

SMOKE AND MIRRORS:

Do AI and Machine Learning Make a
Difference in Cybersecurity?

AI ML

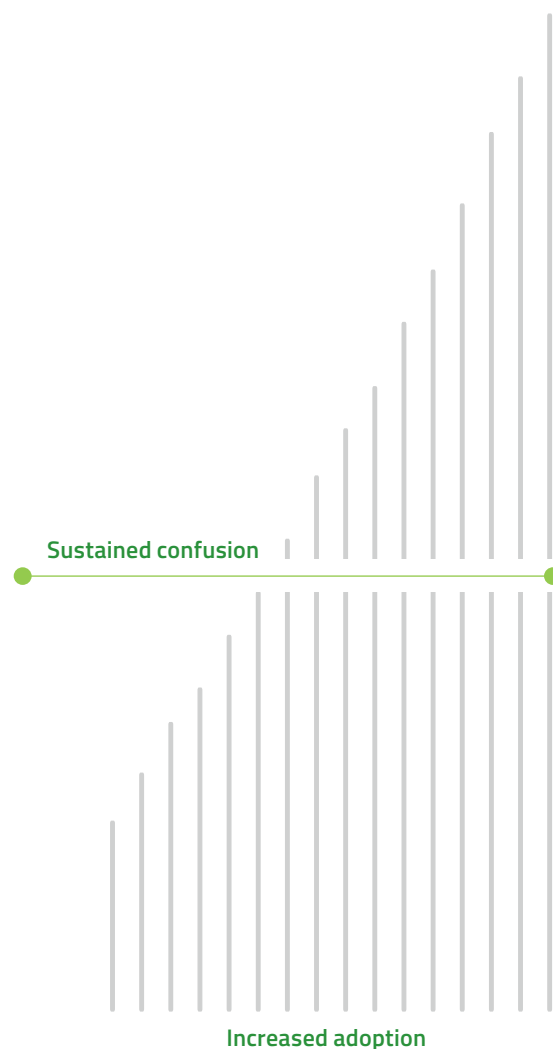
Perspectives from IT pros worldwide

Executive Summary

Over the last several years, the use of artificial intelligence (AI) and machine learning (ML) has maintained consistent growth among businesses. During our 2017 survey of IT decision makers in the United States and Japan, we discovered that approximately 74% of businesses in both regions were already using some form of AI or ML to protect their organizations from cyber threats.¹ When we checked in with both regions at the end of 2018, 73% of respondents we surveyed reported they planned to use even more AI/ML tools in the following year.² For this report, we surveyed 800 IT professionals with cybersecurity decision-making power across the US, UK, Japan, and Australia/New Zealand regions at the end of 2019, and discovered that 96% of respondents now use AI/ML tools in their cybersecurity programs.

Despite the increase in adoption rates for these technologies, more than half of IT decision makers admitted they do not fully understand the benefits of these tools. Overall, this report highlights continued themes of confusion and lack of knowledge regarding the use cases and capabilities of AI and machine learning-based cybersecurity tools, as well as a general distrust in their capabilities, based on how such tools are advertised by vendors.

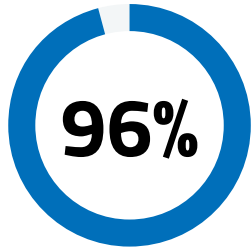
Ultimately, the results demonstrate that continued education, increased awareness, and overall standardization across the industry will help businesses around the world become more resilient against cyberattacks and other IT challenges.



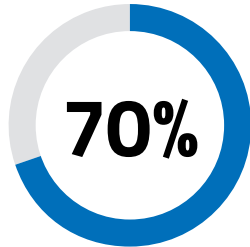
¹ Webroot. "Game Changers: AI and Machine Learning in Cybersecurity; a US/Japan Comparison." (December 2017)

² Webroot. "Knowledge Gaps: AI and Machine Learning in Cybersecurity." (January 2019)

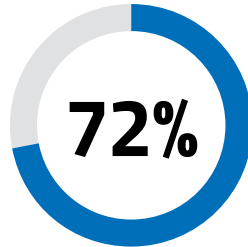
Global Findings



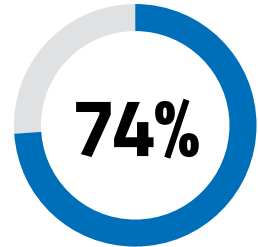
96% currently use cybersecurity products with AI/ML.



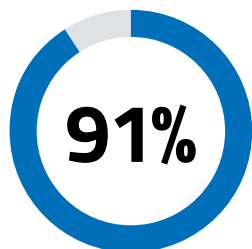
70% plan to use even more AI/ML-based cybersecurity tools in 2020.



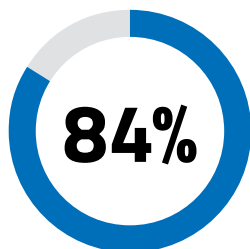
72% say it is very important that cybersecurity advertising mention the use of AI/ML.



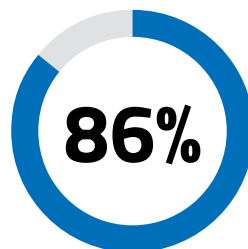
74% agree that, as long as their protection keeps them safe from cybercriminals, they do not care if it uses AI/ML.³



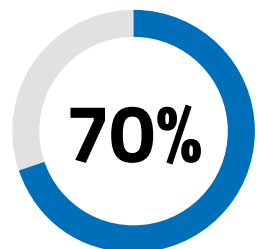
91% say they understand and research the security tools they use, and specifically look for those that use AI/ML.⁴



84% think their organization has everything it needs to successfully defend against AI/ML-based cyberattacks.



