7 UNCOMFORTABLE TRUTHS OF ENDPOINT SECURITY

Results of an independent survey of 3,100 IT managers commissioned by Sophos

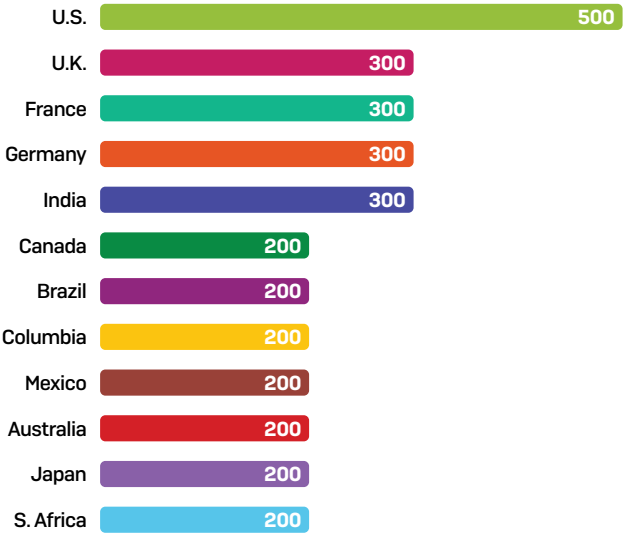
To understand the realities of endpoint security today, Sophos commissioned independent research specialist Vanson Bourne to survey 3,100 IT managers across the globe. The resulting paper reveals the experiences, concerns and future plans of organizations in 12 countries and six continents. It provides deep insight into the day-to-day challenges IT teams face securing their organizations against cyberattacks, as well as their experiences with endpoint detection and response (EDR) technologies.

SOPHOS

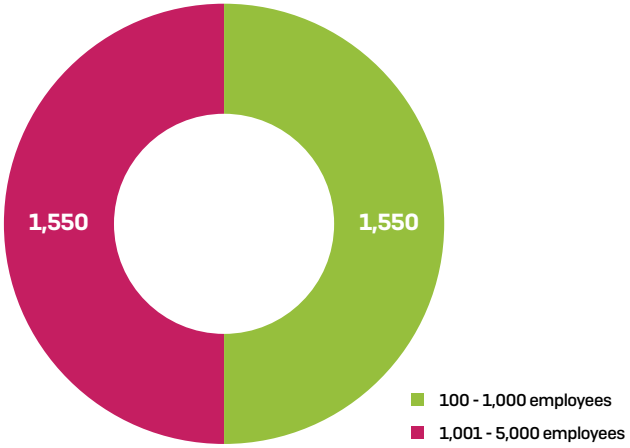
The Survey

U.K.-based research house Vanson Bourne interviewed 3,100 IT decision makers between December 2018 and January 2019. To provide a representative size split within each country, respondents were split equally between 100-1,000 user organizations and 1,001-5,000 user organizations.

