deep instinct

2021

Voice of SecOps

SURVEY REPORT

Introduction

Deep Instinct published its first "Voice of SecOps" research report in July, 2021 to take the global pulse of SecOps professionals. It contained several stand-out findings, including this show stopper: **83% of cybersecurity professionals believe they should be getting more from their AV and EDR solutions.** The theme of this initial research was clear – CISOs want and deserve better from the cybersecurity industry.

The current research report builds upon the previous findings to go deeper into drivers behind that sentiment and explore pressing issues and priorities, including the following:

Key concerns and overall priorities for CISOs and their teams

Significant factors inhibiting the ability to prevent attacks

Strategic investments and the balance between prevention vs detection

This research is based on findings by The Hayhurst Consultancy, which we commissioned to conduct one of the largest industry research studies in 2021 – surveying 1,500 senior cybersecurity professionals in 11 countries across six core market verticals.

83% of cybersecurity professionals believe they should be **getting more from their AV and EDR solutions.**

Management Summary

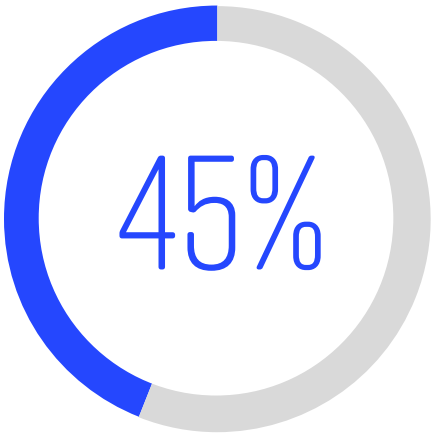
Our research shows that it currently takes SecOps teams the better part of 24 hours to respond to a typical cyber event once it has been detected. Remediation often takes several additional days – and sometimes weeks or months. Given that the fastest ransomware can encrypt in just 15 seconds, there is often substantial dwell time for attackers to move laterally before detection – an "SLA" that is untenable to CISOs and customers.

When an attack is successful, this time lag allows for malware to quickly take root and spread within the host's environment. The longer the attackers remain inside an environment, free to move laterally to reach their goals, the more difficult, risky, and costly incident resolution becomes.

The cybersecurity industry is in clear need of improved cyber controls that will help diminish time-to-resolution and prevent malware from compromising an organization's defenses.
The good news: Nearly half of the professionals surveyed believe that true prevention is possible. 45% of respondents believe it is currently possible to prevent all malware threats from infiltrating their organization's network.

Respondents also have a very positive forward-thinking outlook on prevention. 66% of respondents believe it may be possible to prevent all malware threats from infiltrating their organization's network in the next 2-5 years.

One of the clearest takeaways from the research is that we need to rethink approaches to security in light of the challenges and increased risk that organizations are facing with a higher volume and greater degree of sophistication of today's threats.



of respondents believe it is **currently possible to prevent all malware threats** from infiltrating their organization's network.

The research revealed six key risks that cybersecurity teams are being challenged to mitigate:

Endpoint Risk

The number of endpoints is increasing. The challenge lies in both identifying and protecting them without impacting operational efficiency.

Cloud Risk

Public, private, and hybrid cloud deployments increase the challenge of a business having full visibility into its endpoints. Additionally, a significant number of cybersecurity professionals cannot guarantee that files already stored in their cloud do not contain malware.

File Upload Risk

The increasing volume of file uploads that may contain malware, such as .exe files, as well as those by partners and other third parties, creates a malware monitoring headache.

Hybrid Workforce Risk

The trend to remote work where anywhere and anytime is the new normal and creates a larger, more vulnerable attack surface.

Software Security Exposure Risk

Network attached storage and virtual servers are seen as being especially vulnerable.

Human Risk

Despite investing in training, most cybersecurity professionals don't trust their end users to not click on malicious links.

The Perception of Threat Prevention

It's clear from the research that cybersecurity professionals understand and embrace the fact that their role is one of the most challenging in business today. Businesses have placed more emphasis on both prevention and detection as malware threats increase. Threat detection (62%) has seen a slightly higher increase than prevention (57%), but both are clearly seen as important.

