Cynet
AUTONOMOUS BREACH PROTECTION

SURVEY RESULTS

STATE OF BREACH PROTECTION 2020

FOREWORD

What are the key considerations security decision makers should take into account when designing their 2020 breach protection? To answer that we polled 1536 cybersecurity professionals in the 2020 Status of Breach Protection survey to understand the common practices, prioritizations and preferences of the organization today in protecting themselves from breaches.

An illustrative example is the issue of consolidation. Advanced breach protection today entails the deployment and manual integration of multiple point products. The findings of the survey validate that while lack of consolidation is the dominant practice, most organizations view it as a core problem that must be solved.

Moreover, the survey results reveal a clear inclination within organizations to deploy advanced breach protection on top of the standard AV/Firewall/Email Protection stack. In light of the above, this is expected to make the lack of consolidation a critical issue for many additional organizations.

Another example relates to the balance between cloud and on-prem resources. While there is no arguing that the cloud represents the future of IT, the survey findings indicate that the transit might take place at a slower pace than expected and that the lion's share share of organizations' critical resources still reside on their premises – an insight with significant implications when prioritizing new security projects.

The questions in the survey focused on the following topics:

- Perceived top cyber risks.
- Security products in place.
- The role of security services within the organization security stack.
- Consolidation of the breach protection stack.
- Environment IT architecture with focus on cloud/on-prem balance.

The document contains two parts:

- Key insights: high level summary of the most meaningful learning that was gained from correlating and analyzing the responses.
- Findings: representative survey questions with the response distribution.

The bottom line is that there is no one size fits all in breach protection. However, there is great benefit for any decision maker or anyone who forms an independent opinion on breach protection in having a bird's eye view on how breach protection is practiced today.

ABOUT CYNET

Cynet 360 is the world's first Autonomous Breach Protection Platform that consolidates and automates endpoint, network and user protection across the full security lifecycle: proactive monitoring and control, attack prevention and detection, and response orchestration. Cynet 360 technology is complemented and enhanced by CyOps Managed Detection and Response (MDR) service, which is included in the Cynet 360 offering without additional payment.

By natively integrating all these capabilities into a single platform, Cynet 360 eliminates the need to manually deploy and integrate multiple point products. Cynet 360 enables security teams to conduct all their operations from a single console, introducing simplicity, speed and efficiency, that translate into an unprecedented level of breach protection.

Visit the Cynet 360 website to learn more about how to introduce unmatched simplicity, speed and robustness to your environment's security.

KEY INSIGHTS

1

Lack of consolidation is a major protection inhibitor

Challenges of maintaining a multi-product security stack (especially in advanced security product groups) are stated as both the main obstacle in reaching the desired protection level, as well as an argument for not purchasing additional required security products.

2

Most organizations are prioritizing advanced protection projects in 2020

The majority of organizations that currently deploy a basic security stack of AV, Firewall and email protection, plan to add EDR/EPP, Network Traffic Analysis or SIEM and are planning to do so in 2020.

3

The challenge involved in lack of consolidation is expected to grow

As more organizations add advanced security to their stack, the difficulties in efficiently operating multiple point products will apply to a wider range of organizations.

4

Deployment is the Achilles heel of endpoint protection

Only a small portion of organizations report that they deploy EDR/EPP on more than 85% of their endpoints with no deployment or maintenance issues. As in many cases, EDR/EPP is regarded as the main mean against advanced attacks. This is an alarming figure.

5

Response orchestration beats automation

While a significant number of the organizations we polled orchestrate their IR operations from a centralized interface, only a small part introduce automation to their remediation workflows.

6

On-prem is still at large

Despite the hyped Age of Digital Transformation, the majority of workloads are still on-prem. Security stakeholders should take that into account and prioritize solutions that address the challenges of the on-prem environment.

7

Proactive protection is highly regarded

A significant number of organizations stated the discovery of security vulnerabilities in apps and systems as a primary action item for 2020.

8

Advanced threat protection still involves a high volume of attended alerts

All organizations that deploy SIEM, EDR/EPP, Network Traffic Analysis, UEBA or Deception products state that over 25% percent of alerts are left unattended on a daily basis.

