SOPHOS
Security made simple.

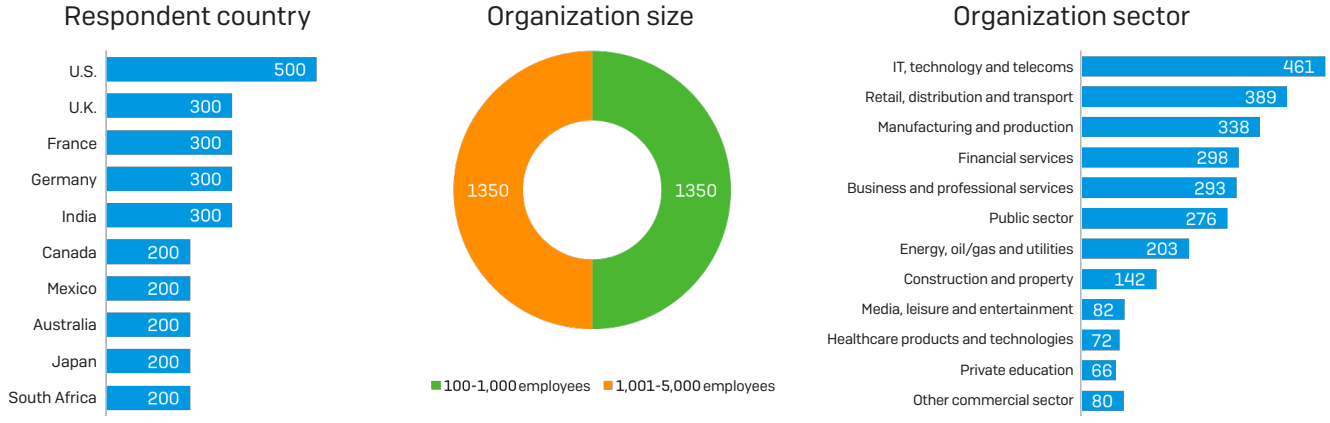
The State of Endpoint Security Today

An independent study of 2,700 mid-sized organizations across five continents

Introduction

In late 2017, Sophos sponsored an independent global research study to gain a deeper understanding into the state of endpoint security in mid-sized organizations across the globe. This extensive research program explores key areas of development and concern: security breaches, technology usage, attitudes to threats, and future investment plans.

Conducted by leading UK research house Vanson Bourne, the study surveyed 2700 IT managers in organizations of 100 to 5,000 users in 10 countries, and across five continents.



Survey demographics: Number of respondents by country, organization size, and business sector

This resulting paper delivers powerful insights into the prevalent cybersecurity issues facing organizations today: from ransomware to exploits and machine learning, it shares the experiences and future plans of IT managers across the globe. It's an illuminating read, providing insight into where the field stands on these issues.

The Shadow of Ransomware

Executive Summary

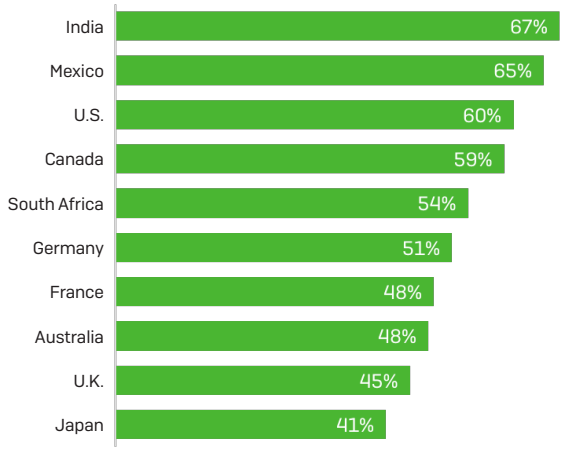
- 54% of organizations were hit by ransomware in the last year
- On average two ransomware attacks per organization
- Median impact per affected organization ≈ US$133K (£100K)
- Healthcare was the top target, followed by energy, professional services, and retail
- India had the highest level of infection, followed by Mexico, U.S., and Canada
- 77% of organizations were running up-to-date endpoint security at the time of the attack
- 54% of organizations do not have specific anti-ransomware protection in place

Unlike lightning, ransomware does strike twice

Ransomware continues to be a major issue across the globe, with 54% of organizations surveyed hit in the last year, and a further 31% expecting to be victims of an attack in the future. Unlike lightning, ransomware can – sadly – strike twice with affected organizations suffered on average two ransomware attacks in the preceding 12 months.

