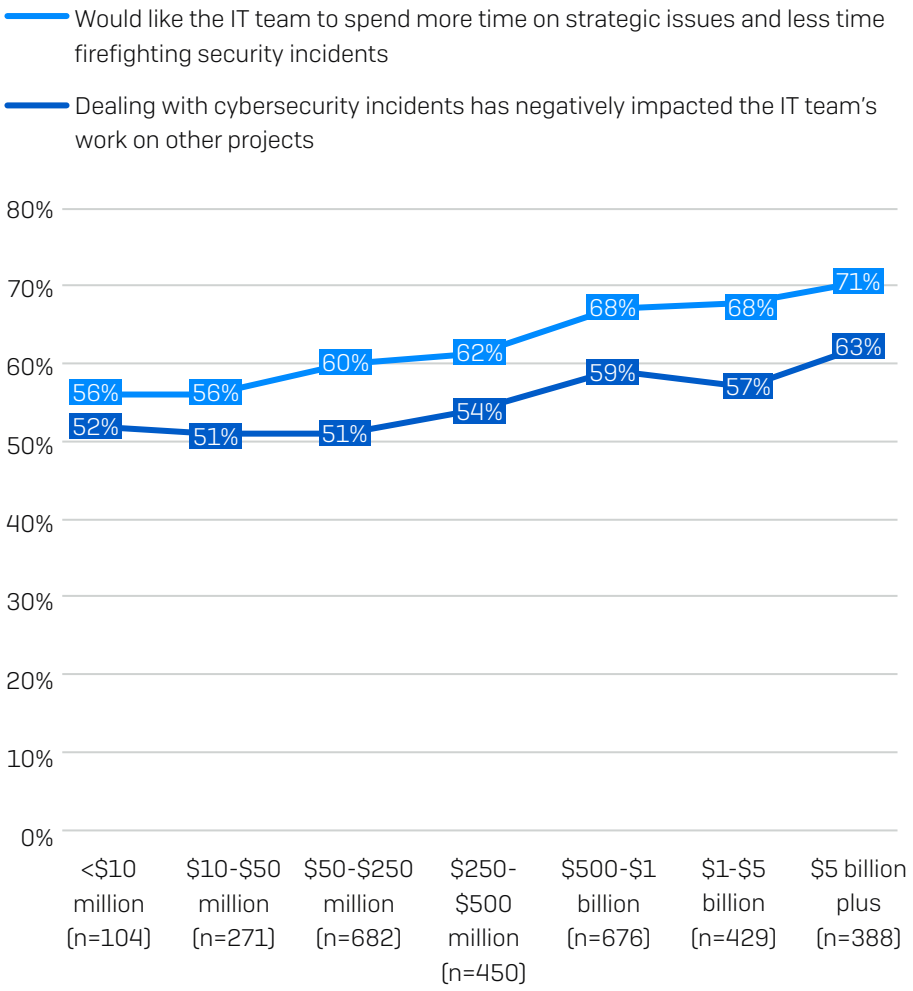
55%
say dealing with cyberthreats has negatively impacted the IT team's work on other projects

For 60% of organizations, cybersecurity and the wider IT function are very tightly linked: 52% have a cybersecurity team within their IT team, while for 8%, their IT team manages their cybersecurity. The remaining 40% have separate cybersecurity and IT teams. The vast amount of time and effort required for cybersecurity has considerable consequences for the IT organization.

Over half (55%) of organizations say that dealing with cyberthreats has negatively impacted the IT team's work on other projects, with the highest-revenue organizations reporting the greatest impact.

The urgent and unpredictable nature of cybersecurity also gets in the way of business-focused efforts: 64%, on average, wish the IT team could spend more time on strategic issues and less time on firefighting. Again, as revenue increases, so does the impact on wider program delivery.