9

Organizations have mixed feelings regarding security outsourcing

While the security skill gap compels organizations to outsource the more advanced portion of their security operations, there is still a strong inclination to keep things in-house, especially in regards to active attack remediation in their environment.

10

Security budgets continue to increase

Close to 70% of polled organizations will have a larger security budget in 2020 than in 2019.

11

Tier 1 security Four products comprise a security standard for most to all organization

Firewall, AV, email protection and vulnerability management are a de-facto common practice and can be regarded as the baseline solutions implemented by most organizations.

14

Tier 2 security stack
The advanced security stack is gaining momentum

SIEM, EDR/EPP and Network Traffic Analysis are present in 30% of organizations that acknowledge the protection limitations of tier 1 products.

15

Tier 3 security stack
High-end products with little footprint

UEBA and Deception feature the least market penetration and are found in a small subset of organizations.

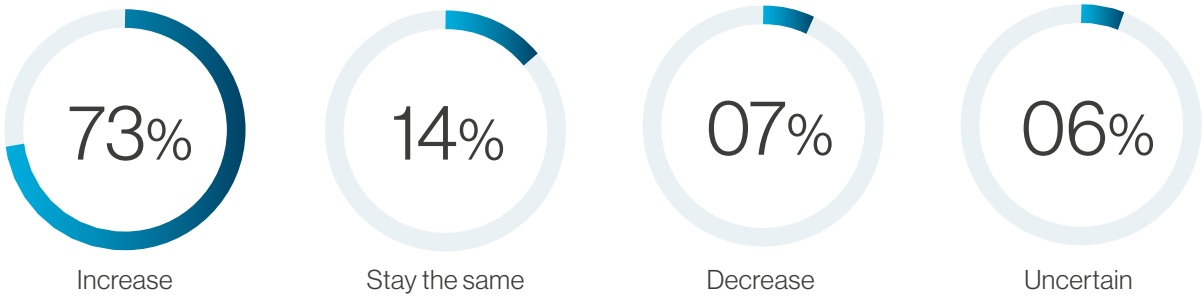
16

Having security products in place does not ease the concern

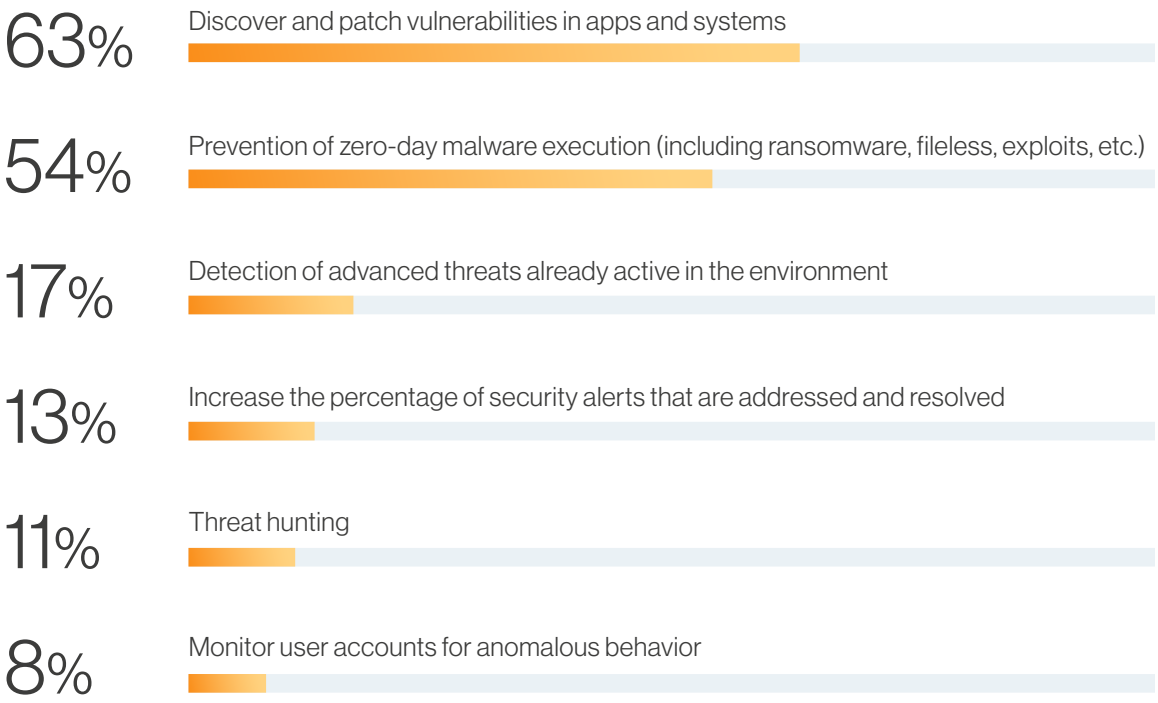
While most organizations have AV and email protection in place, they still state email-based threats and ransomware as their top concern for 2020.