86% believe they could be doing more to prevent cyberattacks.



70% report their organization has experienced a damaging cyberattack in the last 12 months, despite having AI/ML-based tools in place.

³ 74% refers to 38% who agree and 36% who strongly agree with the statement "As long as the tools we use help protect us against cybercriminals and other cyber threats, I don't care if it uses AI/ML."

⁴ 91% refers to 42% who agree and 49% who strongly agree with the statement "I understand and research the cybersecurity tools we use and specifically look for ones that use AI/ML to protect my organization."

Regional Highlights

UNITED STATES

- Feel the most secure due to use of AI/machine learning in cybersecurity tools
- Most likely to work with vendors that use the most technologically advanced cybersecurity methods
- Most likely to research the cybersecurity tools they use and specifically look for ones that use AI/ML
- Most likely to say they are completely knowledgeable about the types of threats AI/ML-based solutions help them find
- Highest intended investment rate for cybersecurity (in general) 2020

UNITED KINGDOM

- Highest use of AI/machine learning in current cybersecurity tools
- Consider costs the largest factor when selecting cybersecurity tools
- Spend the largest portion of budget on tools that use AI/ML
- Most likely to work exclusively with vendors who have proven solutions
- Least likely to prioritize vendors who use the most technologically advanced cybersecurity methods
- Lowest intended investment rate for AI/ML-based cybersecurity in 2020

JAPAN

- Lowest current use of AI/machine learning in cybersecurity tools
- Spend the least amount of their budget on tools that use AI/ML
- Are generally likely to work with vendors that use the most technologically advanced methods to combat cyber threats
- Most likely to admit having experienced a damaging cyberattack in the last 12 months
- Highest intended investment rate in AI/ML-based cybersecurity for 2020

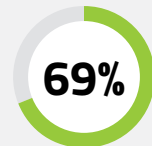
AUSTRALIA / NEW ZEALAND

- Consider costs the largest factor when selecting cybersecurity tools
- Most likely to want to fully understand a solution before adopting it
- Most likely to believe cybersecurity vendors are being intentionally deceptive in their AI/ML marketing
- Most likely to admit that, while some of their tools claim to use AI/ML, they are unsure what that means
- Most likely to invest in regulatory compliance for 2020

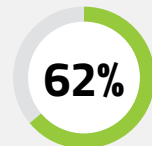
Current Outlook

AS CYBERATTACKS CONTINUE TO INCREASE IN PREVALENCE, MORE BUSINESSES ALL OVER THE WORLD ARE TURNING TO ADVANCED CYBERSECURITY TOOLS TO PROTECT THEMSELVES.

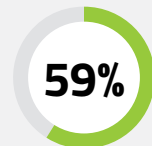
TOP 5 ROLES AI AND MACHINE LEARNING PLAY IN GLOBAL CYBERSECURITY PROGRAMS



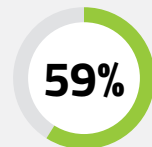
Threat alerts and detection



Automated network analysis



Pattern recognition



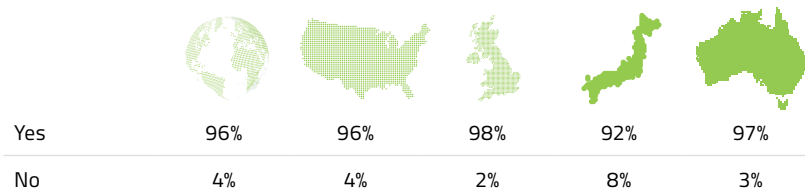
Email scanning



Threat hunting

A full 96% of global respondents across the US, UK, Japan, and Australia/New Zealand say they are already using AI/ML tools in their cybersecurity programs. Furthermore, they dedicate about half (51%) of their total cybersecurity spend specifically to products that use AI/ML, and 70% plan to use more of these types of tools in 2020.

FIGURE 1: Do you currently use products with artificial intelligence (AI) or machine learning (ML) capabilities in your cybersecurity program? *



* Note: due to rounding, some percentages may not add up to exactly 100%.

FIGURE 2: Approximately how much of your total cybersecurity spend goes toward tools that use AI/ML?

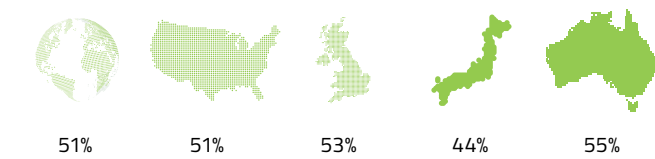












FIGURE 3: What role have AI/ML capabilities played in your company's cybersecurity program?

					
Threat alerts / detection	69%	81%	70%	61%	62%
Automated network analysis	62%	66%	61%	62%	61%
Pattern recognition	59%	63%	62%	57%	53%
Email scanning	59%	63%	58%	55%	61%
Threat hunting	58%	53%	58%	57%	62%
Employee awareness training	56%	57%	56%	51%	59%
User behavior modeling	54%	54%	58%	52%	53%
Decrease in response time	50%	44%	52%	48%	56%






Nearly seven in ten IT decision makers (69%) believe they spend enough to get all the tools needed to protect their company from cyber threats, while just under a third (29%) believe they could be spending more to achieve a stronger level of security.