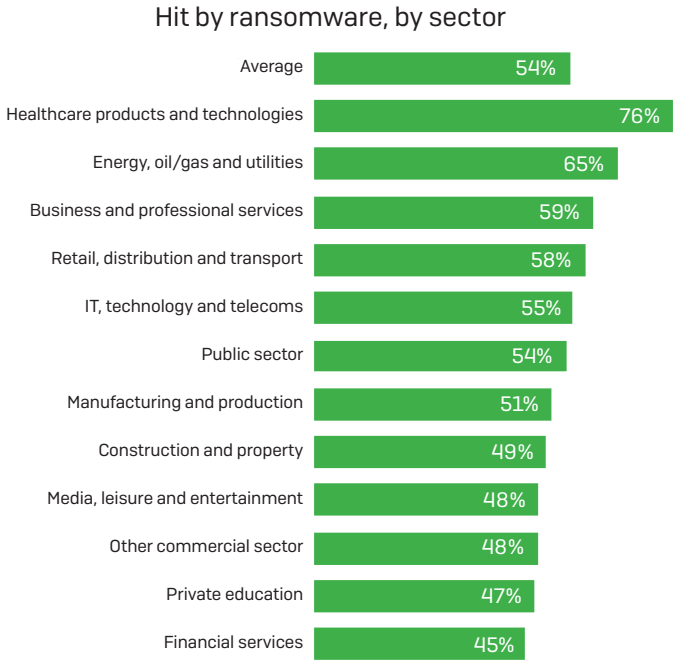
While ransomware held organizations hostage in every country surveyed, the extent of ransomware attacks varied significantly across the survey group. India tops the table of ransomware victims with a full two-thirds (67%) of respondents hit by ransomware in the previous year. Conversely, at the other end of the scale, in Japan four in ten (41%) had suffered an attack. Language likely plays a significant role here – ransomware attacks frequently start with a phishing email. The same English-language email can be used in at least six of the countries surveyed, whereas an email in Japanese can only be used in a single geographic area. In this case, the complexity of their language gives the people of Japan an added defense.

Hit by ransomware, by country



% of organizations hit by ransomware in the previous 12 months

Propensity to suffer a ransomware attack varies greatly by industry sector. Healthcare stands out with 76% of respondents falling victim in the last year. At the other end of the scale, financial services are the sector least likely to have suffered a breach, though even that industry felt the pressure with 45% of respondents attacked by ransomware.



% of organizations that had been hit by ransomware in the previous 12 months, by sector

Although both healthcare and financial services hold high-value data, healthcare is often perceived as a soft target, leading to increased frequency of attack. That assumption is not without merit – healthcare tends to have an aging IT infrastructure, leaving security holes, as well as restricted resources for improving IT security. Healthcare organizations are also considered to be more likely to pay a ransom.

Interestingly, hackers are not discriminating by organization size. The likelihood to suffer an attack is about the same for both smaller and larger companies responding to the survey: 50% of the 100-1,000 user organizations had fallen victim, compared with 58% of those in the 1,001-5,000 user category. Big or small, everyone is a target.

Traditional endpoint protection alone is not enough

With over three quarters (77%) of ransomware victims already running up-to-date endpoint security, organizations are discovering the hard way that stopping ransomware requires specialized protection.

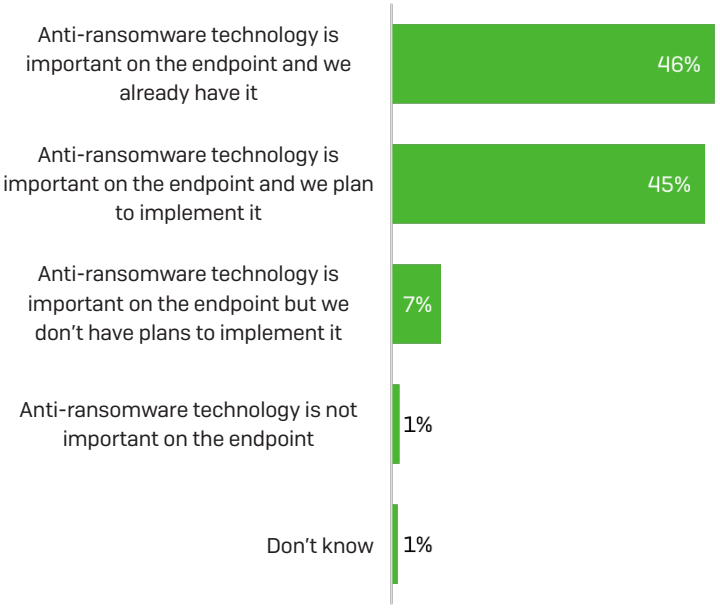
Percent of organizations hit by ransomware in previous 12 months that were running up-to-date endpoint protection at the time of the attack