Cybersecurity negatively impacting IT program delivery



To what extent do you agree or disagree with the statement: Dealing with cybersecurity incidents has negatively impacted the IT team's work on other projects, I would like the IT team to spend more time on strategic issues and less time firefighting security incidents (base numbers in chart)

Financial Impact

The challenging cybersecurity environment has multiple financial impacts for an organization. The highest individual bills occur in the event of a major cyber incident. As reported in the Sophos State of Ransomware 2022 report, the average ransomware remediation bill comes in at $1.4 million.

However, the financial impact of dealing with cyberattacks is not limited to the clean-up costs. With the average IT Security Specialist salary in the U.S. currently just shy of $100,000 per year[2], the hourly resource cost for each security alert investigation is considerable. While salaries will vary based on local conditions, the financial impact of the lengthy incident investigation process is considerable.

2 Based on average IT Security Specialist salary as of March 2023, https://www.indeed.com/career/it-security-specialist/salaries

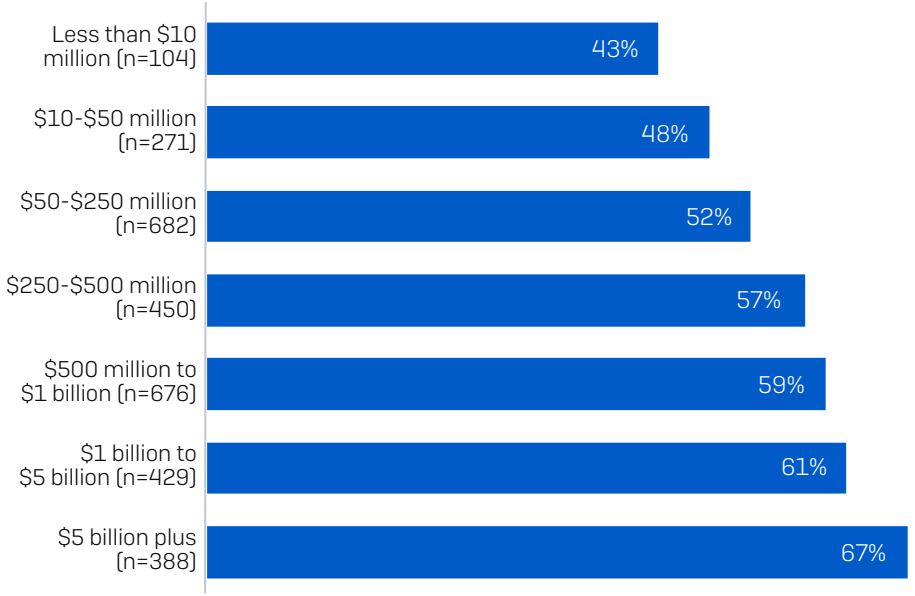
Team Impact

57% of respondents say that worrying about the organization being hit by a cyberattack sometimes keeps them up at night. Given the high costs of recruiting and retaining staff in this space, this is a cause of both welfare and economic concern. It also suggests that defenders do not have full confidence in their security tools.

Burn out is a major issue in cybersecurity. Too many alerts and having too much to do puts considerable stress on employees. Over-stretched teams are more likely to miss important signals, adding further pressure. Ultimately, people will eventually break.

The propensity for cybersecurity worries to stop people from sleeping increases steadily as organization revenue grows, starting at 43% of those in organizations with less than $10 million annual revenue and rising to 67% in organizations that turn over $5 billion or more.

Percentage of respondents that say worrying about the organization being hit by a cyberattack keeps them up at night



To what extent do you agree or disagree with the statement: Worrying about the organization being hit by a cyberattack sometimes keeps me up at night (base numbers in chart)

Recommendations

Addressing the situation requires a straightforward three-step approach: implement a more scalable incident response process that accelerates response time; leverage adaptive defenses to slow down adversaries; and create a virtuous cycle that improves protection and lowers cost.