FIGURE 4: How would you categorize your company's current spend on cybersecurity-related tools and services?

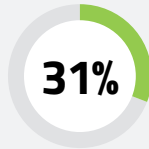
					
We spend enough to get all the tools needed to protect our company from cyber threats.	69%	69%	63%	68%	77%
We spend an adequate amount, but there is more we could spend to be more secure.	29%	30%	35%	30%	21%
We spend less than we should on cybersecurity-related tools.	2%	0%	3%	3%	2%

Interestingly, despite the widespread adoption and use of AI/ML-based security tools (and the beliefs most companies surveyed hold about the effectiveness of their spending and programs), nearly three-quarters (70%) of global respondents report they experienced a damaging cyberattack within the last 12 months!

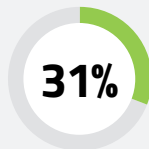
FIGURE 5: Has your organization experienced a damaging cybersecurity attack in the last 12 months, despite having cybersecurity tools in place that use AI/ML?

					
Yes	70%	46%	73%	81%	79%
No	30%	54%	27%	19%	21%

TOP 5 REASONS ORGANIZATIONS FAILED TO PREVENT CYBERATTACKS, ACCORDING TO GLOBAL RESPONDENTS



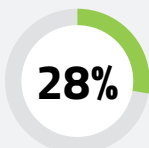
Lack of training



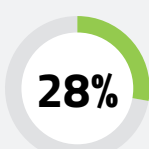
Cybersecurity vendor



Employee negligence




Struggle to keep up with the latest technology



Struggle to properly install/configure new technology

FIGURE 6: What do you think are the reason(s) that your company was unable to prevent the cybersecurity attack?



	Global	US	UK	Japan	Australia
Lack of training	31%	29%	23%	44%	28%
Cybersecurity vendor	31%	34%	29%	39%	25%
Employee negligence	30%	34%	32%	29%	29%
Struggle to keep up with the latest technology	28%	33%	28%	25%	27%
Struggle to properly install/configure new technology	28%	28%	27%	31%	25%
Lack of CISO/IT team	27%	26%	22%	29%	28%
Inexperienced team	26%	20%	24%	38%	20%
Hardware issue	26%	31%	23%	26%	25%
Personal device issues	23%	25%	22%	23%	24%
Budget	23%	16%	27%	20%	29%
Lack of tools	23%	22%	18%	28%	22%
Not having the correct tools	22%	19%	22%	30%	15%
Lack of support from leadership	20%	22%	18%	18%	23%

“

As criminals continue to find more new and innovative ways to attack businesses and home users, it's up to us as cybersecurity professionals to ensure we all understand the threats and the most efficient and effective methods to stop them. Realistically, we can't expect to stop sophisticated attacks if more than half of IT decision makers don't understand AI/ML-based cybersecurity tools. We need to do better. That means more training and more emphasis not only on our tools and their capabilities, but also on our teams' ability to use them to their best advantage.

– Hal Lonas, SVP and CTO, SMB and Consumer, OpenText

”

Confusion and the Part Vendors Play



DESPITE NEARLY ALL COMPANIES IN OUR GLOBAL SURVEY CLAIMING TO USE CYBERSECURITY TOOLS WITH AI/ML, THERE'S STILL A LOT OF CONFUSION.

Nearly seven out of ten (68%) IT decision makers worldwide agree that, although their tools claim to use AI/ML, they aren't sure what that means.⁵ Nearly three in five (59%) admit they are somewhat-to-very uncertain what capabilities they are getting out of their AI/ML-based cybersecurity tools.⁶

FIGURE 7: How much do you agree with this statement: 'I know some of our tools claim to use AI/machine learning, but I'm not sure what that means.'?

	World	US	UK	Japan	Australia
Strongly agree	35%	31%	33%	30%	45%
Agree	33%	23%	31%	35%	42%
Neither agree nor disagree	7%	5%	10%	11%	5%
Strongly disagree	23%	38%	26%	20%	7%

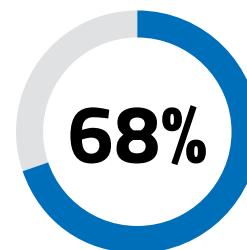


The hype around artificial intelligence has led to many myths. Enterprise architecture and technology innovation leaders implementing AI projects must separate reality from the myths to devise future strategies, or enhance existing ones, that will deliver business value outcomes.

— Gartner “Debunking Myths and Misconceptions About Artificial Intelligence,” Saniye Alaybeyi, et al 18 January 2019



On top of this confusion as to the benefits AI/ML cybersecurity tools may bring, a full 70% of respondents believe cybersecurity vendors' marketing is intentionally deceptive about their AI/machine learning-based services.⁷ And yet, a nearly equal number of respondents (72%) consider it very important, when selecting a new cybersecurity tool, that the vendor advertise its use of AI or ML. Why do so many people simultaneously hold these seemingly opposing views? More curious still: 77% of IT decision makers worldwide consider their organization more secure due to its use of AI/ML-based cybersecurity—even though close to the same percentage of respondents admitted they don't understand what AI/ML does for their organizations.



68% don't understand what AI/ML does for their organizations.

⁵ 68% refers to 33% who agree and 35% who strongly agree with the statement “I know some of our tools claim to use AI/ML, but I'm not sure what that means.”