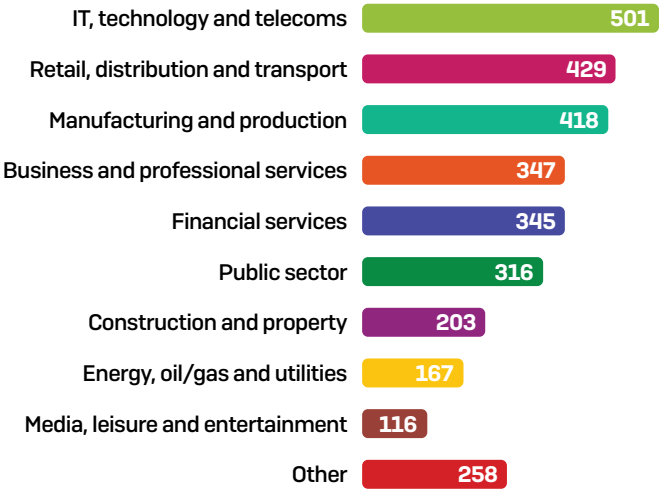
Number of respondents per country



Split of respondents by organization size



Split of respondents by industry



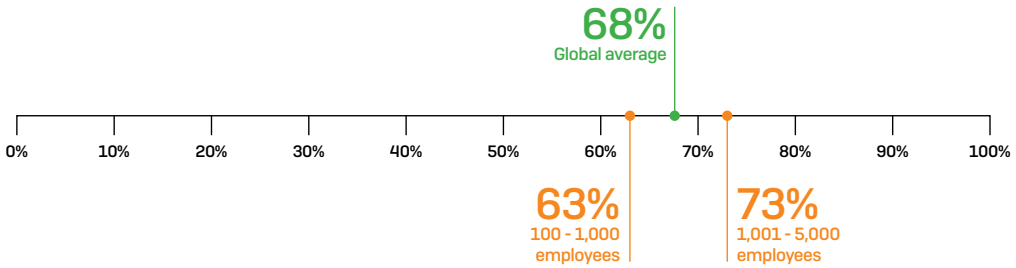
Truth #1: It is now the norm to be a cyberattack victim

More than two-thirds (68%) of organizations say they were hit by a cyberattack in the last year. Larger organizations suffered more attacks (73%) than smaller ones (63%). There are two likely reasons for this difference:

- Larger organizations are more targeted by cyber criminals – they are considered to be more lucrative victims
- Larger organizations are more aware that they've been hit by a cyber threat as they have more IT resources to detect and investigate issues

Definition: Fell victim to a cyberattack

Experienced a cyberattack that they were unable to prevent from entering their network and/or endpoints

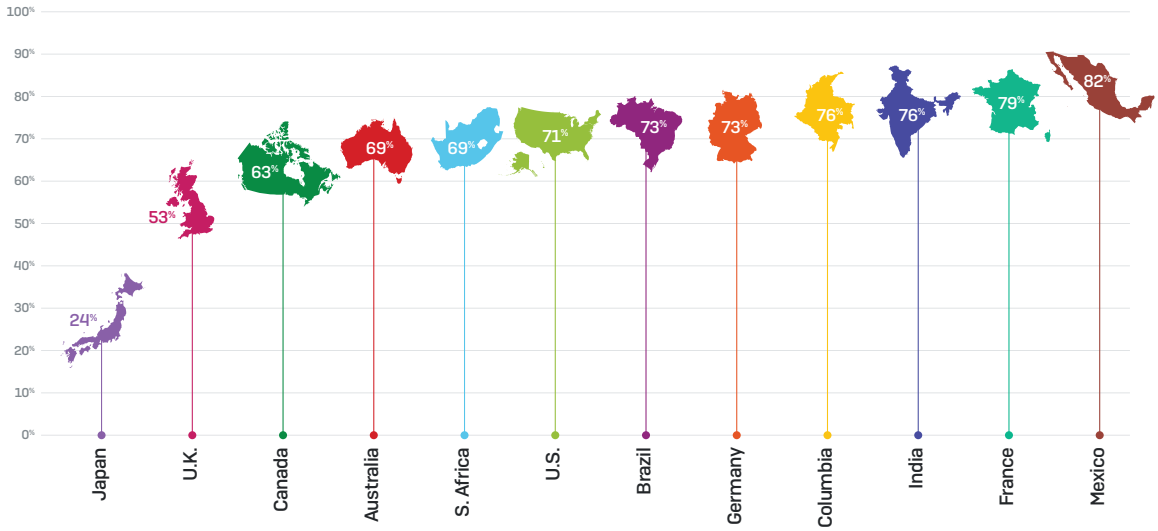


Percentage of organizations that fell victim to a cyberattack in the last year. Asked to all respondents (3,100)

Of course, these are just the attacks that organizations have discovered. The actual number could well be higher.

The key takeaway here is that **everyone should assume that they will be victim of a cyberattack**. Start from this position when planning and evaluating your security strategy, rather than assuming that threats won't get through or you will evade the attention of attackers.

There are significant regional variations in levels of cyberattacks. Japan reported the fewest attacks with only 24% falling victim to a cyberattack in the last year, while Mexico reported the most with 82% of respondents admitting they were hit.