Endpoint protection status	Total
Running up-to-date endpoint protection	77%
Not running up-to-date endpoint protection	21%
Don't know	1%

Base 1468

Following the high-profile WannaCry and Petya ransomware outbreaks in 2017 and the high level of ransomware victims, it's unsurprising that almost everyone surveyed (98%) agrees that having anti-ransomware technology on the endpoint is important. However, over 50% of organizations don't have anti-ransomware technology in place, putting them at increased risk of attack.

Respondents' views on incorporating specific anti-ransomware technology into their organization's endpoint protection



The level of investment in protecting against ransomware varies significantly between sectors. Energy, oil/gas, utilities, and healthcare are the industries that have invested most significantly in anti-ransomware technology. They are considered high value targets for criminals, and run on bespoke and quite expensive equipment running on old technology – like MRI scanners for healthcare or drills in the oil industry.

Conversely, media, public sector, and private education are least likely to have invested in anti-ransomware technology. The reasons for this vary, but often are the results of budget constraints – the public sector particularly falls victim to this challenge – or a lack of awareness. Limited IT resources also put these organizations behind on adding anti-ransomware protection.

Respondents' views on incorporating specific anti-ransomware technology into their organization's endpoint protection by sector

	Average	Business and Pro Services	Construction and property	Energy, oil / gas, utilities	Financial services	Health	IT, tech, telecoms	Manuf-acturing	Media, leisure, entertain	Public sector	Private education	Retail, distribution transport	Other
Anti-ransomware technology is important on the endpoint and we already have it	**46%**	47%	46%	53%	52%	53%	44%	46%	38%	39%	35%	46%	51%
Anti-ransomware technology is important on the endpoint and we plan to implement it	**45%**	42%	46%	42%	41%	42%	47%	46%	51%	50%	45%	43%	36%

The healthcare conundrum: Biggest victims, largest investors in prevention

Healthcare presents an interesting equation. They are the most likely to suffer an attack (76%), and yet are also the most invested in anti-ransomware protection (at 53%, alongside energy, oil/gas, and utilities).

How does this dichotomy play out? In part, it's because criminals continue to see healthcare as an easy target, so a disproportionate amount of attacks are aimed at the industry. Also, the older technology healthcare relies on (such as the afore-mentioned MRI machines) only run on old operating systems.

Healthcare also tends to fight a battle against limited or restricted resources in this area. A lack of people, hardware, and software lead to patchy security, so even when one part of the organization has the necessary anti-ransomware protection, it's not across the board. Malware can still get in.

And there's also the issue of quality. Not all anti-ransomware protection is created equal. Some options simply aren't as effective at stopping an attack.

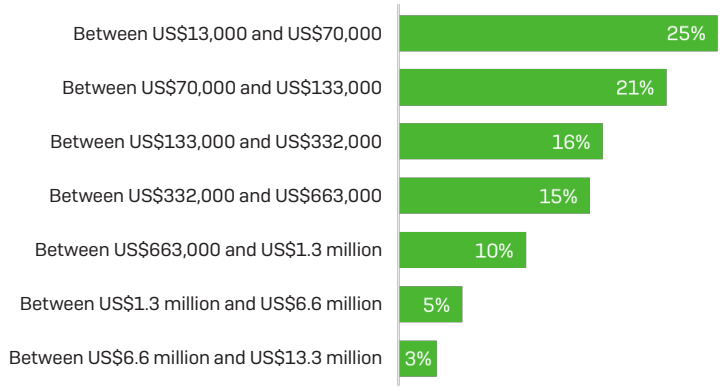
Fortunately, healthcare organizations are learning from experience and have chosen to invest in anti-ransomware technology after seeing the harm caused by earlier breaches.