A "Shields Up" analogy is useful here. Stopping advanced, persistent adversaries requires organizations optimize the efficacy of their defenses ("shields"), including context-sensitive technologies that can elevate the level of protection in proportion to the situation. Crucially, they also need to use the time that their defenses buy them to apply human expertise to address the root cause. requires

Strong Shields Are Essential

The quality of your cybersecurity technologies is paramount, and security controls should:

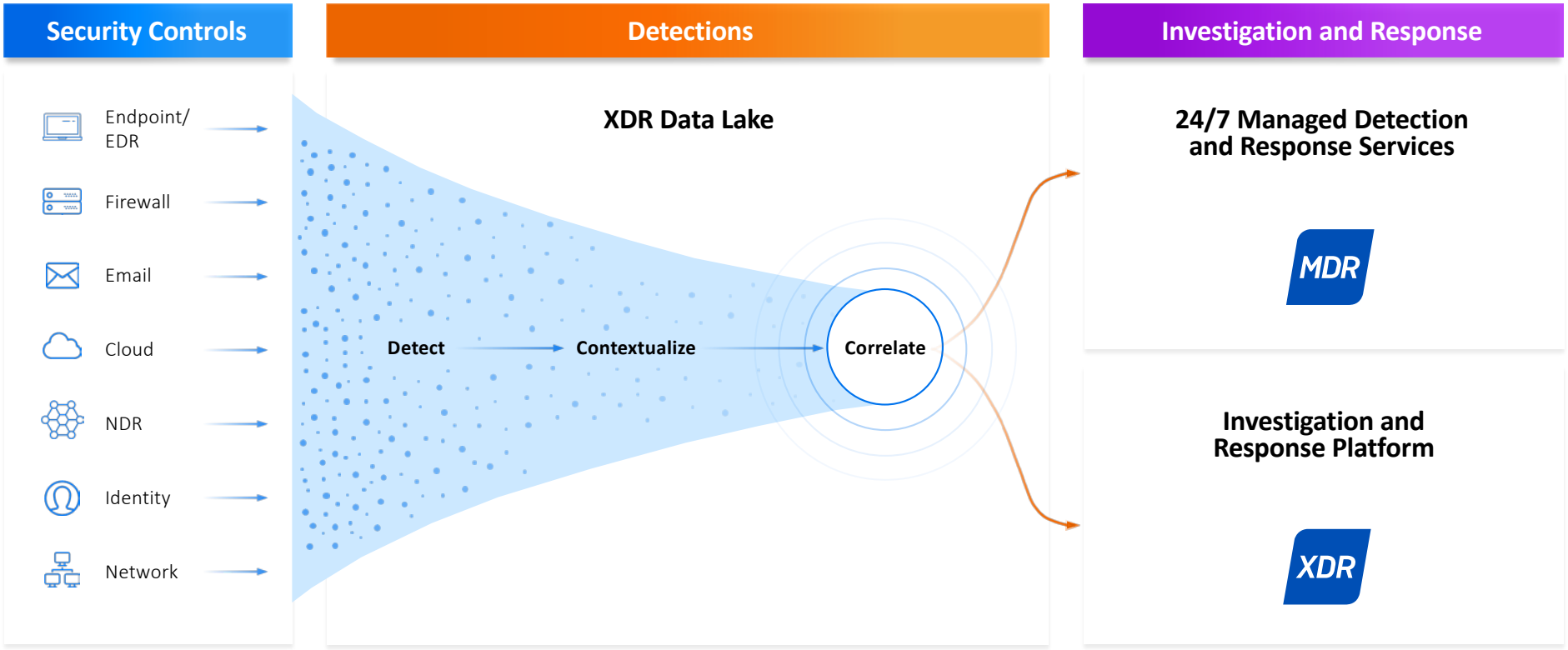
- **Optimize prevention,** automatically detecting and stopping as many threats as possible early in the attack chain. In doing so, you reduce the risk to the organization while freeing up defenders to focus on fewer incidents.
- **Reduce exposure** by making it easy to ensure security investments are correctly and optimally deployed and avoid misconfiguration issues.
- **Disrupt adversaries**. Technologies that automatically detect and disrupt adversarial activity frustrate attackers while buying defenders time to neutralize the incident.