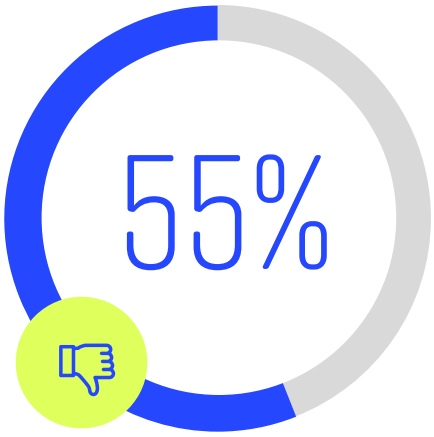
More than half (55%) of the 1,500 professionals we surveyed believe it is not currently possible to prevent all malware from infiltrating their organization's network.

In fact, only one in eight respondents (13%) currently believe preventing all malware is "definitely possible" (with the balance of respondents unsure).

That view is consistent in every country we surveyed for this research – most pointedly in Italy, where not a single respondent believed it is definitely possible to prevent all malware from infiltrating their organization's network at this moment.

However, cybersecurity professionals may take comfort in the fact that their peers in the Technology space are twice as likely as those in other sectors to believe that prevention of all malware is indeed currently possible.

Respondents in the largest companies were most likely to believe that malware prevention is currently possible – this despite the fact that they are protecting the most complex hybrid environments, a majority of which contain legacy systems.



More than half (55%) of the 1,500 professionals we surveyed believe it is **not currently possible to prevent all malware** from infiltrating their organization's network.

The top factors inhibiting organization's prevention capabilities are as follows:

44%	Our current security stack lacks comprehensive threat prevention for never seen-before-malware
43%	Improbability of identifying zero-day threats before they activate
39%	Lack of trained staff available to implement more prevention measures
29%	Volume of endpoints that need protection

Overall, the survey showed that in the next two to five years there is a 59% increase in optimism regarding the viability of prevention. There is conclusive evidence that the larger the company – either defined by revenue or employee headcount – the more likely respondents were to believe that complete prevention is possible.

Just 8% of the largest companies believed it would not be possible to prevent all malware in the next two to five years.

Given that larger companies are the most likely to invest in new technology and innovation, there is hope to all organizations as new solutions to prevent malware become available.

Most Feared Tactics Employed by Threat Actors

In our survey, we discovered the average time to respond to an incident globally is 20.9 hours, and the evolving tactics of threat actors are of great concern.

Bad actors "setting up hidden persistence" (41%) and "searching for data / memory pages" (40%) are the two key tactics most feared by cybersecurity professionals. Italy (50%) and UK (49%) respondents were significantly more likely to cite the latter than their peers.

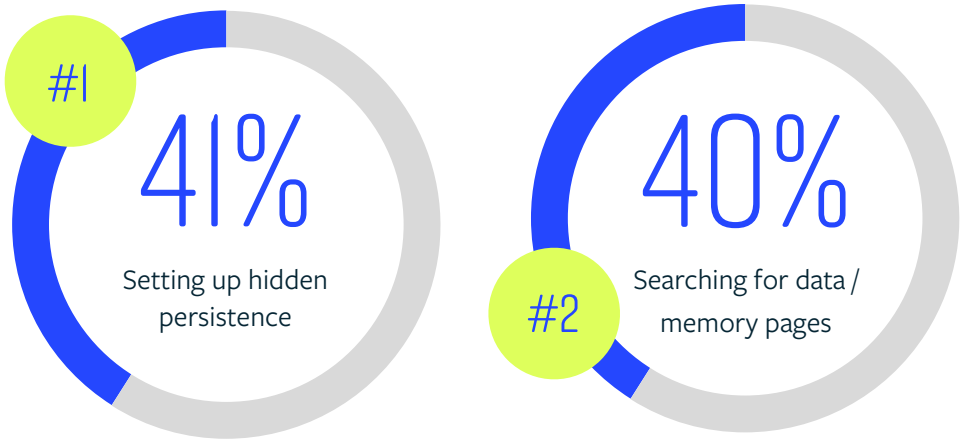
Setting up hidden persistence, the act of hiding inside the network and remaining there to execute attacks regardless of the termination of programs, is significantly more concerning in the manufacturing vertical (49% respondents) than in other verticals, and C-Suite respondents are significantly more likely than their staff (46% vs 36%) to see hidden persistence as a key barrier to ensuring a reliable defense against advanced attacks.