⁶ 59% refers to 28% who agree and 31% who strongly agree with the statement “I'm not certain what capabilities I'm getting out of using of AI/ML-based cybersecurity tools.”

⁷ 70% refers to 33% who agree and 37% who strongly agree with the statement “I think cybersecurity tool vendors are being purposefully deceptive when it comes to how they market their AI/ML cybersecurity tools.”

FIGURE 8: How much do you agree with this statement: 'I think cybersecurity tool vendors are being purposefully deceptive when it comes to how they market their AI/ML cybersecurity tools.'

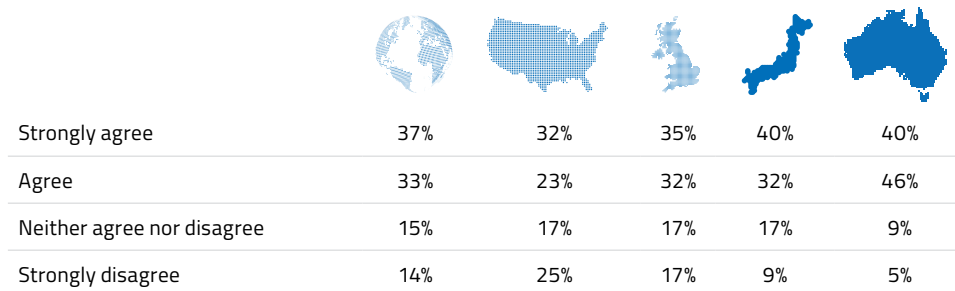


FIGURE 9: When selecting a new cybersecurity-related tool, how important is it that the manufacturer advertises its use of AI or machine learning applications to deliver its service?

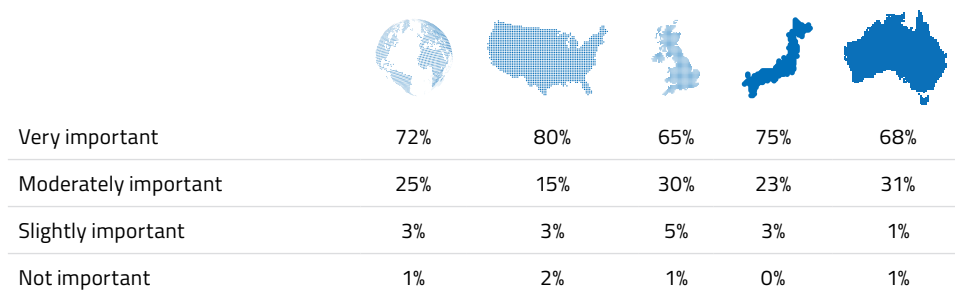
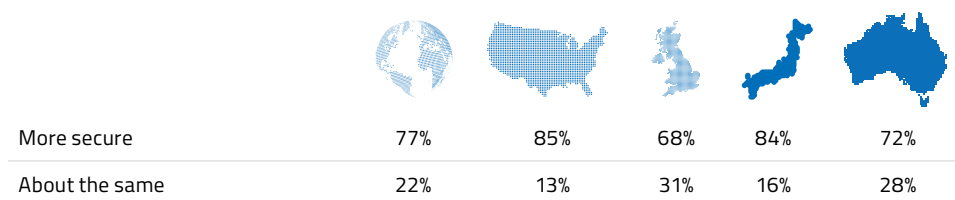


FIGURE 10: Do you think your organization is, or would be, more secure due to its use of AI and/or machine learning cybersecurity tools?



For yet another puzzle, we need only ask how many IT decision makers specifically look for AI/ML to protect their businesses. The answer is a full 91%.⁸ These same respondents also agree that they understand and research the tools they use. But 74% agree they don't really care if their tools use AI or machine learning, as long as those tools are effective in stopping cyberattacks.

⁸ 91% refers to 42% who agree and 49% who strongly agree with the statement "I understand and research the cybersecurity tools we use and specifically look for ones that use AI/ML to protect my organization."

FIGURE 11: How much do you agree with this statement: ‘I understand and research the cybersecurity tools we use and specifically look for ones that use AI/ML to protect my organization.’?

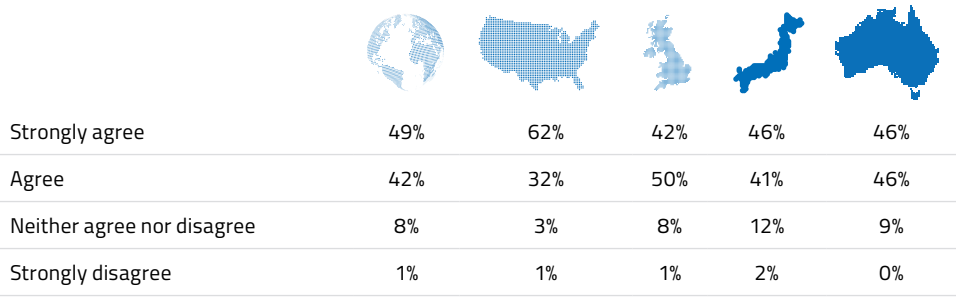
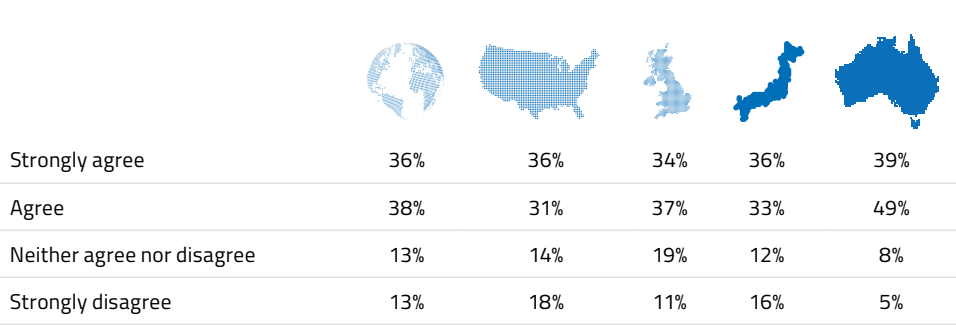
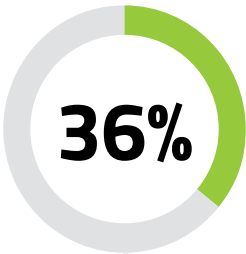