SURVEY FINDINGS

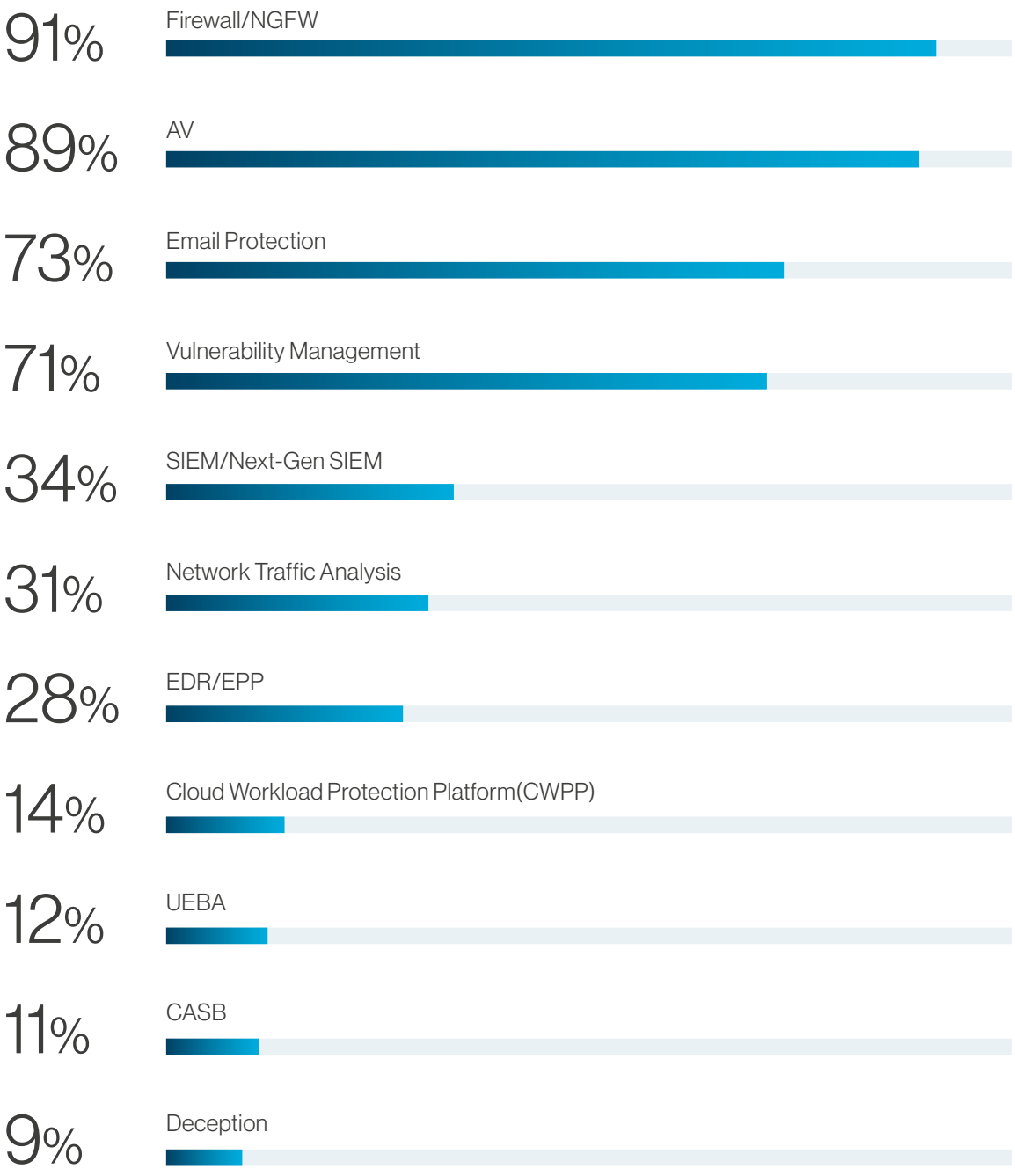
Over the next 12 months, what do you anticipate will happen to your security budget?