Smaller businesses were significantly more likely than the largest to fear "malware that behaves like an installer of auto-update component of regular software" (40% vs 21%), and phishing (36% vs 25%).

Rounding out the top five concerns are the disabling of AV or EDR solutions (31%) and attackers deleting their logs to cover their tracks (29%).

What is clear from our research is that there is no single tactic being employed by cybercriminals – they will utilize a number of different methods to compromise a company's defenses, making it all the more difficult for organizations to detect them once they infiltrate the network.

The two key tactics most feared by cybersecurity professionals.



PERHAPS IT IS NOT MORE DATA THAT IS NEEDED, BUT A MORE EFFECTIVE USE OF IT.

Key Barriers to Detecting More Threats

Having identified the key threats, we then asked respondents to identify the key challenges to detecting threats and improving their security posture.

The top barrier cited was the sheer volume of never-before-seen malware, with 44% of respondents citing this as their key concern (this was most significant for 56% of Japanese respondents and 57% of those working in the Public Sector). **Coming in a close second (30%) was the time it takes to investigate threats once they are discovered.**

As we examine in more detail in section 4 below, the third barrier was the time taken to investigate threats, cited as a key concern for 39% of respondents.

A lack of qualified SecOps staff was reported as a key threat detection challenge by 35% of respondents, with more than half of Healthcare (52%) and Public Sector (55%) respondents believing this issue to be particularly acute.

Interestingly, when we asked respondents to rank their top security concern from a range of options, "lack of telemetry" was only cited by 13% of respondents as top security concern, with only 8% citing a "lack of forensics."

This is telling us that organizations are not lacking for data. Given the focus on adopting solutions like EDR, NDR, and XDR which rely on user, network, and threat telemetry, combined with a lack of confidence in preventing threats, leads us to conclude that perhaps it is not more data that is needed, but a more effective use of it.

Interestingly, and somewhat contrary to other published research, the speed at which organizations are digitally transforming does not appear to be a root cause of the current challenges that SecOps teams face. Only 8% of respondents "strongly agree" that the pace of transformation is creating blind spots for them.

The Increasing Time Pressure on SecOps Teams

Security incidents are a constant concern for CISOs and their teams. Not only do they present a serious threat to a businesses' operability, they can also be incredibly time consuming for the SecOps team to resolve, leaving fewer resources for basic security hygiene.

As stated earlier, the average time globally to respond to a security incident is 20.9 hours – and even a well-resourced SecOps team with around-the-clock coverage can often take a full 24 hours to resolve an incident.

The picture changes a little by country – Sweden is typically the slowest to respond (25.5 hours), but even the quickest – the Netherlands – still take 17.2 hours, on average, to resolve an incident.

Financial Services appears to be the quickest sector to resolve an incident (15.9 hours) – but it is also happens to be one of the most tightly-regulated sectors, with some of the highest regulatory fines. The Public and Healthcare sectors (probably the most under-resourced) are the slowest – taking an average of 24.4 and 24.0 hours to resolve, respectively.

As demonstrated earlier, it would seem that the largest companies are the best resourced to remediate. Cybersecurity professionals at the biggest companies we surveyed claimed to respond the quickest (14.7 hours for U.S. $10B+ companies), and those at smaller companies respond the slowest (25.2 hours for U.S. $500M - $1B companies).