FIGURE 12: How much do you agree with this statement: ‘As long as the tools we use help protect us against cybercriminals and other cyber threats, I don’t care if it uses AI/ML.’?



The stark differences in these findings highlight IT decision makers’ desire to use whatever means are necessary to effectively protect their organizations, even if it means embracing technologies they don’t understand. Only 5% of those surveyed report feeling their teams need to fully understand a solution before the company will adopt it.

The Reality of the Threat Landscape



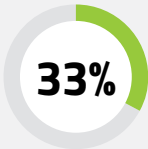
OVERALL, BARELY MORE THAN A THIRD (36%) OF IT DECISION MAKERS SAY THAT THEIR CURRENT TOOLS HELP STOP ALL OF THEIR CYBERSECURITY-RELATED THREATS.

Nearly nine out of ten (86%) of those surveyed are certain their company could be doing more to better defend against cybersecurity attacks. Fewer than two out of every five (39%) consider themselves completely knowledgeable about the types of threats that AI/ML-based tools help them find or combat.

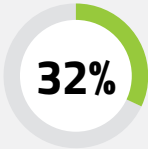
TOP 3 THINGS COMPANIES COULD DO TO BETTER DEFEND AGAINST ATTACKS, PER GLOBAL RESPONDENTS



Invest in AI/machine learning-based cybersecurity solutions



Security awareness training



Invest in new security software

FIGURE 13: Do you think there is more your company could be doing to better defend against cybersecurity attacks?






					
Yes	86%	78%	89%	89%	89%
No	11%	16%	10%	9%	11%
I don't know	3%	5%	1%	3%	1%

FIGURE 14: Are you and/or your organization knowledgeable about the types of threats that AI/ML-based threat intelligence solutions help you find/combat?











					
Completely knowledgeable	39%	47%	35%	43%	33%
Knowledgeable	46%	45%	52%	36%	49%
Somewhat knowledgeable	12%	5%	10%	19%	13%
Slightly knowledgeable	3%	2%	4%	2%	5%

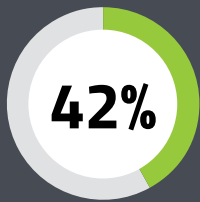
FIGURE 15: What could your company be doing better to defend against cyberattacks?

					
Invest in AI/ML-based cybersecurity solutions	38%	41%	36%	42%	32%
Security awareness training	33%	36%	33%	39%	24%
Invest in new security software	32%	38%	34%	28%	29%
Hire more IT staff	23%	22%	26%	21%	23%
Incentive-based learning	19%	15%	15%	20%	27%
Support from leadership	18%	13%	19%	14%	24%
Purchase new equipment	17%	16%	16%	19%	17%
Hire a CISO	15%	13%	16%	12%	17%



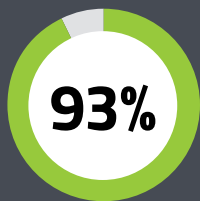
THE HUMAN ELEMENT

Ultimately, while many survey respondents aren't sure if AI/ML is benefiting their cybersecurity strategies, nearly half (42%) of global IT decision makers saw an increase in worker productivity.



SAW AN INCREASE IN WORKER PRODUCTIVITY

They also reported an increase in automated tasks (39%), an increase in effectiveness at their job/role (38%) and a decrease in human error (37%). And a full 93% of respondents worldwide agreed (50% agreed strongly) that the use of AI/ML makes them feel more confident in performing their roles as cybersecurity professionals.



AGREED THAT THE USE OF AI/ML MAKES THEM FEEL MORE CONFIDENT IN THEIR IT ROLES

In contrast, eighty-four percent of global respondents say their organization has everything it needs to successfully defend against AI/machine learning-based cybersecurity attacks. This highlights a level of over-confidence in companies' ability to thwart cybersecurity attacks, and in the protocols they currently have in place.

FIGURE 16: Do you think your organization has everything it needs to successfully defend against AI/ML-led cybersecurity attacks?

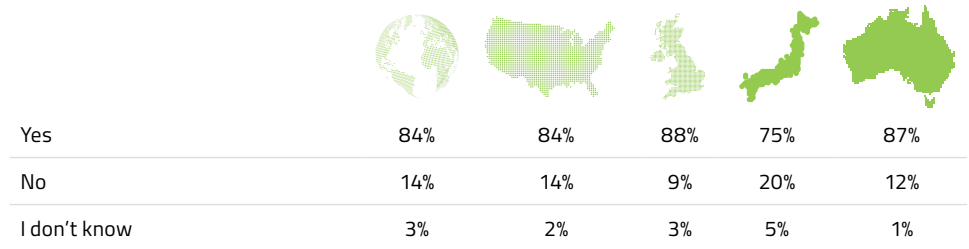


FIGURE 17: How much do you agree with this statement: 'The use of AI/ML makes me feel more confident in performing my role as a cybersecurity professional.'?