The high cost of a ransomware attack

The cost of a ransomware attack extends way beyond any ransom paid. The survey revealed that the total financial impact of a ransomware attack – including downtime, work hours, device cost, network cost, lost opportunities, and ransom payment – was invariably many thousands of dollars, euros, yen, pounds, pesos, rand, or rupees.

The median cost of a ransomware attack is nearly US$133,000 (£100,000), almost evenly split between businesses that reported the cost at more than this amount (51%) or less (49%). The most common cost organizations experienced was between US$13,000 and $70,000, but nearly half of the respondents (46%) incurred costs between $13,000 and $133,000.

Approximate cost to the respondents' organization to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc....)



The survey has also revealed that **ransomware costs U.S. businesses more than the GDP of Jamaica.** Based on the survey results, we estimate that ransomware cost U.S. businesses of 100 or more people $18.6 billion in the last year. By comparison, the GDP of Jamaica was $14 billion in 2016.

The Sophos perspective

Despite a series of high-profile ransomware attacks in 2017, organizations are starting 2018 with inadequate protection against ransomware. Meanwhile, those that are implementing anti-ransomware technology will need to ensure that the option they chose has dedicated anti-ransomware capabilities rather than generic threat protection.

Sophos believes it's time for more independent, 3rd party testing of the efficacy of anti-ransomware products and their ability to stop previously unknown threats so that organizations and IT professionals can make informed decisions.

Lastly: we expect to see even more ransomware attacks in 2018, fuelled by Ransomware-as-a-Service (RaaS) and amplified by the resurgence of worms. Now is not the time to delay upgrading your technology. Add dedicated anti-ransomware protection before it's too late.

Sophos recommendations

No matter what, your organization is a target. You've got to be prepared. Small, medium, or large, all companies have been attacked by ransomware.

Start with knowledge. Make sure you educate yourself and your end users. Train your employees with attack simulations so they can identify an attack if they see one. End users – and human error – is so often the weakest link in your security, but well-trained users can be your strongest asset.

Investigate advanced technologies to know what your options are. Traditional antivirus or endpoint security will only block known ransomware, and with the speed new malware is developed and released, you need true anti-ransomware protection to block zero-day attacks.

Upgrade your technology. The options available have advanced significantly in recent years to stop ransomware and prevent the use or exploits. And remember, the cost of investing in defensive technology is nothing compared to the impact of an attack. You'll save money, and your reputation by being protected.

Stopping Exploits

Executive summary

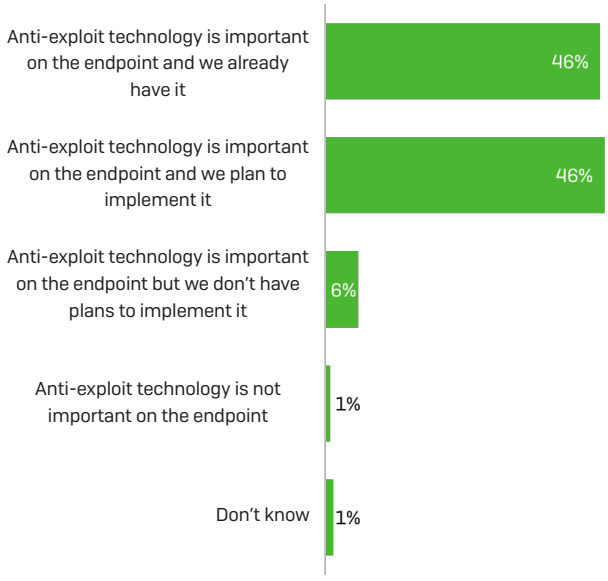
- 54% of organizations don't have anti-exploit technology in place
- 2/3 of IT managers don't understand what anti-exploit technology is
- U.S. has the greatest understanding of anti-exploit technology, followed by Mexico

Stop the exploit, stop the attack

Exploits, the techniques hackers use to take advantage of vulnerabilities in legitimate software, have been deployed in many high-profile attacks. The use of the Eternal Blue exploit in the WannaCry ransomware attack generated headlines around the globe. In light of this media coverage, it's unsurprising that almost all respondents (98%) agree that having anti-exploit technology on the endpoint is important. However, over half