Percentage of organizations that fell victim to a cyberattack in the last year, split by country. Asked to all respondents (3,100)

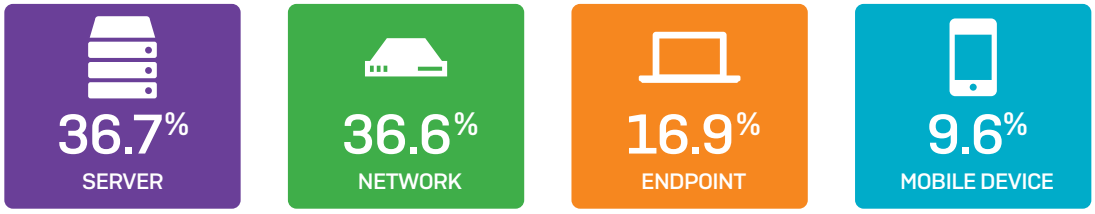
One explanation for this discrepancy is that cyberattack targets are not equally dispersed around the globe. When looking at individual threats we often see clear geographic targeting at play. For example, Emotet has, to date, particularly targeted the Americas, Northern and Western Europe, Australia, and India, while WannaCry wreaked the most havoc in Ukraine.

Unlike lightning, cyberthreats strike twice

Rubbing salt in the wound, the average number of incidents experienced by organizations that fell victim to a cyberattack was two. Additionally, 10% of organizations surveyed suffered four or more cyberattacks in the last year. This suggests that many organizations have ongoing weaknesses in their defenses that are exploitable.

Most attacks are discovered on the server or network

Looking at where in their environments organizations discover cyberattacks reveals a number of interesting insights.



Location where organizations found/discovered the most significant cyberattack they fell victim to in the last year. Asked to respondents from organizations that fell victim to a cyberattack in the last year (2,109)

1. Most threats (36.7%) are discovered on the server

Servers are generally considered "safe" by IT administrators as users don't log into them, but in fact the data shows they are most at risk. Modern attacks often start at endpoints before moving laterally to servers, the higher-value targets. The fact that organizations are catching the threats on the servers rather than the endpoints suggests a lack of visibility into what's happening earlier in the threat chain, as well as endpoint security gaps. It is also possible that attacks are noticed on the server because that is when they can cause the biggest impact to the business.

2. Nearly one in 10 threats are discovered on mobile devices

With 9.6% of threats discovered on mobile devices, the data suggests that mobile threats are a significant danger, and organizations need to ensure all devices with access to corporate information are properly secured.

3. India is nearly twice as likely to discover threats on mobile devices

While 9.6% of threats are discovered on mobile devices globally, in India this number is almost double at 18.8%. This is likely a reflection of both the technology and cultural factors. Firstly, with nine out of 10 mobile phones in India running Android, the preferred platform of mobile malware authors, Indian devices are particularly vulnerable to mobile threats. India also has one of the highest rates of bad app installation, increasing their propensity to mobile infections. In addition, sole reliance on mobile devices for business is much higher in India than in many other parts of the world, therefore the likelihood of a mobile device falling victim to a malicious attack is also likely to be higher.

https://economictimes.indiatimes.com/tech/software/the-critical-flaw-in-indias-mobile-security/articleshow/65085273.cms