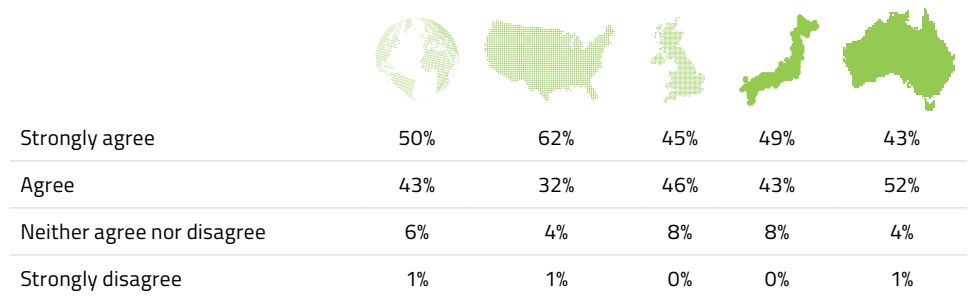
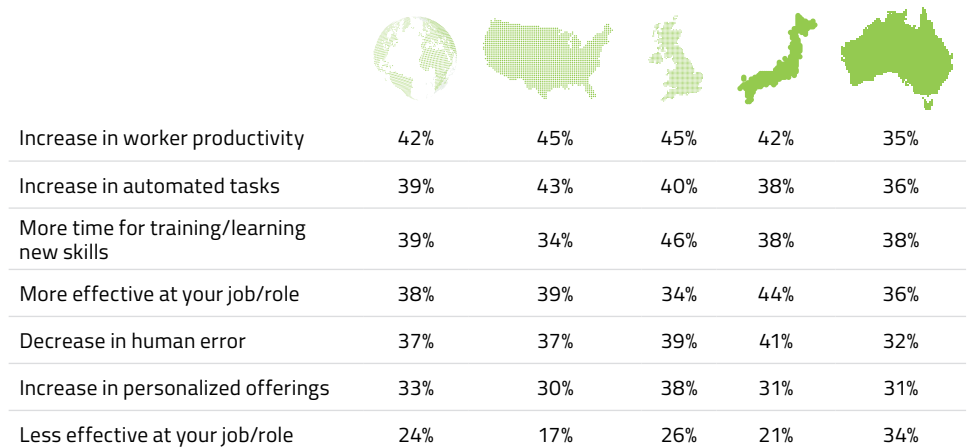


FIGURE 18: Has your company experienced any of the following after implementing AI/ML capabilities? Check all that apply.



Despite these clear indicators of the value AI/ML can bring, many IT professionals around the world expressed concerns that such technologies would render human security analysts obsolete. Globally, 42% of respondents said they believe human security analysts will be completely eliminated by an increase in AI/ML, and an additional 40% expect human security analysts to be partially eliminated. In contrast, when asked if AI/ML technology would create more new roles in the workforce than it would eliminate, only 5% considered this technology a threat to the workforce. These findings indicate that the majority of IT decision makers are unsure of the impact AI will have on security-related jobs.

FIGURE 19: Which statement most closely resembles your personal viewpoint on the role of AI/ML in the current workforce environment?

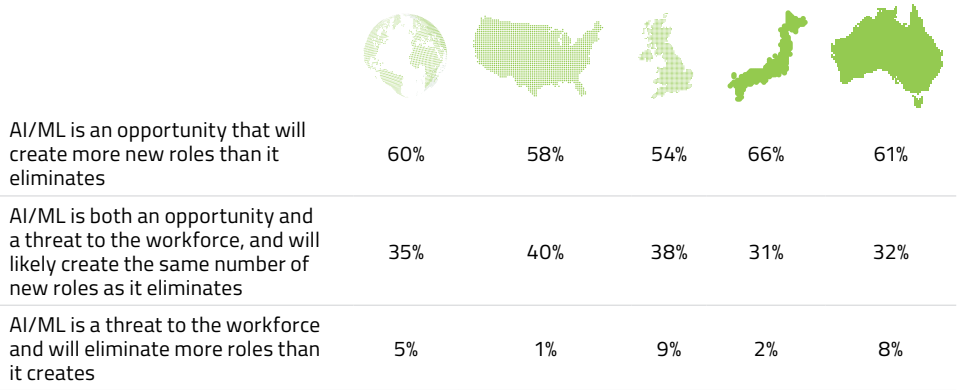
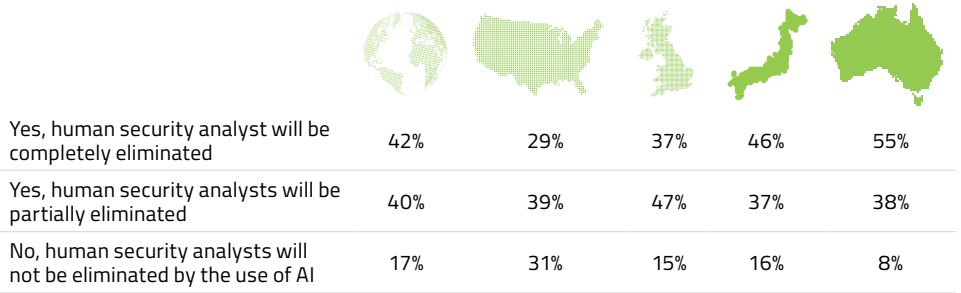


FIGURE 20: Do you believe that the use of AI will eventually reduce or eliminate the need for human security analysts?



