AI and automation for cybersecurity

How leaders succeed by uniting technology and talent

IBM

How IBM can help

IBM Security applies AI technologies such as machine learning and natural language processing to help security operations analysts stay ahead of threats while reducing response times and costs. For more information, please visit: ibm.com/security/artificial-intelligence.

Key takeaways

By offloading routine tasks, AI plus automation enables cybersecurity teams to use scarce human expertise where it is needed most.

The pace and volume of security incidents demand a new operational approach

AI plus automation increases visibility and productivity across security operations. Leading AI Adopters are monitoring 95% of network communications and cutting time to detect incidents by a third.

AI for security is gaining traction

Executives report widespread adoption of AI for security operations, with 93% either already using or considering implementation.

Leaders in security AI adoption are improving key cost performance measures

Top performers increased their return on security investment (ROSI) by 40% or more and reduced data breach costs by at least 18%, helping to free funding that can be reinvested in their cybersecurity workforces.

Rapid change elevates cyber risk

Modern digital operations are driving value yet also creating new vulnerabilities.

Cybersecurity threats surged in 2021, with Colonial Pipeline and several water treatment facilities in the United States among the targets whose systems were attacked.[1] One recent study reported ransomware increased 105% from 2020 to 2021, with manufacturing becoming the most targeted industry.[2] The past year has also seen some of the most impactful supply chain attacks to date. From the SolarWinds and Microsoft Exchange Server exploits to Apache Log4j vulnerabilities, high-profile attacks filled news feeds, raising awareness—and alarm—among business leaders and their customers.[3]

What makes today's situation categorically different from the past?

In brief, the pandemic accelerated digital transformation, amplifying both opportunities and risks.[4] Now there are substantially more remote workers. More cloud users. More cloud services. Essential systems integrations with third-party partners. An astounding number of edge devices passing IoT data to the cloud. All interconnected and interdependent, delivering sophisticated connectivity and creating value at speeds and scales impossible just a few years ago.

But the benefits of innovation also come with a cost: new devices, new partners, and new integrations open the organization in ways that can radically increase its overall attack surface. More threat vectors have emerged—from an unwitting supplier to a disgruntled employee, from exfiltration of data to denial of service to ransomware. And to complicate matters further, threat actors are evolving their own tactics, techniques, and procedures—using artificial intelligence (AI) and automation to probe for weaknesses and unleash more efficient attacks (see Figure 1).[5]

The net result is a stark realization for many executives: today's "always-on" digital operations are driving value but also creating new vulnerabilities. For all the efficiencies enabled by advanced technology services, many organizations are slowly realizing their digital footprints are replete with complexities and unknowns. Adding to the dynamics, short-handed security teams are overwhelmed with too much data from disparate sources, an abundance of tools, yet often a scarcity of insights. These challenges can easily exceed the skills of even the most knowledgeable security experts and the capacity of the largest, most talented cybersecurity operations teams.

Current operational reality demands a new approach

To position their teams for success, cybersecurity leaders must assume a more preventive and proactive posture for protecting core business operations. Our research suggests more organizations are opting for a forward-looking approach to threat management, adopting AI-powered automation to drive improved insights, productivity, and economies of scale.

AI technologies can transform security in four key ways:

- Machine learning capabilities help identify patterns, take inventory of new assets and services, and refine the performance of AI models.
- Reasoning capabilities help inform data analysis, enhance scenario modeling, and anticipate new attack vectors.
- Natural language processing can be used to mine text data sources, improve threat intelligence, and enrich knowledge resources.
- Automation can help orchestrate time-intensive tasks, improve response times, and reduce the burden for human analysts.

Taken together, these capabilities have the potential to transform security operations.

In this report, we show how this combination of AI and automation can deliver substantially better performance, whether in the form of speed, insights, or flexibility. These performance improvements enable cybersecurity teams to shift their focus to what really matters: proactively protecting against, detecting, responding to, and recovering from threats while reducing costs and complexity.

FIGURE 1

Security disruptors

Security operations teams are facing new challenges

- New and expanding attack vectors
- Attackers are shifting to adaptive, multi-variant threats
- Attackers are shifting to automation
- Cyber skills gap and capacity constraints
- Lack of visibility and coordination with third-party providers
- Lack of insights across data types–metadata, contextual, behavioral
- Information overload from disparate data sources and tools

Chapter 1

AI for security rapidly gains traction

To understand how AI is being used to support security operations and to quantify its impact on cybersecurity performance, the IBM Institute for Business Value (IBV) partnered with APQC (American Productivity and Quality Center) to survey 1,000 executives with overall responsibility for their organization's IT and operational technology (OT) cybersecurity. They represent 16 industries and 5 global regions (see Study and research methodology on page 32).