The Public and Healthcare sectors (probably the most under-resourced) are the slowest

24.4
HOURS

24.0
HOURS

Percentage of Endpoints protected by a security agent:

99%

of the 1,500 Cyber Security professionals surveyed reported that they did not believe all of their endpoints were protected by at least one security agent.

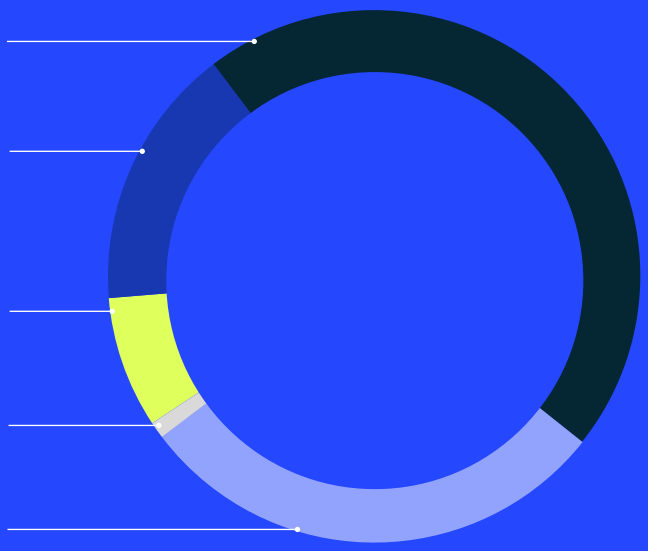
46% reported one-half to three-quarters

16% reported one-quarter to one-half

8% reported under one-quarter

Only 1% reported 100% of coverage

29% reported three-quarters to 99%



The Root Causes of Concern

We also explored the multiple attack surfaces and overall risk areas that are top of mind for respondents.

ENDPOINT RISK

Our research has identified that the seemingly exponential rise in the volume of endpoints that businesses need to protect is a key source of risk exposure.

Yet despite this, 99% of the 1,500 Cyber Security professionals surveyed reported that they did not believe all of their endpoints were protected by at least one security agent. This was evident even of the best-resourced companies in the most technologically advanced sectors.

On average, respondents reported that only 63% of their endpoints were installed with at least one security agent. (The U.S. had the highest coverage at 67.4%; Spain had the lowest at 54.8%.)

Financial Services had a higher proportion of endpoints secured than any other vertical (71.8%), compared to the Public Sector with the fewest (53.4%).

That said, where endpoint security agents are deployed, cybersecurity professionals use multiple agents to shore up their defenses. **Most secured endpoints typically have four agents deployed**. Technology companies were likely to have the highest average number of agents deployed (4.4), while the Public Sector and Manufacturing, the least (3.4).

What is the perception of organizations on installing more security agents?

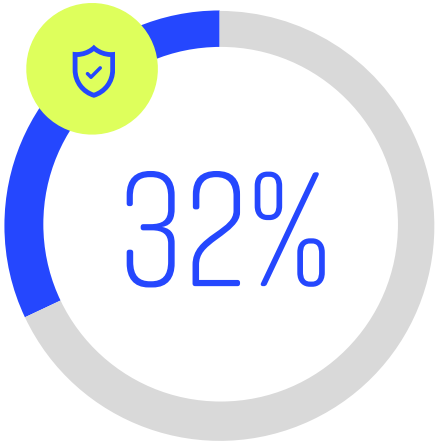
With the disappearance of the perimeter and increasingly distributed and hybrid workforces, cybersecurity professionals understand that their endpoints represent a growing attack surface. The survey responses provided insights into the perceptions of cybersecurity teams regarding installing more agents.

31% of respondents said they "will install as many (endpoint protection agents) as they believe necessary to mitigate risk," while an even higher proportion (46%) would only take this step "provided system performance itself is not impacted."

Our research shows that only one-third (32%) of respondents claim that every endpoint has the same level of protection. (U.S. respondents were the most likely to make this claim (42%), as were respondents in Financial Services (47%), and the largest companies (66%).

Cybersecurity professionals are largely unable to ensure consistent endpoint protection – 46% of respondents claim they are working towards this goal, and a further 19% cited a desire to do so, but lacked the needed tooling to accomplish this goal.