"A key benefit of AI is making your workforce more efficient. Machines never get tired or need rest; they work 24x7. They can identify patterns in massive amounts of data or alert streams to help security analysts and IT security professionals predict new emergent behaviors, which helps security itself become more proactive."

— Cathy Yang
Product Manager, Threat Intelligence



THE REALITY

While there are approximately 2.8 million professionals currently working in the cybersecurity field, a recent study determined an additional 4 million trained workers would be needed to close the skills gap.⁹ AI/ML is a very effective method of augmenting human knowledge and decision-making, but it does not negate the need for the human expert in the first place.

⁹ (ISC)2. "2019 (ISC)² Cybersecurity Workforce Study." (November 2019)

Looking to the Future

A STRONG MAJORITY OF IT DECISION MAKERS CONSIDER THE USE OF AI AND MACHINE LEARNING TO BE ESSENTIAL TO ADDRESSING CURRENT AND FUTURE SECURITY THREATS.



FIGURE 21: Does your organization plan to use more or fewer AI/ML cybersecurity tools in 2020?

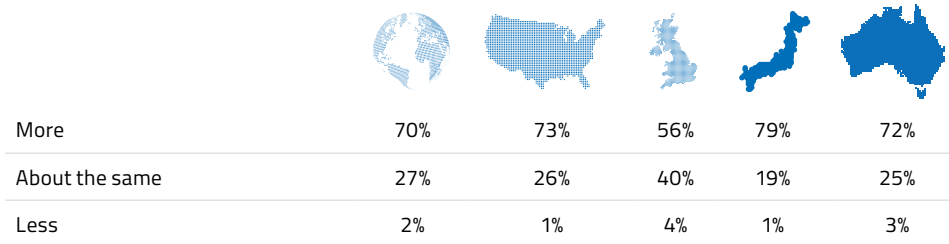
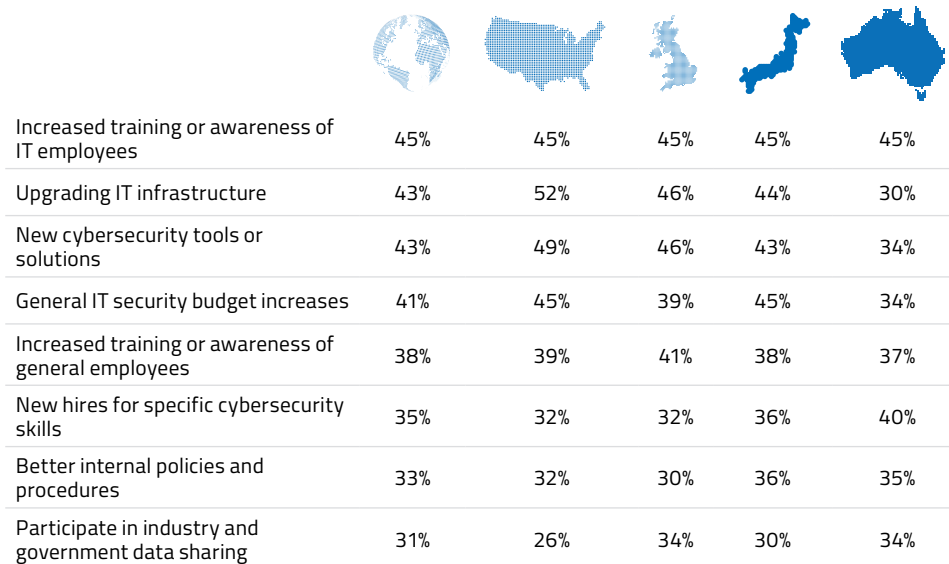


FIGURE 22: What are some areas that your organization needs to focus on to successfully defend against AI/ML led cybersecurity attacks?