We asked respondents to provide information about the performance of their organization's security function and the extent to which they are applying AI and automation to manage cyber risk and compliance. They also described how they are using AI to support security operations for protection and prevention as well as detection and response processes. We used these insights to assess the impact of AI on cybersecurity performance, with an emphasis on productivity, resilience, and associated business benefits.

Overall, we found the majority of companies—globally and across industries—are adopting or are considering adoption of AI plus automation in their security functions. 64% of respondents have implemented AI for security capabilities in at least one of the security lifecycle processes, and 29% are considering it. In other words, AI for security may soon become a near universal capability (see Figure 2). The remaining 7% who are not considering use of AI plus automation for security place themselves in a precarious position, where they most likely will struggle to keep pace with the increasing speed and volume of security events.

FIGURE 2

Widespread adoption

Only a small group is not considering use of AI in security operations

We refer to the 64% who are currently piloting, implementing, operating, or optimizing AI security solutions as the "AI Adopters." While their application of AI for security is still nascent—most have been using it for less than 2 years in a business-as-usual environment—the uptake is expected to be rapid. When considering their specific uses of AI, the percentage of AI Adopters leveraging AI to support protection and prevention will grow by approximately 40%, on average, in the next three years, with the same growth expected across detection and response.

This expected accelerated adoption of AI for security is consistent with findings from other research. One recent study predicts cybersecurity-related AI spending will increase at a compound annual growth rate of 24% through 2027 to reach a market value of $46 billion.[6]

Technology plus talent yields positive results

AI Adopters recognize how AI-driven insights and AI-powered automation complement the expert-level identification and response capabilities of their security subject matter experts. They see that like a skilled security analyst, security AI systems are adept at identifying abnormal behaviors, assessing vulnerabilities dynamically, and flagging anomalous activity that can indicate new threats. 65% of Adopters report that this application of AI has had a significant positive impact on their security operations (see Figure 3 on page 7). But unlike a human analyst, security AI uses machine learning and automation to match the relentless speed and scale of hybrid multicloud operations—with a level of consistency and depth far beyond the capabilities of even the most capable, most qualified security professional. (See Perspective "What makes security AI so effective?")

For example, AI is being used to track normal behaviors and automate model building. To do this, AI security solutions flag variances from expected behaviors and analyze the threat implications of exception paths. Augmenting threat response to automate containment and optimize business continuity is cited as highly impactful by 57% of Adopters. By understanding anomalous activity in context, AI security solutions can determine which security policies and controls are at risk, supplement an alert with relevant insights, then initiate prescribed remediation actions.

This way of working as a "cyber assistant" for human experts underscores one of the most vital benefits of security AI: relieving pressure on security teams facing ongoing shortfalls in skills and resources. 60% of AI Adopters report that automated data enrichment and second-screen capabilities that help analysts operate more efficiently have been extremely beneficial for their security functions. Because AI threat models reference far more events over longer time horizons and across a variety of operating conditions, they can bring expert capabilities to bear on threats that may elude human analysts.

Enriched by AI-generated insights, AI-driven automation capabilities can isolate threats by user, device, or location, then initiate appropriate notification and escalation measures while human experts determine how best to investigate and remediate. For organizations that have developed these capabilities, cybersecurity analysts can shift their focus to what really matters: developing the skills and expertise to address more complex problems that require human judgement.

Perspective

What makes security AI so effective?

Security AI and automation are rapidly becoming essential to defending an expanding attack surface and responding to the huge increase in security events. What makes AI so effective? In short, it's the combination of iterative machine learning and analytical model tuning.

Tuning is the process of optimizing an analytical model's performance without making it overly reliant on variables that are likely to change from one situation to the next. Behind the scenes, machine learning algorithms use countless examples to identify patterns and learn how best to respond to different variables. This training process is key to improving how the AI model performs.