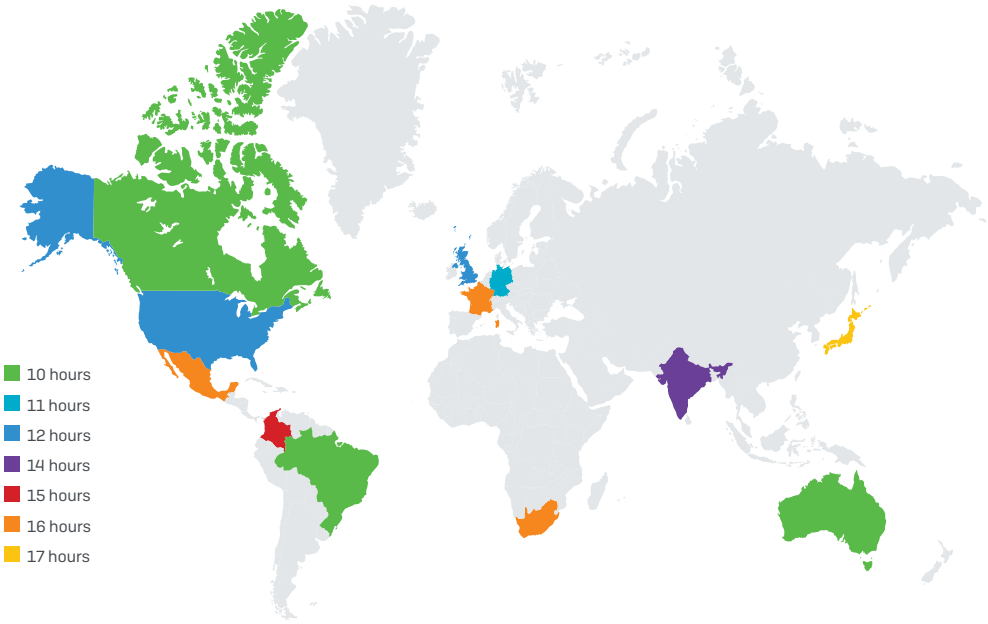
Truth #2: IT teams lack visibility into attacker dwell time

We asked organizations how long it took to discover the most significant cyberattack in the last year. For those that knew the answer, the average was 13 hours.

Average time the most significant threat was in their environment before being detected

Clearly 13 hours is a huge amount of time for a hacker to have uninterrupted access to your systems and data. In this amount of time, a cybercriminal can wreak significant damage, including exfiltrating sensitive data, stealing credentials, installing money-stealing Trojans, installing ransomware, and more.

The time it takes to discover threats varies from country to country: Australia, Brazil and Canada are quickest, taking 10 hours on average; while at the other end of the spectrum, Japanese IT teams take on average 17 hours.



Average time the most significant threat was in the organization before it was discovered. Asked to all respondents who knew how long the threat was in their environment (1,744 respondents)

Thirteen hours is just the tip of the iceberg

While 13 hours is a long time, it is important to remember this this is actually a best-case scenario.

Furthermore, the average dwell time of 13 hours cited by the 1,744 survey respondents who knew how long the threat was in their organization's environment before it was detected may at first glance seem incongruous with other research, such as the Verizon Data Breach Investigations Report, which states that 68% of data breaches take months or longer to discover. This difference in data is hugely illuminating and provides deeper understanding into the realities facing organizations that do not currently have a robust dedicated threat detection and response team.

With 17% of threats, organizations do not know how long it was in their environment before being discovered.

Organizations only see part of the story. As we saw earlier, most threats are discovered on the server, suggesting a lack of visibility at the endpoint. As a result, it's likely that organizations are only seeing an excerpt of the threat trail, rather than the complete situation, resulting in underestimating the time the threat was in their environment. As a result, they are making security decisions with only partial information, and an incomplete understanding of their cyber risk.

Organizations lack the tools they need to accurately assess dwell time. For the vast majority of small- and mid-sized organizations, being able to fully understand how long a threat was in their organization requires time, tools, and expertise that they don't have.