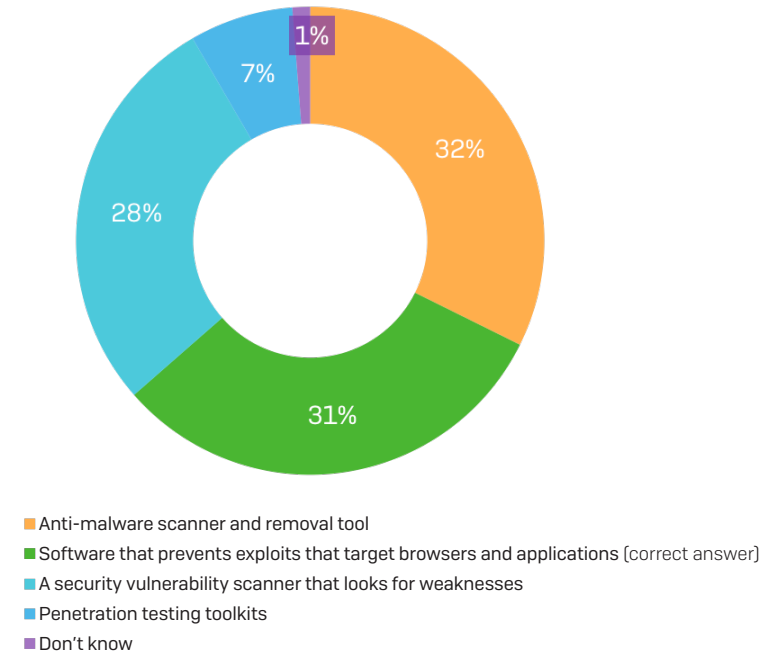
of organizations surveyed (54%) say they don't have anti-exploit technology on the endpoint in place, leaving them vulnerable to attack.

Respondents' views on incorporating specific anti-exploit technology into their organization's endpoint protection



Despite 46% saying they have anti-exploit tech in place, less than a third of respondents (31%) were able to correctly identify the definition of anti-exploit software. This suggests that a significant proportion of organizations have a misplaced belief that they are protected from this common attack technique, and are in fact at significant risk.

What is the best description for anti-exploit software



Level of understand varied from country to country, with the U.S. at the top of the list with 39% defining it correctly, compared to just 22% in France. Perhaps surprisingly, smaller organizations demonstrated a better understanding of anti-exploit technology than larger ones, with 34% of those in the 100-1,000 user band able to define it correctly compared with 29% in the 1,001-5,000 user group.

Correctly defined anti-exploit software

U.K.	France	Germany	U.S.	Canada	Mexico	India	Australia	Japan	South Africa
35%	22%	32%	39%	26%	35%	28%	34%	26%	30%

% of respondents who correctly identified the definition of anti-exploit software by country

Sophos recommendations

Given the widespread use of exploits in today's attacks and the significant lack of around anti-exploit technology, urgent action is needed to understand how to stop these threats. If you don't understand exploits, it's time to learn. If you think you understand exploits, it's worth refreshing your knowledge to make sure you're aware of the latest approaches.

The time is now to upgrade your technology. To protect against exploit techniques used in malware attacks make sure you have the security solutions in place to stop them.

Advanced Threats and Machine Learning

Executive summary

- 87% agree: threats have become more complex over the last year
- 60% say their current cyber defenses are not enough
- 60% plan to implement predictive threat technology like machine or deep learning within the next year
- Canada, India, and Mexico have the highest levels of machine learning technology
- India is most optimistic about the potential of machine learning

You are not alone

The survey confirmed that dealing with today's sophisticated malware attacks is a growing challenge for almost all IT managers, right across the globe:

- 83% agree that stopping malware threats has become harder over the last year
- 87% agree that malware threats have become increasingly complex over the last year

While these views are widely held in all geographies surveyed, IT managers in Japan are feeling the greatest change with 92% saying that stopping threats has got harder and 97% agreeing that they have become more complex.