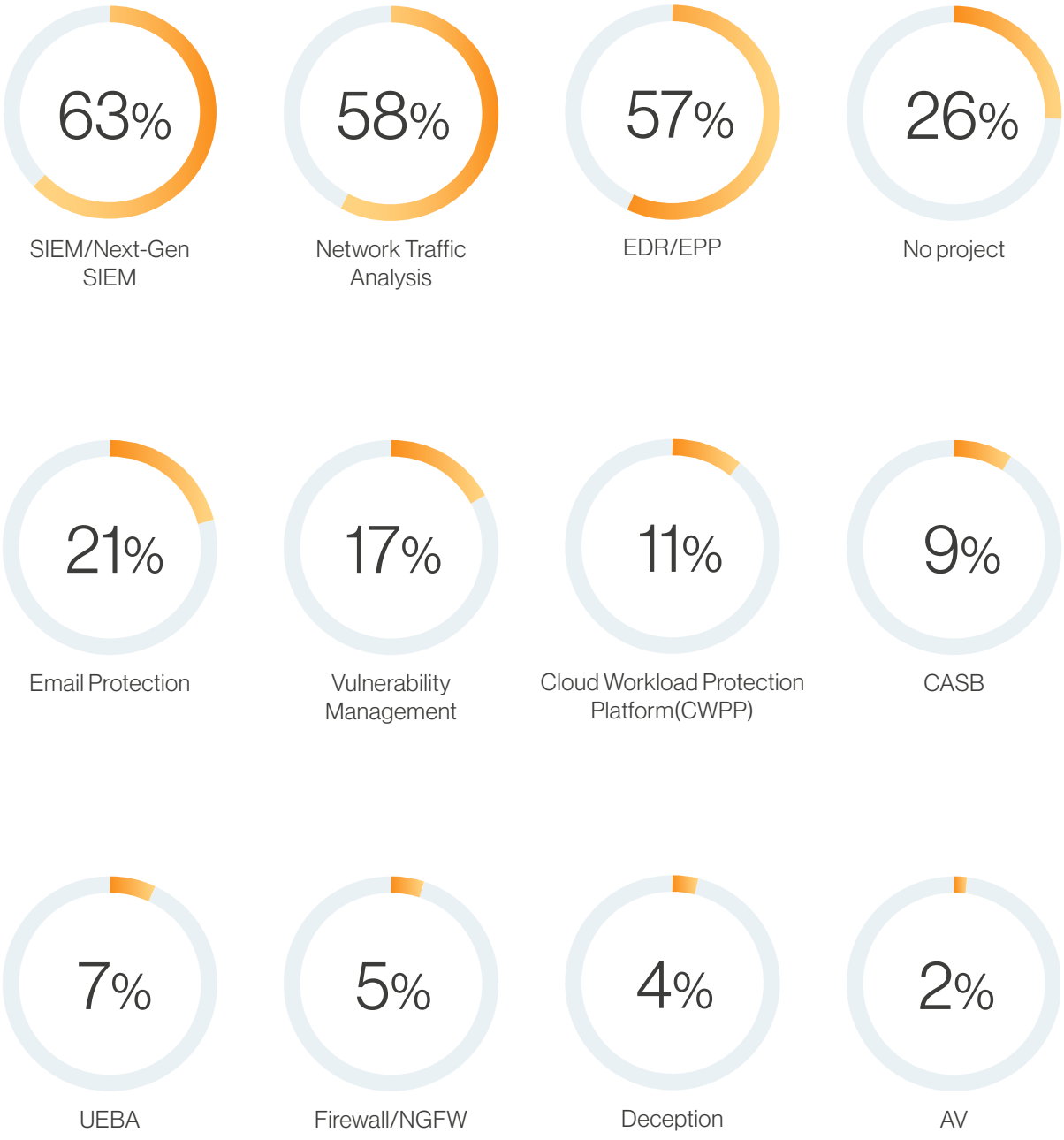
Which of the following breach protection use cases will be a primary focus for your organization over the next year?