This leads us to the conclusion that organizations are making budget-driven decisions about which endpoints to protect based on which ones represent the greatest risk to the organization should they become compromised.



Only one-third (32%) of respondents claim that **every endpoint has the same level of protection.**

Challenges at the Endpoint

25% One-quarter of the respondents stated that user experience is hindered by latency issues on the endpoint

26% Complexity was cited by 26% as impeding their ability to install more endpoint security agents.

35% Only 35% of respondents claim all their endpoints have the same level of visibility to ensure consistent patching.

38% Again, only 38% of respondents claim the ability to consistently block a threat across all their endpoints.

While the U.S. is in front with 54% of respondents who believe they can block a threat across all endpoints, it still means that almost half the businesses in perhaps the world's most technologically advanced economy face significant challenges when trying to ensure adequate and consistent endpoint protection.

20% are "very confident" that the files stored in their cloud are **not malicious**.

CLOUD VISIBILITY AND STORAGE RISK

Given the widespread gaps in endpoint protection, part of the challenge is the result of the unintended consequences from increased cloud adoption.

When asked what the main challenge was with regards to installing endpoint agents, "cloud limiting our visibility into endpoint behaviour" was cited more than any other reason amongst our respondents (30%).

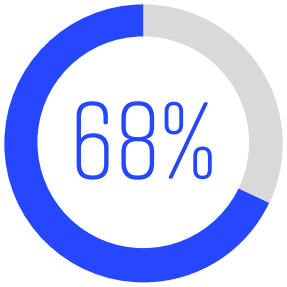
Under 20% are "very confident" that the files stored in their cloud are not malicious. C-Suite respondents tended to be slightly more confident that files stored in the cloud were not malicious as compared to their staff. Spanish respondents (9%) were the least confident in this regard, with Swedish and German respondents also significantly more likely to lack confidence in this regard compared to the average.

Financial Services (27%) and Technology (30%) respondents had the highest confidence, comparatively speaking. Not surprisingly, the relative confidence was also highest at the larger companies compared to the smaller ones. But even then, only 30% of respondents at businesses with revenues of U.S. 10bn+ were "very confident" that the files stored in the cloud were not malicious.

RISK OF MISTAKEN UPLOAD OF MALICIOUS FILES

Regardless of whether data is stored in a private or public cloud or locally on-premises, the increasing volume of file uploads that are a necessary part of conducting business in an interconnected world creates further challenges.

When asked "to what extent, if at all, are you concerned about users, partners, suppliers, and customers unwittingly uploading malicious files through your applications?" 68% of respondents in our research had some concern with regards to the unwitting upload of malicious files. CISO's were 5% less likely than their staff to be very concerned about this issue. While 76% of organizations with 5,000 to 10,000 employees expressed the highest level of concern, over half (55%) of organizations with 50,000 plus employees still harboured a high level of concern. Respondents in Healthcare (19%), Manufacturing (21%), and the Public Sector (20%) were significantly more likely than their peers (12%) to be "very concerned" about this issue.



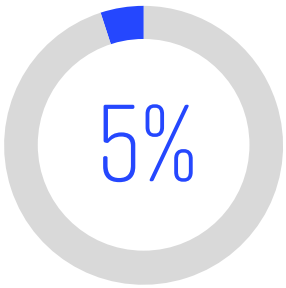
of respondents in our research had **some concern** with regards to the unwitting upload of malicious files.

Executable files (.exe, .com., .dmg, etc.) seem to be ones considered most threatening (33% of respondents citing them as being the most concerning with 47% in Japan and 42% in Germany), system files like .dll and pdf files ranked #2 and #3, respectively.

Interestingly, for Financial Services respondents, pdf files were as big of a concern as .exe files – possibly because of the large-scale requirement of financial services customers to upload pdf files, like mortgage applications or insurance contracts, as part of an application process.