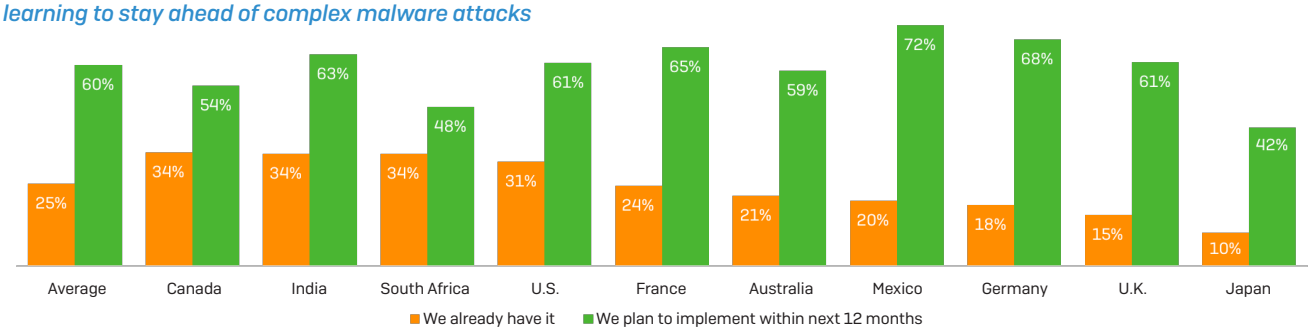
	Agree that stopping threats has gotten harder over the last year	Agree that malware threats have gotten more complex over the last year
UK	85%	89%
France	74%	79%
Germany	77%	87%
U.S.	88%	90%
Canada	76%	82%
Mexico	81%	86%
India	89%	88%
Australia	85%	84%
Japan	92%	97%
South Africa	85%	89%

Traditional endpoint technologies are often unable to keep up with today's complex, advanced attacks. A full 60% of respondents admitted that their current endpoint defenses are not totally sufficient to block the attacks they have seen in the last year. While responses were consistent across geographies and organization sizes, healthcare stood out as the sector with least confidence in their endpoint defenses with 72% agreeing they are not up to the job. Given the high propensity for healthcare organizations to suffer a ransomware attack, this is not surprising.

It's therefore no surprise that organizations are increasingly looking to predictive threat prevention technologies such as deep learning and machine learning to help them stay ahead of these malware threats. 85% of organizations already have (25%) or plan to implement predictive threat technology within a year (60%).

The survey revealed some significant variation in plans for predictive technologies across the globe. Canada, India, and South Africa lead the pack with one third (34%) of respondents already using predictive threat technologies such as deep and machine learning. Mexico has the most extensive plans for these technologies with 72% planning to implement them within the next year. Japan stands out as the country most cautious in approach to predictive technologies with just 10%, the lowest of all countries surveyed, already using them and 41% stating they have no plans to implement it.

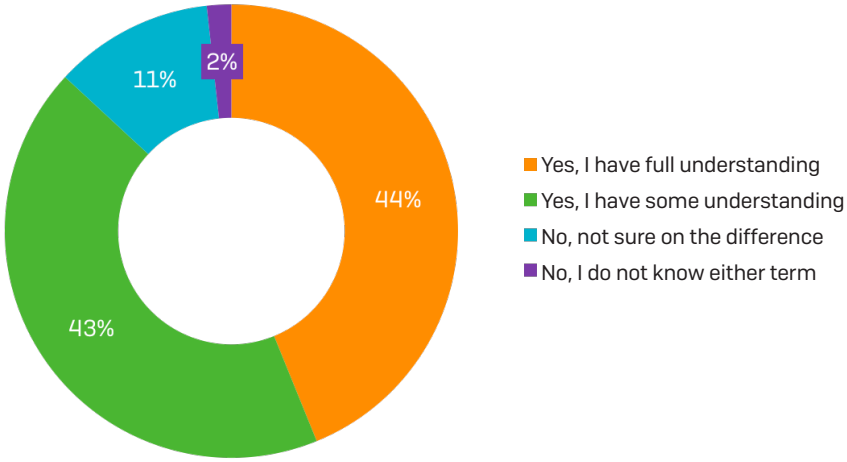
Respondents' views on incorporating predictive threat technologies such as machine and deep learning to stay ahead of complex malware attacks



Confusion around the difference between machine and deep learning

Although machine learning is a hot topic, nearly six in ten (56%) admit they do not have a full understanding of the difference between machine learning and deep learning. As a result, they are unable to fully evaluate the security options available to them.