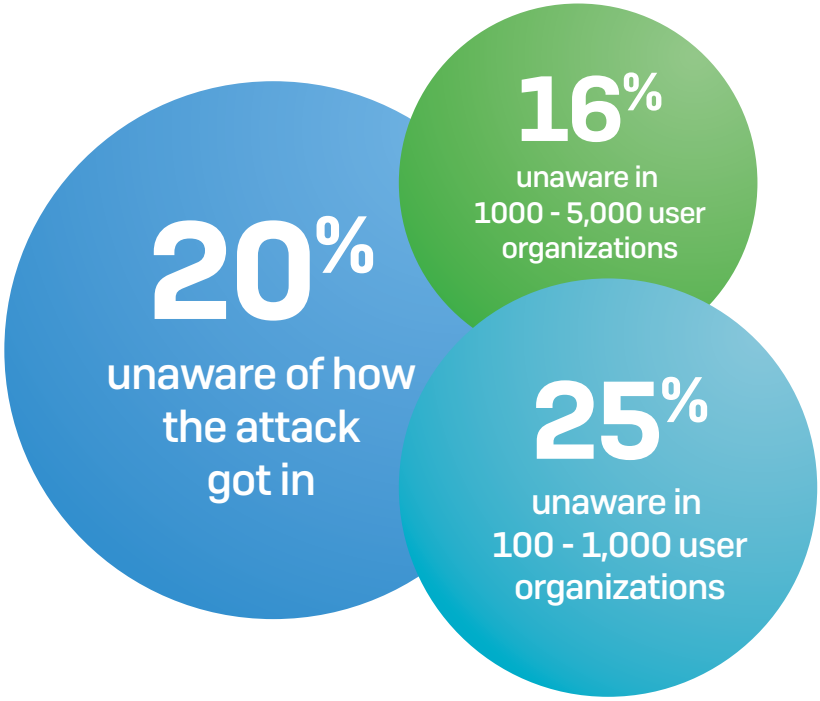
Different types of threats are easier to spot than others. Threats vary greatly in distribution method, techniques used, and end goals. Generic spray-and-pray threats which succeed due in part to their volume (the belief that if I send out enough attacks, one will get through) are generally less well-disguised than sophisticated, highly-targeted stealth attacks. And in fact, many of these "mass market" threats are spotted and stopped within seconds.

The Verizon Data Breach Investigations Report focused solely on data breaches, whereas the Sophos survey participants responded based on a broader range of cyberattacks. The most impactful, damaging threats are often the most sophisticated, with the longest dwell time.

With cybercriminals now masters of disguise, IT managers are acutely aware of the need to identify the tricky, advanced attacks that cause the greatest damage. Indeed, survey respondents said that the most important feature in an endpoint detection and response (EDR) solution is the ability to identify suspicious events.

Truth #3: IT teams can't plug their security gaps because they don't know what they are

A key element of an effective security strategy is to stop threats from getting into the organization in the first place. Yet one in five IT managers are unaware how their most significant cyberattack entered their organizations. As a result they are unable to protect these entry points.



Percentage of respondents that are unaware of how the most significant cyberattack to hit their organization got in. Asked to all respondents that fell victim to a cyberattack in the last year (2,109)

Larger organizations are more likely to know how threats got in than smaller ones. This is likely due both to having more skilled resources and more comprehensive cybersecurity solutions than smaller companies. Often smaller organizations simply don't have the resources or expertise to investigate what happened during an attack – instead, they just focus on cleaning it up. Cybercriminals target organizations of every size. However, the inability of smaller companies to identify their security holes means they are more vulnerable.

Truth #4: Organizations lose 41 days each year investigating non-issues

Organizations spend, on average, four days a month investigating potential security issues, or 48 days a year. However only 15% turn out to be actual infections. As a result, organizations are spending 85% of the time investigating non-issues, equivalent to around 41 days each year. This clearly has significant financial and productivity implications:

- Direct cost – the financial and resourcing impact of spending such significant amounts of time investigating non-issues
- Opportunity cost – the IT activities that staff are not getting to because they are investigating non-issues

This huge inefficiency also helps explain why the most desired EDR feature is identification of suspicious events. By having effective tools in place to help organizations identify what is suspicious, they can focus their limited resources in the right places, rather than searching for needles in a haystack. Being able to better identify suspicious events, organizations will:

- Improve efficiency: use their limited resources more effectively
- Reduce exposure: find and address actual security incidents faster
- Minimize risk: focus resources on the suspicious events that are most likely to put the organization at risk

Truth #5: Four out of five organizations are struggling with threat detection and response due to lack of security expertise

Lack of security expertise in the face of these threat challenges is a major issue. With 80% of IT managers admitting they wish they had a stronger team in place to properly detect, investigate, and respond to security incidents, it's clear that organizations are flying blind due to a shortage of cybersecurity skills.

There is a marked difference in desire for a stronger team between organizations that were hit by a cyberattack (85% want a stronger team) and those that weren't (71% want a stronger team). This suggests that those organizations that have suffered a cyberattack show greater awareness, both of their own lack of security expertise (they've learned the hard way that threats can get through their defenses) and of the challenges in stopping today's advanced attacks and the need for specialist cybersecurity skills to address them.