HYBRID WORKFORCE RISK

One of the key impacts of COVID-19 on SecOps has been the significant increase in the proportion of a company's workforce that was quickly transitioned to work off-site (and many plan to continue with a hybrid workforce going forward). Even as remote work globally has now become more of the norm than an aberration, hybrid workforces carry their own distinct cyber risks that may have not been fully planned for or mitigated at this stage.



of respondents had **"no security concerns"** about a hybrid workforce.

Only 5% of respondents had "no security concerns" about a hybrid workforce. Clearly, nearly all of those surveyed see security gaps that should be addressed. Companies large and small appear to be equally affected – company size did not appear to have any influence on the extent to which respondents agreed on the level of security concern.

Key concerns regarding hybrid working cited by our respondents were, "how cybersecurity teams can ensure employees have secure remote access" (55%), and "preventing use of unapproved services" (51%). "Bring Your Own Device (BYOD)" ranked a close third (47%).

Not surprisingly, the Healthcare sector was significantly more likely to cite their current security solutions as being insufficient to cope (53%) versus their peers in other industries. Given the conditions and stresses on healthcare networks – from the past year, cybersecurity should not be another major risk factor causing hardship for SecOps in this sector.

OTHER SECURITY EXPOSURE RISK

When we look beyond the endpoint there are some significant areas of exposure that play into an organization's security posture.

When asked where else organizations felt concern about their security exposure, "Network Attached Storage (NAS)" (65%) and "Virtual Servers" (62%) were most likely to be cited as having a "substantial" or "critical" threat exposure. "DNS" came in third at 53%, followed closely by "IoT," "SaaS," and "Containers."

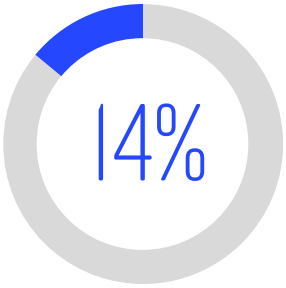
NAS is seen as a particular threat in Italy (83%), Canada (79%), Australia (76%), and Spain (75%). IoT was seen as a significant threat in Australia (56%) and France (54%).

DNS is seen as a more significant threat to Retail & eCommerce respondents (60%) than in other verticals (average 53%).

In the context of this survey, two of the most commonly used software packages, Microsoft O365 and Google Workspace, were the least likely to be cited as having "significant" / "critical" threat exposure (15% and 9%, respectively).

MALICIOUS LINK RISK

Some of the biggest cyber exposure in any organization is human in nature, rather than systemic. No matter how much training employees are provided, attackers invariably find ways into an environment, outsmarting even the most diligent and disciplined end users. And CISOs and their teams are aware of vulnerabilities present with the human element. Only 14% of respondents have "complete" confidence in their employee's ability to spot malware links before clicking on them.



of respondents have **"complete"** confidence in their employee's ability to spot malware links before clicking on them.

Staff in some countries appear to be more trusted than in others by their security teams. U.S. and Dutch respondents had the highest overall confidence in their colleagues not being fooled by threat actors – 57% and 59%, respectively, being "completely" or "fairly" confident. Yet only 2% of Italian respondents were "completely confident" that their colleagues would be able to spot a malware link without clicking on it.

Respondents at the largest companies surveyed are more confident in their colleagues, yet still only 23% are completely confident in their end users to identify malicious links.

Technology industry respondents have the highest confidence in their colleagues in this regard – 74% either being "fairly or completely confident." Yet almost half of respondents working in the Public Sector (46%) had some level of concern that their colleagues would not be able to spot a malware link without clicking on it.

Future Investments in Security Solutions

Companies faced with staffing shortages, a high volume of alerts, and long incident response times have a careful balancing act to follow with regards to how best to deploy their resources.

As we referenced at the start of this report, research shows that businesses are increasingly investing in both prevention and detection, with detection showing the greater increase in investment. (Threat detection has seen a slightly higher increase (62%) than prevention (57%), but both are clearly seen as important.)

The security solutions most likely to be attracting increased investment are "Threat Intelligence" (46% increase in investment), "SIEM" (37% increase in investment), "Endpoint Protection" (36% increase in investment), and "Endpoint Detection and Response" (34% increase in investment).