TOP 5 AREAS ORGANIZATIONS SHOULD FOCUS ON TO STOP AI/ML-LED CYBERATTACKS, PER GLOBAL RESPONDENTS

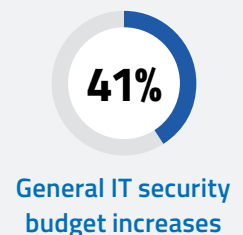
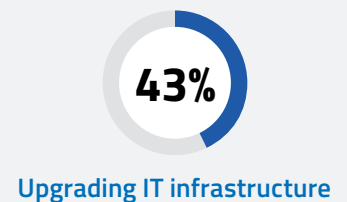
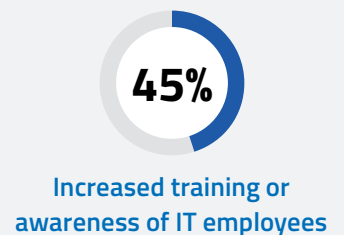
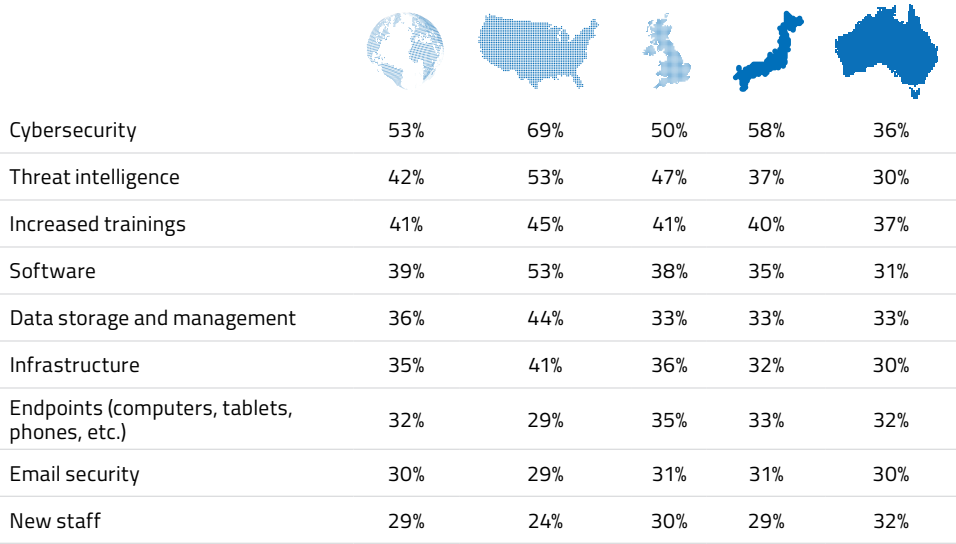
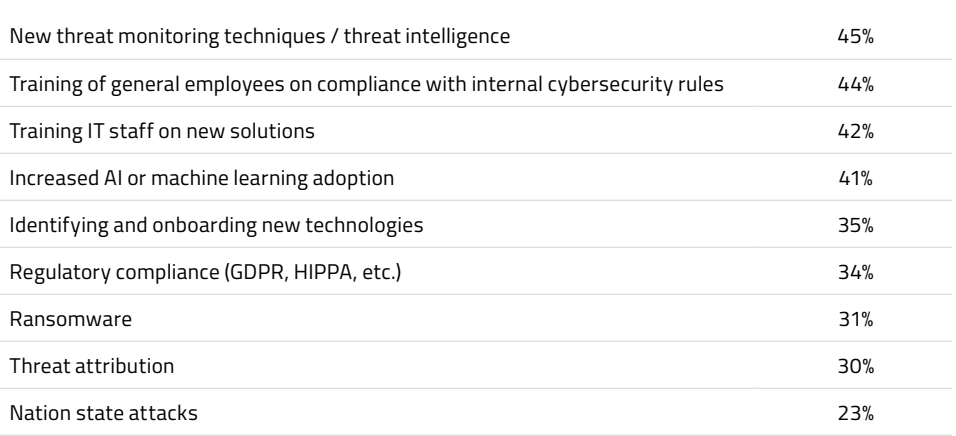


FIGURE 23: In what IT areas does your organization plan to increase investment 2020?



Additionally, when asked which cybersecurity-related areas they specifically planned to focus on in 2020, some of the most notable were new threat monitoring techniques/threat intelligence, better training, and increased AI or machine learning adoption.

FIGURE 24: Thinking about your organization’s cybersecurity plans for 2020, what are the biggest areas you plan to focus on?



**TOP 5 AREAS
RESPONDENTS PLAN TO
INCREASE INVESTMENT**



Overall, the need for increased training and upgrades to cybersecurity and infrastructure were consistently underscored.

Conclusion

It's clear from these findings that there is still a lot of confusion around artificial intelligence and machine learning, especially in terms of these technologies' in business cybersecurity. In spite of a small amount of regional variance, the overall results of this survey indicated a relatively even amount of skepticism across all geographies, with respect to how much benefit AI/ML brings. This uncertainty highlights a lack of knowledge regarding the use cases and capabilities of AI/ML in organizations' cybersecurity programs, which may be heightened by the need to keep up with the latest technology. Even more poignant is that nearly three quarters (74%) of IT decision makers worldwide really don't care whether they're using AI or ML, as long as the tools they use are effective in preventing attacks.

Overall, as IT decision makers become more knowledgeable about what works best for their organization, investment in these capabilities will begin to pay off, leaving organizations more resilient in the face of evolving cyberattacks and business needs.

With the majority of respondents planning to continue to increase spending on AI/ML technologies in 2020, it'll be crucial that they improve their understanding in order to realize maximum value. By vetting and partnering with cybersecurity vendors who have long-standing experience using and developing AI/ML, and who can provide expert guidance, we expect businesses will be more likely to achieve the highest levels of cyber resilience and efficiency possible, and to effectively maximize the capabilities of the human analysts on their teams.



As organizations continue to more frequently incorporate AI into their business practices, they need to ensure they know all the AI offerings available and choose based on what would best serve their needs. Not all AI is created equal.

— Krishna Roy, Senior Analyst, 451 Research



Methodology

This survey was conducted by LEWIS between November 15 and December 3 and consisted of an online questionnaire of 38 questions total, requiring approximately 8 minutes or fewer to complete. Survey responses were received from 800 full-time IT professionals at the IT Director level and above; approximately 200 were from each geography (US, UK, Japan, and ANZ). Respondents represented organizations that had 1000 or more employees, and all had decision-making authority for cybersecurity software purchases at their organization.

About Webroot

Webroot, an OpenText company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at [webroot.com](https://www.webroot.com).

385 Interlocken Crescent Suite 800

Broomfield, Colorado

800.870.8102

[webroot.com](https://www.webroot.com)