Address The Root Cause with People and Technology

Shields buy defenders valuable time to investigate and respond to attacks. They don't guarantee 100% prevention, however, which is why timely, well-informed, and well-executed root cause remediation is essential.

As the research has shown, adversaries do not follow a single path. Leveraging telemetry from across the security environment, using the security controls organizations already have, enables defenders to see and respond to threats faster while increasing return on existing investments.

Finding malicious activity among the benign alerts is often akin to hunting for the needle in the haystack, or even in a pile of needles. Processing the signals through an Extended Detection and Response (XDR) platform that adds contextual insights and correlates related alerts enables in-house defenders to quickly focus on what's important. Investigation and response can be performed via an XDR platform by the in-house team. Alternatively, organizations can outsource the detection, investigation, and response work to a specialist Managed Detection and Response (MDR) service.



Accelerating the Defender Flywheel

Once a flywheel starts spinning at high speed, it wants to keep spinning. The more force behind a flywheel, the faster it goes. Organizations can accelerate their cybersecurity flywheel by combining security technologies and human expertise. Comprehensive security controls reduce the volume of alerts that defenders need to deal with, enabling them to focus on neutralizing attacks and elevating their security posture. In turn, this increases the efficacy of their security controls, creating a virtuous circle.

Most Organizations Plan to Adopt the Security Controls and Services Needed

The survey revealed that most organizations plan to add threat detection and response solutions to their security stack within the next 12 months. Over three quarters (78%) plan to add Endpoint Detection and Response (EDR) and/or Extended Detection and Response (XDR) tools in the coming year.

Investigating and responding to advanced cyberthreats is a specialist skill and providing 24/7 coverage requires a minimum of five or six people. With a shortage of in-house cybersecurity skills/expertise listed as one of the top three perceived cyber risks for 2023, many organizations are looking to external experts for support: 44% of organizations plan to start working with a Managed Detection and Response (MDR) provider within the next 12 months.

Percentage of organizations that plan to adopt detection and response solutions within the next 12 months

78%	44%
EDR/XDR	MDR

Sophos Can Help

Sophos provides the services and technologies that enable organizations to accelerate the defender flywheel and move ahead of adversaries. We defend over 550,000 organizations against the most advanced threats, and Sophos MDR is the world's most trusted MDR service.

Start with the Strongest Shields

Our endpoint/EDR, firewall, email, network, and cloud solutions slow down attackers and give defenders the time and insights they need to respond:

- **Optimize prevention:** Sophos blocks 99.98% of threats automatically out of the gate, minimizing risk and enabling defenders to focus on fewer incidents that require human intervention.
- **Reduce exposure:** Optimal protection settings are deployed automatically from day one, eliminating security gaps. Built-in Account Health Checks highlight missing software and configuration issues that can lead to avoidable infections.
- **Disrupt adversaries.** Adaptive Active Adversary Protection immediately activates heightened defenses when a "hands-on-keyboard" endpoint intrusion is detected, frustrating attackers and buying defenders time to respond.