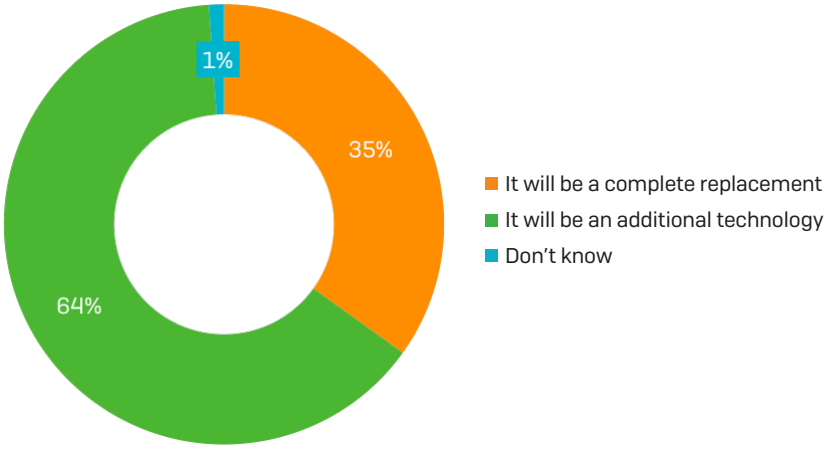
Question: Do you understand the difference between machine and deep learning?



Machine learning is the future

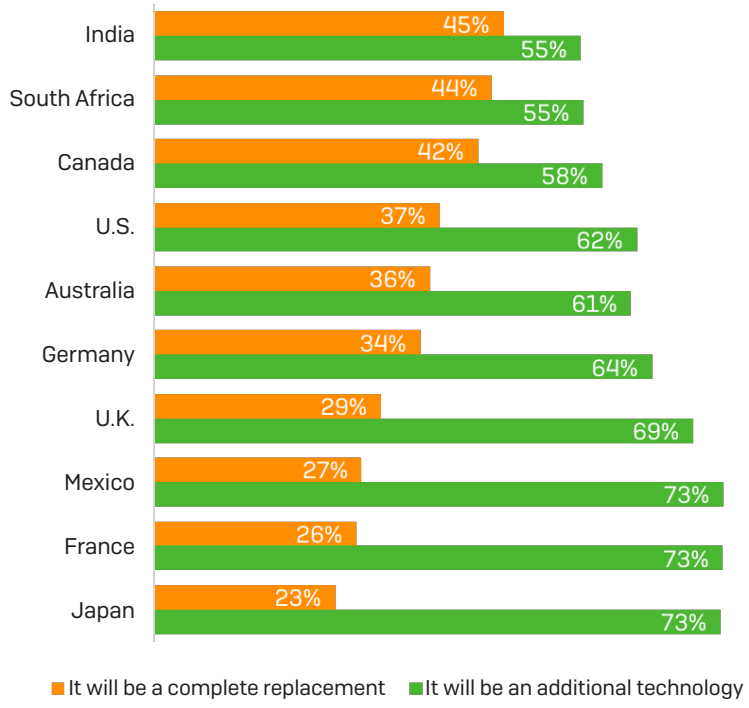
As we've seen, the vast majority of organizations surveyed either have or plan to implement predictive threat technologies like machine or deep learning. However, attitudes vary regarding where these products fit in their security infrastructure. For almost two-thirds (64 %) of organizations, machine and deep learning is considered an additional technology for their endpoints, compared to 35% who see it as a complete replacement for traditional endpoint protection.

Question: Does your organization see machine and deep learning as an additional detection technology for your endpoints or as a complete replacement for antivirus?



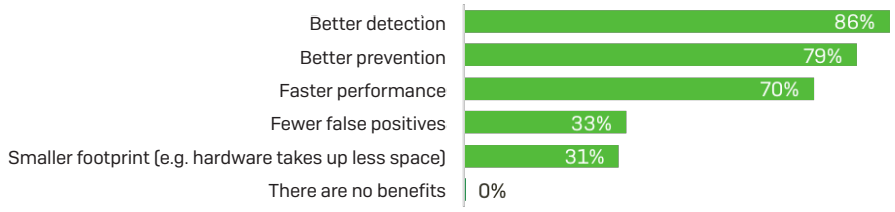
Indian organizations have the most confidence that it will be a complete replacement (45%), while, again, Japanese respondents showed most caution to this technology.

Question: Does your organization see machine and deep learning as an additional detection technology for your endpoints or as a complete replacement for antivirus?



The number one benefit organizations are looking for when it comes to machine and deep learning is better detection, with on average 86% of respondents anticipating this benefit.