Unfortunately, addressing this shortage of skills is no easy task. While organizations recognize they need better help, bringing that help into the business is another matter. A full 79% of respondents agree that cybersecurity recruitment is a challenge. In this light, putting the teams they need in place is an uphill battle, and organizations will have the lean on technology such as artificial intelligence to fill in the gaps.

Truth #6: More than half of organizations don't see the value of their EDR solutions

EDR has swiftly become must-have technology. More than nine out of 10 IT managers surveyed (93%) either have or plan to have EDR in their security arsenals. Of those respondents who don't currently have EDR, a massive 89% plan to add it to their defenses, with 61% planning to do so within the next six months. In light of the earlier revelations about time spent investigating security incidents and the lack of visibility into the threat chain, these EDR plans make a lot of sense.

93%
Want EDR in their security arsenal

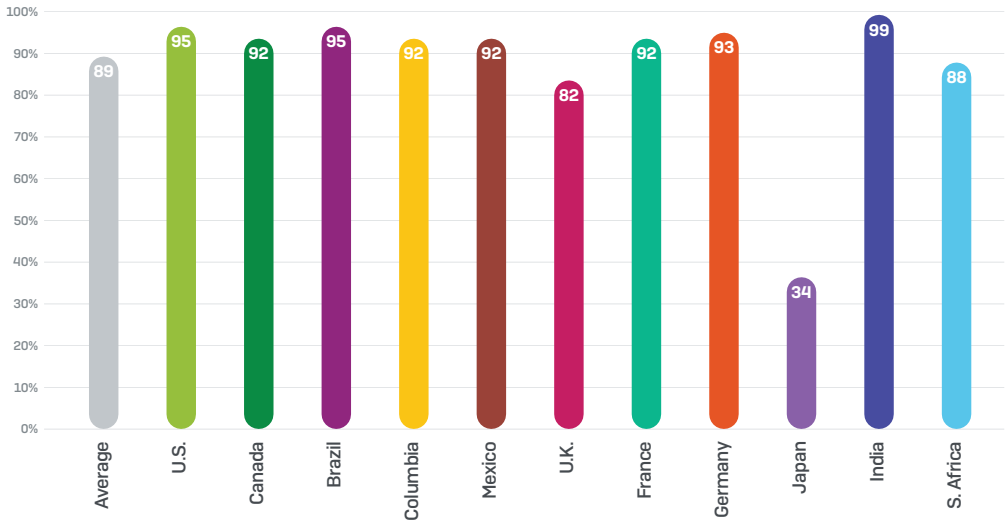
9 in 10
Without EDR, plan to add it

61%
Without EDR, plan to add it within six months

EDR for All
Equal demand for big and small

Interestingly, we see almost equal demand for EDR from both smaller and larger organizations. EDR is clearly no longer exclusive to big enterprises, but rather a tool for all.

Looking across the countries surveyed, Japan stands alone in terms of EDR adoption plans.



Percentage of respondents that plan to add EDR capabilities. Asked to all respondents that don't currently have EDR (1990)

In all countries other than Japan, at least 8 in 10 organizations without EDR technology plan to add it. India tops the list with 99% of organizations that don't currently have EDR planning to add it, closely followed by Australia (97%), the U.S. and Brazil (both 95%). However in Japan just one in three (34%) organizations without EDR technology plan to add it to their security defenses.

Just having EDR is not the answer

While EDR is a powerful tool that can elevate your cyber defenses, you need to have the resources in place to use it effectively and get the most from your investment. Unfortunately, over half of the survey respondents who invested in EDR are unable to do that. For 54% of organizations, EDR was money wasted as they are unable to get full benefit from their solutions.

54%

can't take full benefit from their EDR solution

Interestingly, although you might suspect that smaller organizations would struggle more to get the benefit from their EDR investments, the reality is that organization size is not a factor here. Response data was nearly the same for organizations of all sizes surveyed.

There are a few possible explanations for these results, and it's likely that both come into play across the survey respondents:

Lack of EDR management resource. Organizations need to consider who will manage their EDR solutions to ensure they can take full advantage of them. As we've already seen, lack of cybersecurity skills is a widespread issue.