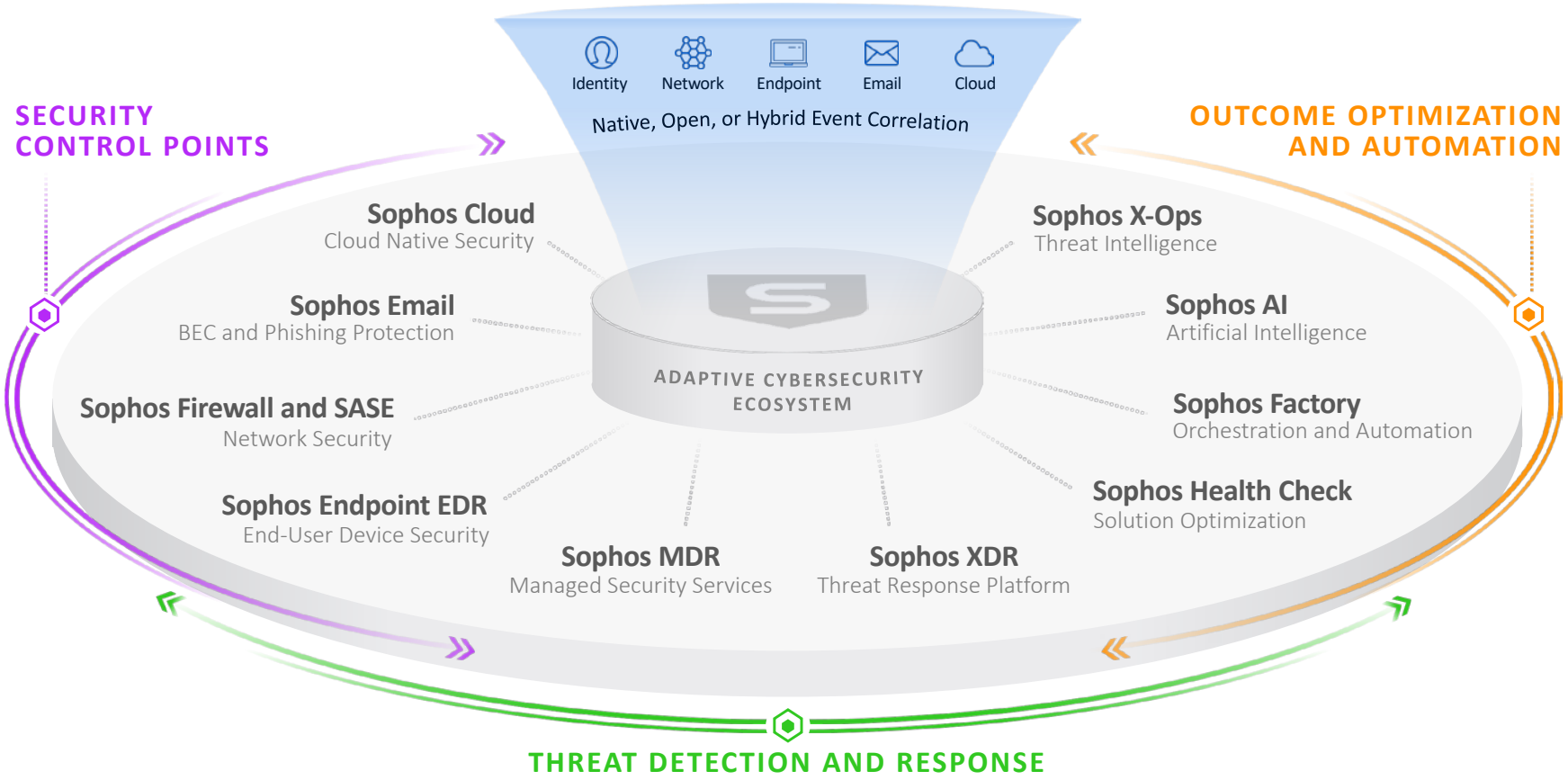
Optimize Detection, Investigation and Response

The more defenders see, the faster they can act. At Sophos we use detections from across the security environment, integrating telemetry from both Sophos and third-party security controls to accelerate detection and response, and increase return on existing security investments.

The Sophos MDR service brings together over 500 experts to hunt for, investigate and respond to active adversaries and other attacks on your behalf 24/7/365. With an average threat response time of just 38 minutes, Sophos MDR is considerably faster than the in-house team average. Alternatively, organizations can use the Sophos XDR platform that includes full EDR functionality to investigate and respond to attacks directly or work in collaboration with the Sophos MDR team.

Wherever your organization is today, and where it wants to be in the future, Sophos can help you accelerate your defender flywheel and move ahead of today's advanced adversaries. For more information, visit www.sophos.com or speak with a security advisor.

Achieve Optimal Cybersecurity Outcomes with Sophos



2023-03-29 (WP-NP)

SOPHOS