Which of the following breach protection technologies are you currently deploying in your organization?

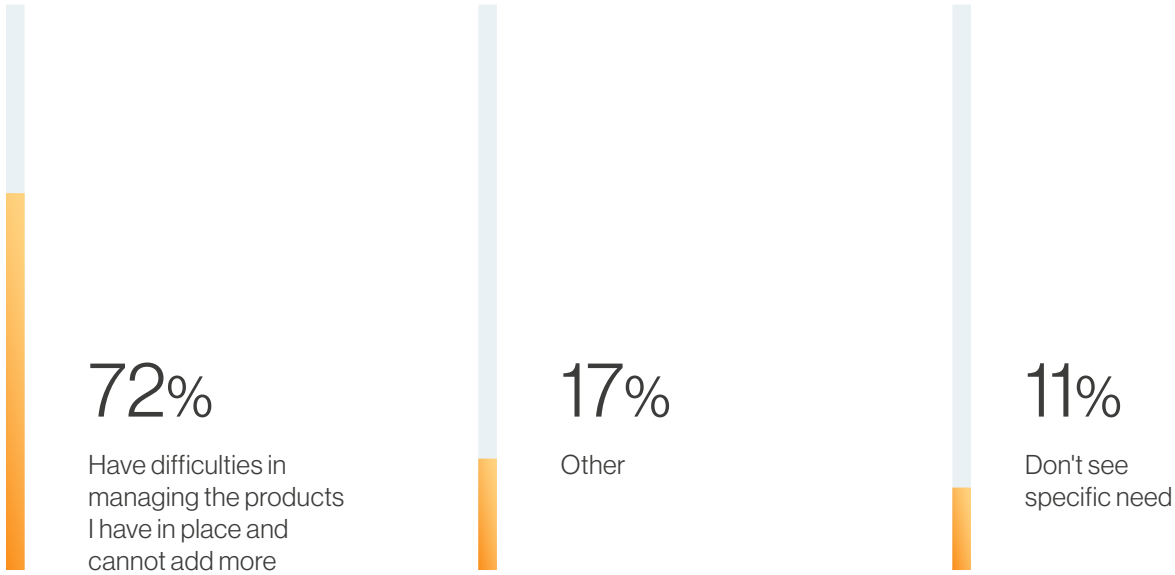


Which breach protection projects will be the main focus for your organization in 2020?

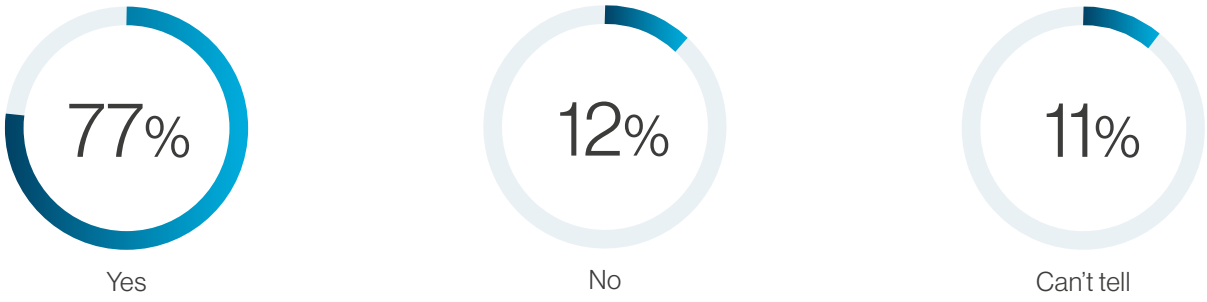


For those who don't have projects planned in 2020:

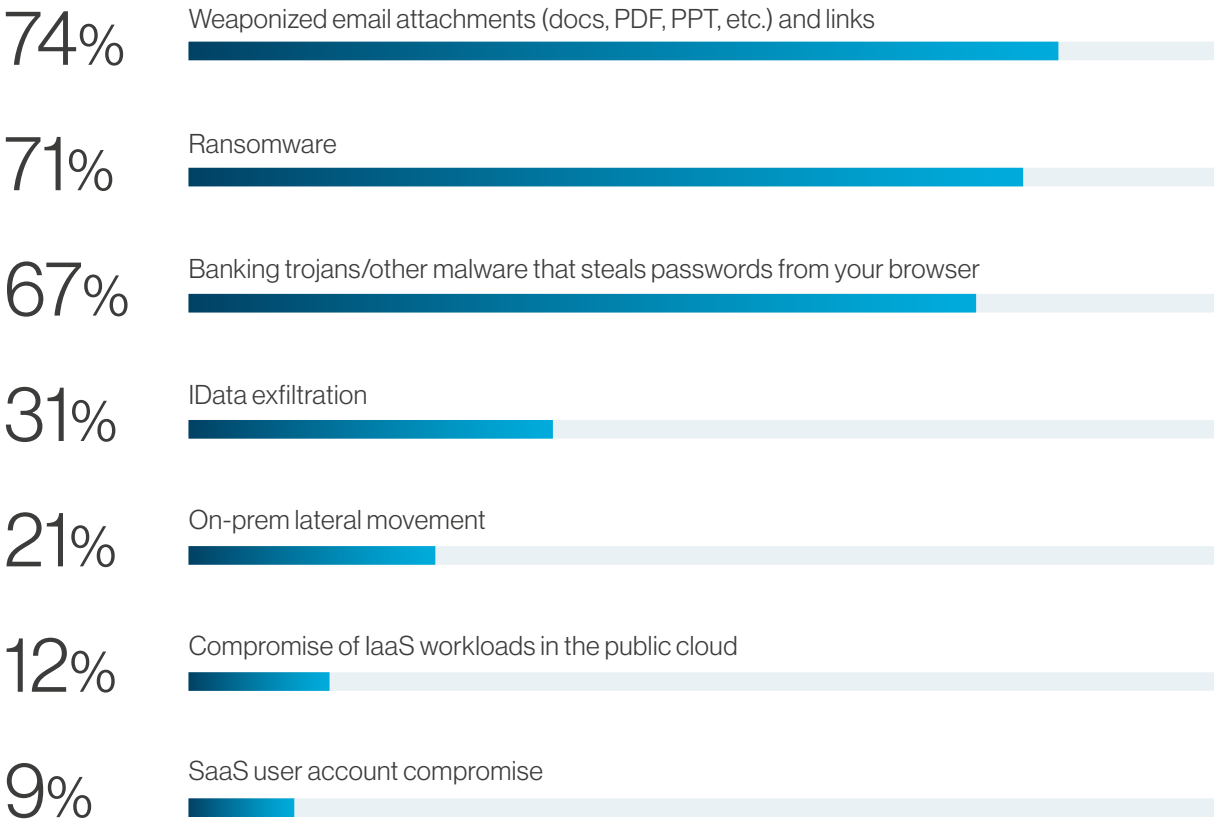
Why don't you have a breach protection plan in scope?