Usability: Skills mismatch. Technology can only add value if it can be used effectively. Organizations should give due consideration to how easy an EDR solution is to use, and how that fits with their available skills and resources.

Truth #7: Once bitten, twice shy – cyber victims learn the hard way

The survey revealed very distinct differences in some areas between those who had been victims of a cyberattack and those who had avoided hackers. Organizations that fell victim to a cyberattack in the last year are:

- More cautious – they investigate twice as many incidents as other organizations
- Spending more time on cybersecurity – they spend four days a month investigating potential incidents, rather than three for non-victims

There are likely a few factors at play here:

1. **They've dialed up their security following the incident.** Victims will likely have a much greater appreciation of the impact of cyberattacks and are willing to dedicate more time, effort, and resources to stopping them.
2. **They have limited visibility into their environment.** Poor cyber defenses mean more threats get through and they have less ability to look into them. As a result, they have more potential incidents to investigate, with less tools to do so, which takes more time.
3. **They're more aware of what to look for.** As a result of suffering an attack, these organizations are more conscious of the signs that should make them suspicious.

The truth about EDR

This survey has revealed a number of challenges faced by organizations across the globe when it comes to endpoint security, as well as challenges with EDR technology. So what's the truth about EDR, and how does it really fit into the endpoint protection picture?

The reality is that EDR can help address many of the challenges revealed by the survey. Start with understanding cyberattacks. Two out of three organizations suffered a cyberattack last year. However, 17% of IT managers don't know how long the threat was in their environment, and 20% don't know how it got in. EDR can provide answers to these questions, enabling organizations to identify the root cause of the attack, how long it's been in their system, and the potential impact. Armed with this information, organizations can put in place the defenses they need and plug their security holes.

We also saw that it takes organizations, on average, 13 hours to discover a threat. EDR can also proactively identify suspicious events, enabling IT teams to detect attacks that may have gone unnoticed for much longer. As a result, EDR enables organizations to take effective steps to reduce the likelihood they become yet another cyberattack victim.

Another insight from the survey is that organizations spend 48 days a year investigating potential security incidents. EDR can slash this time by offering expert analysis and guided incident response into potential incidents that teams of all sophistication levels can understand and act upon. This dramatically reduces the time spent detecting and responding to incidents.

Yet we've also seen that 54% of those organizations with EDR can't fully benefit from their solution. This is why it is so crucial to choose an EDR solution that works for your organization, rather than one that will just add more work. A properly implemented EDR solution can help organizations use their limited resources more efficiently.

Conclusion

Cybersecurity is an ever-present challenge for organizations of all sizes across the globe. In this light, there are several important points we can take from the experiences of 3,100 IT managers across 12 countries and six continents.

First, when planning their cybersecurity strategies, organizations should start from the assumption that a threat will make its way through their defenses. While doing so, they should also be mindful of the limitations to their visibility into threats and their resulting inability to identify – and block – the gaps in their security armor.

Second, the vast majority of organizations see EDR as an integral part of their security strategies. This is no surprise; EDR is an effective tool to address a number of the challenges highlighted in the survey. At a time when cybersecurity skills are in short supply, an intelligent EDR solution can provide the threat insight and expertise needed to stay ahead of threats.

However, as the survey revealed, simply purchasing EDR is not enough. For far too many organizations, their investments in EDR turn out to be money wasted as they are unable to take full advantage of their EDR solutions. To avoid falling into this trap, every organization should fully consider both the capabilities and usability of an EDR solution before adding it to their security arsenal.

About Sophos

Sophos is a global leader in endpoint and network security. More than 100 million users in 150 countries rely on Sophos as the best protection against sophisticated threats and data loss. **Intercept X Advanced with EDR** enables organizations to understand the scope and impact of security incidents, detect attacks that may have gone unnoticed, analyze files to determine if they are a threat, and confidently report on their organization's security posture at any given moment. Built-in machine learning and threats intelligence from SophosLabs enables you to add expertise, not headcount. For more information and to start a 30-day free trial, visit www.sophos.com/intercept-x.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

To start an EDR 30-day free trial, visit www.sophos.com/intercept-x

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2019-02-26 WP (RP)

SOPHOS