Approximately one-third of organizations plan to decrease, replace, or retire legacy antivirus solutions, only surpassed by a decreased investment in web proxies (45%) and vulnerability scanners (40%).

While these investments point to more data, it was evidenced in the research that most organizations felt that more telemetry was not what they needed. A considerable proportion of endpoints remain unprotected, and confidence in cloud-based data not harboring malware is low. Ransomware, zero-day threats, and never-before-seen malware are the most significant issues with regards to securing a company's defenses. This is compounded by the impact of hybrid workforces and a lack of skilled security staff.

Rethinking Prevention

As evidenced by the widespread pessimism that malware cannot be prevented before it takes root, the research has identified that traditional security solutions are unable to mitigate vulnerabilities with anything close to 100% certainty.

Yet the fact that cybersecurity professionals' pessimism is not entirely universal suggests that some believe that good preventative solutions are currently available, if not yet widely known about or adopted.

There is an opportunity to meet the attacker earlier, before they reach the endpoint, as evidenced by a small proportion of respondents (11%) who believe they will not need to install further endpoint security agents in the future. Intriguingly, respondents in the Technology sector (26%) were more likely than those in any other sector to hold this view.

Given the risks and costs of detecting and responding to a threat after it executes on the endpoint, organizations must consider how to achieve the following:

- Effectively predict and prevent cyberattacks without the need for human intervention.
- Reduce the burden of detecting malware after it executes on the endpoint.
- Preserve the integrity of cloud and local storage by preventing malicious files.

The research suggests the following:

- There is optimism that real prevention offers an opportunity to stop malware before it reaches the endpoint and infects the network.
- A lack of universal security agent coverage on the endpoint leaves a gap in security defenses.
- While anti-virus investments are decreasing, there is hope regarding future prevention solutions that will offer a more robust first line of defense.
- Earlier identification of ransomware and zero-day threats offers an opportunity for organizations to reduce risk.
- We cannot rely on humans as a first line of defense, and need to address how to provide better prevention at the front line.
- Files that are uploaded by end users or customers into the cloud represent a high security risk.
- There is an opportunity to improve the impact of endpoint agents on operational efficiency.
- Automation will improve an organization's ability to respond faster.
- While more data is not needed, there is a desire for better data and correlations of events to help combat the current threat landscape.

There is confidence in the possibility of complete prevention in the next 2-5 years. If we plan to move ahead of sophisticated attackers who are constantly shifting attacks and creating harder-to-detect malware, we must address how to stop threats earlier, before they land inside our networks.

Appendix

About the Research

Deep Instinct commissioned research on the threats faced by the cybersecurity community from independent marketing and market research company Hayhurst Consultancy in July, 2021.

Hayhurst Consultancy used their experience to examine the views of 1,500 cybersecurity professionals in 11 countries on the threats they face and the steps they are taking to combat them. All surveys were conducted under the Market Research Society Code of Conduct primarily using a telephony data collection approach supplemented by online research, as required.

Respondent Base

Interviews were conducted with 1,500 senior Cyber Security subject matter experts from companies in the U.S. (200), UK (200), Germany (200), France (200), Canada (100), Sweden (100), Italy (100), Spain (100), Netherlands (100), Japan (100), and Australia (100).

All interviewees worked for businesses with 1,000 employees or more, and for businesses with revenues of at least U.S. $500M annually.

Interviewees came from a broadly representative s ample of businesses in Financial Services, Retail & eCommerce, Healthcare, Manufacturing, Public Sector, Critical Infrastructure and Technology / related advisory businesses.

Typical job roles of interviewees were CISO, CTO, ITO, Chief Security Officer, Head of Information Security, Information & Security Risk Manager, Malware Analyst, etc.

All respondents were screened for having some level of input into the management of information security in their company. Half of the respondents were CISOs or in an equivalent role.

Report author

Simon Hayhurst
www.hayhurstconsultancy.co.uk