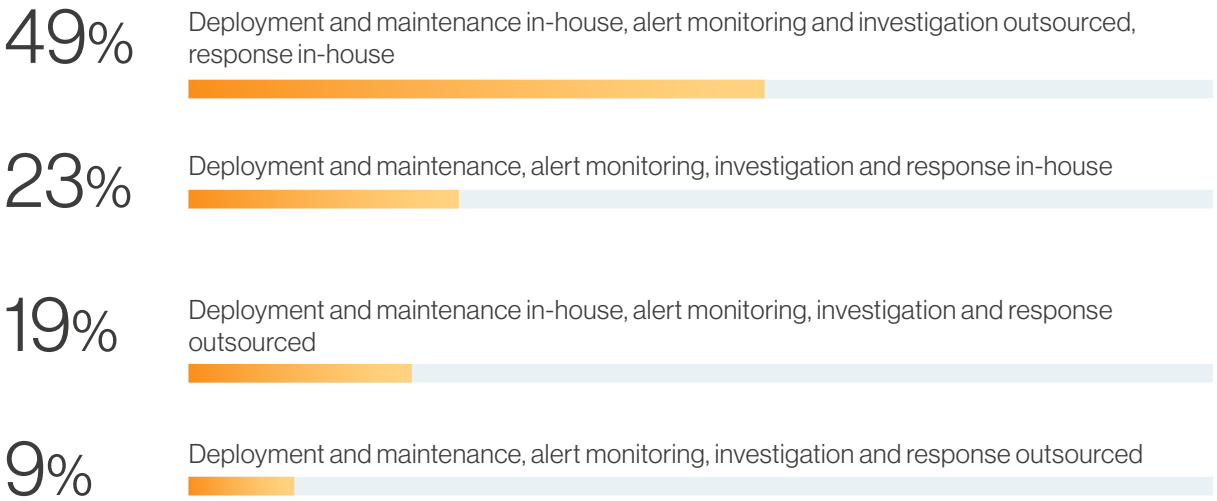
If you could get the additional capabilities you need as a consolidated offering in one of your already deployed products, would you reconsider investing in such a project?



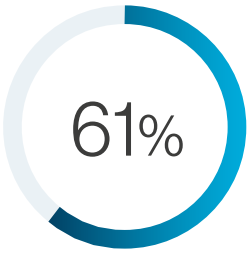
Which of the following cyberthreats will be a focus for your team over the next year?



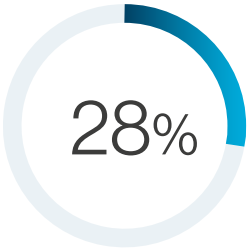
What best describes your in-house vs. outsourced breach protection balance?



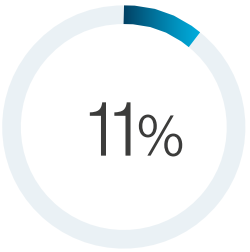
Which of the following best describes the level of breach protection consolidation in your organization?



Low There is no central aggregation of security alerts and the investigation takes place from each product's management console.

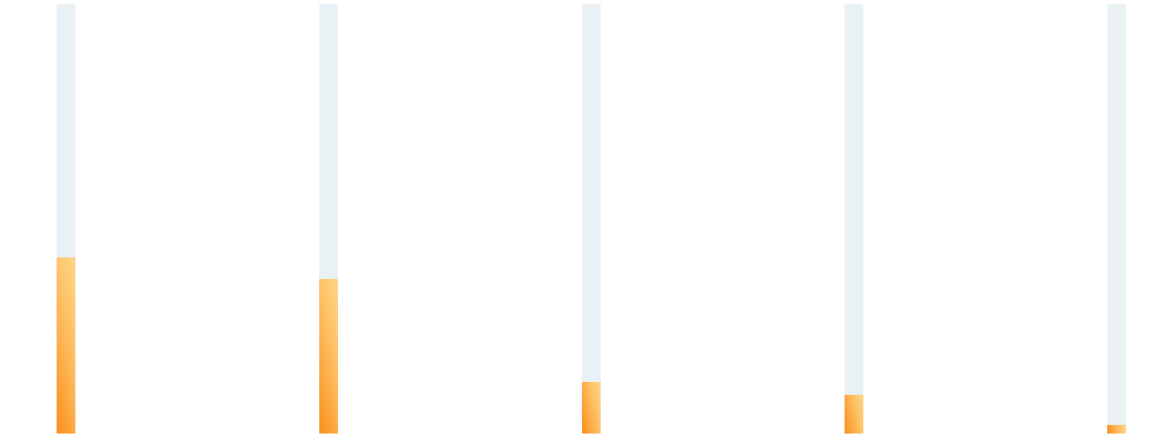


Medium All network, user and endpoint security alerts are displayed on a single dashboard, but normalizing and rating is manual.