Question: What are the most important benefits your organization is looking for when it comes to predictive threat prevention technologies provided through machine and deep learning?



They do, however, have some anxiety, with nearly two-thirds (65%) very or extremely concerned about false positives with this technology.

Despite this caution, overall attitudes towards machine learning are hugely positive: the majority (94%) of respondents believe that machine learning will "live up to the hype," with over two in ten (21%) going so far as to state that it will solve all of their technology issues.

	Average	U.K.	France	Germany	U.S.	Canada	Mexico	India	Australia	Japan	South Africa
Machine Learning will live up to the hype	94%	90%	96%	94%	97%	97%	98%	99%	89%	79%	93%
Machine Learning will solve all our technology issues	21%	13%	19%	10%	26%	20%	32%	45%	14%	9%	17%

Respondents' views on machine learning

While belief that machine learning will live up to the hype is widespread across survey respondents, on the question as to whether it is a panacea for our technology issues differ greatly. As noted above, IT managers in India are most optimistic with a full 45% saying it will solve all our technology issues. In contrast, just 9% of Japanese and 10% of German respondents shared this view.

The Sophos perspective

Machine learning is becoming mainstream. Despite being relatively new, the vast majority of organizations plan on implementing machine learning in the next 12 months. However, Sophos agrees with the majority of survey respondents: machine learning is an additional layer of security, not a total replacement for all endpoint protection.

As there is a lack of full understanding about the difference between machine learning and deep learning, the security industry needs to take the lead in enabling organizations to make informed decisions on machine and deep learning. This means independent, public testing of security products and available education on these technologies, how they're used, and the differences between them.

Sophos recommendations

Malware's not getting any simpler to defend against and cybercriminals area already using machine learning in their attacks. You need to make sure your defenses keep pace with the threats against you. The sooner everyone take on machine or deep learning protection the better.

The lack of education must be overcome – professionals need to avail themselves of educational opportunities and investigate machine and deep learning to get a better understanding of the differences between them, and what those differences mean in terms of security. Not all machine learning options are the same. Make sure you have the right protection for your organization.

Conclusion

This survey has revealed that IT security remains a highly challenging and complex area for organizations across the globe, fuelled by the ever-increasing complexity of malware attacks and the financial incentives for attackers.

The gap is growing between the knowledge and skills of the attackers, particularly around the areas of ransomware and exploits, and that of the IT professionals charged with stopping them. Although this creates an opportunity for cybercriminals, it can be addressed through education.

As the survey has shown, traditional security solutions are no longer enough to keep organizations ahead of today's complex threats. While there is a number of advanced technologies available, a lack of understanding of how they work makes it hard for organizations to evaluate them effectively and put in place the necessary protection.

Sophos calls on the security industry to make it easier for IT managers to understand and evaluate these technologies through increased open, independent testing and education.

Further Reading

- Exploits Intercepted – A very readable guide to what exploits are, how they work, and how to stop them
- Exploits Explained – A deep dive into the actual exploits used by hackers today and the protection capabilities that block them
- How to Stay Protected against Ransomware – How ransomware works and what steps you can take to protect against it
- Machine Learning for Cybersecurity Demystified – A collection of articles on machine learning
- Sophos Intercept X Deep Learning Datasheet – A clear explanation of deep learning and why it consistently outperforms other machine learning models

Introducing Sophos Intercept X

Sophos Intercept X is the world's most comprehensive next-gen endpoint protection. It uses multiple technologies, including deep learning, ransomware prevention, and anti-exploit capabilities to protect against ransomware and never –before-seen malware.

Intercept X runs along antivirus products from Sophos and other vendors, elevating protection against ransomware and advanced attacks. When used with Sophos Endpoint Protection it gives you the most complete endpoint protection available to stop both known and unseen threats.

Independent experts and customer testimonies confirm the effectiveness of Intercept X:

"Intercept X stopped every complex, advanced attack we threw at it." ESG Labs

"One of the best performance scores we have ever seen." AV-TEST

Security Innovation of the Year
Computing Security Awards 2017

"In the past 12 to 18 months, we have not experienced any serious incidents or outages. Intercept X is the best possible protection against ransomware and other internet threats."
Gus Garcia, Security and Information Officer, Diocese of Brooklyn

For more information and to start a free 30-day trial, visit www.sophos.com/interceptx.

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

North American 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

2-2-18 NA (GH)

SOPHOS