High All network, user and endpoint security alerts normalized and displayed on a single console.

Considering the overall alerts generated by the security products in your environment, what is the approximate daily average of alerts that are ignored due to the security team's capacity limits?



20%-40%	40%-60%	0%-20%	60%-80%	80%<
41%	36%	12%	9%	2%

What are the greatest inhibitors you encounter in achieving the level of protection you aim for?

78% Management, maintenance and operational overhead of the security products already deployed

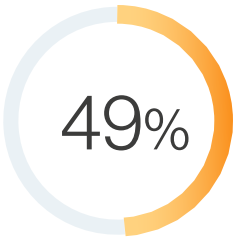
67% Skill level of the security team

53% Size of security team

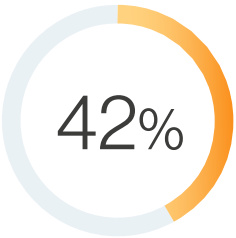
47% Insufficient budget for all the security products my environment requires

31% Alert volume exceeding capacity of security team, leaving potentially critical events unaddressed

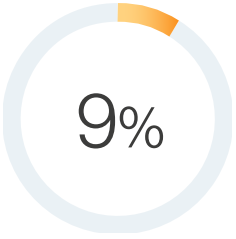
What level of orchestration and automation best describes the state of incident response workflows in your organization?



Low remediation of each type is carried out separately on the respective product (EDR to isolate infected endpoints, Active Directory for compromised user accounts, Firewall to block ports, URLs and IPs, etc.).



Medium a single dashboard from which the user can orchestrate remediation workflows manually with little or no automation.



High a single dashboard from which the user can configure automated playbooks for all of the components in the environment (endpoints, Active Directory, firewall, etc.).

Within the incident response workflows, what are your preferred choices to outsource?

73% Alert monitoring and prioritization

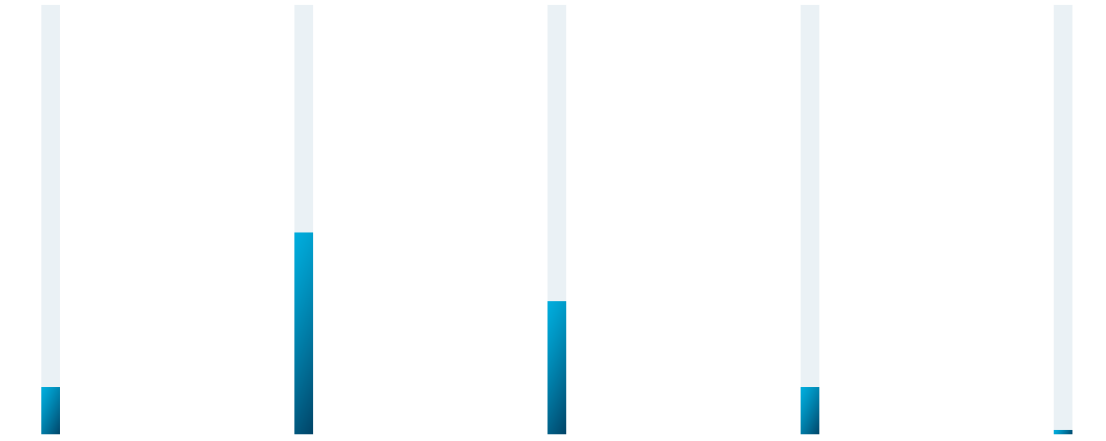
54% Investigation of attack's root cause, scope and impact.

43% Proactive threat hunting

31% I prefer to handle all incident response in-house.

12% Remediation of compromised entities (endpoints, user account, files, etc.).

Within the endpoint protection products you deploy (not counting AV), what percentage of your endpoints are not covered due to deployment issues, software clashes or any other operational inhibitors?



0%-15%	15%-30%	30%-45%	45%-60%	60%>
11%	47%	31%	11%	1%

What is your preferred deployment model for security products?

What best describes the architecture of your environment?