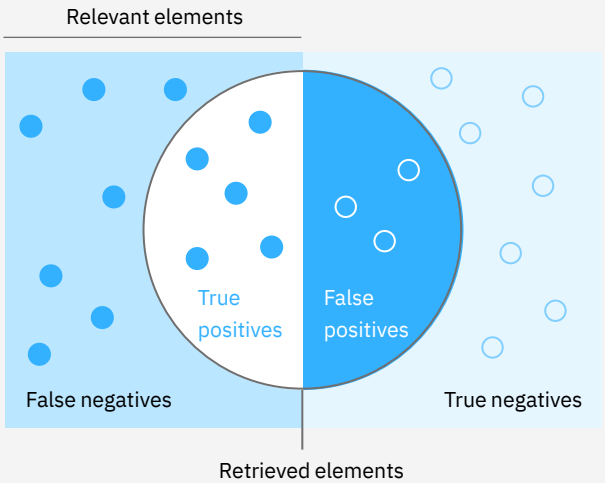
Improving model precision and recall through machine learning, AI security solutions can help reduce alert fatigue for analysts by distinguishing actual security threats—true positives—from ordinary events—false positives and true negatives (see Figure). These solutions help triage the majority of security events, enrich those events with contextual data insights, then support analyst inspection and investigation activities. By using AI to improve the signal-to-noise ratio, analysts can spend their time focusing on actual threats that pose the greatest risk.

How many retrieved items are relevant?

Precision = 

How many relevant items are retrieved?

Recall = 



Source: Adapted from https://en.wikipedia.org/wiki/F-score

AI plus automation ultimately creates more enriching work environments by allowing analysts to refocus on complex problems that require human judgement.

Because AI can analyze both unstructured and structured data sources—synthesizing internal and external data with threat intelligence services and open source intelligence (OSINT)—it can provide a comprehensive portrait of situational variables and threats in context. For cybersecurity analysts, this reduces the time to detect, respond to, and recover from incidents.

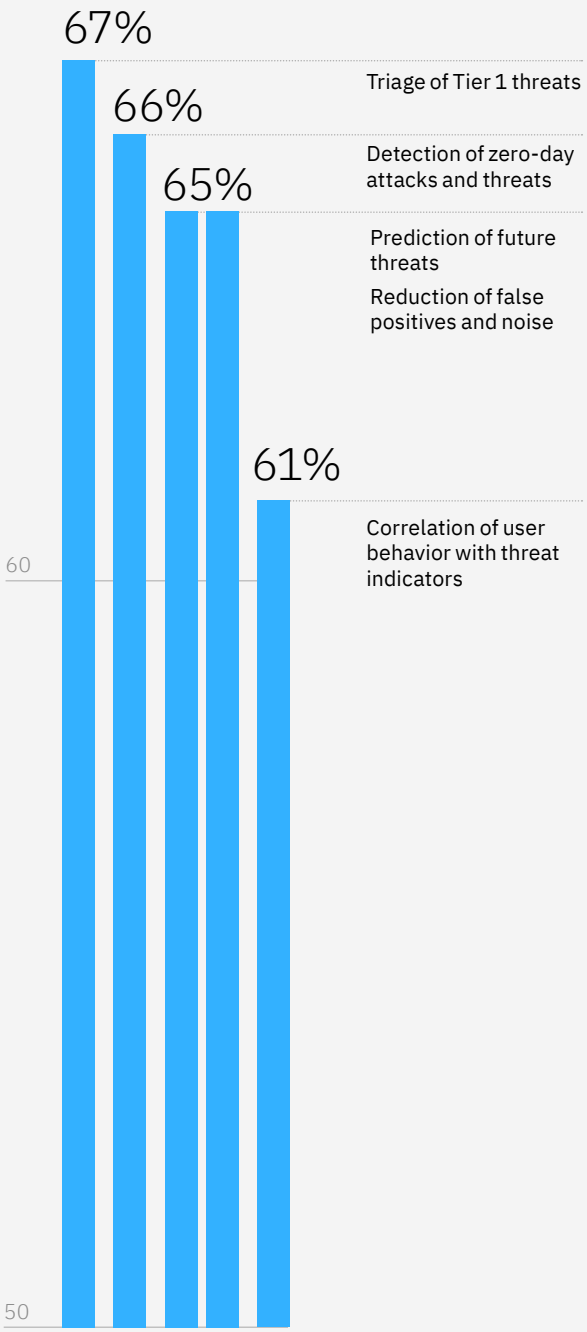
By facilitating more efficient escalation, review, and remediation procedures, AI enhances security governance and compliance. By automating repeatable, time-intensive tasks, AI can mitigate fatigue and help improve the analyst's ability to make better, more informed decisions—faster and with fewer errors. And by routing the sheer volume of events through security AI plus automation solutions, leaders make the most of skilled human analysts and their hard-to-find skills. The end result is a more enriching, more satisfying work environment—something that can make a real difference in attracting and retaining hard-to-find cybersecurity talent.

AI Adopters who have successfully coupled AI insights and automation with the expertise of their employees cite additional beneficial impacts of AI applications on their security outcomes (see Figure 3). 67% report that the ability to triage Tier 1 threats more effectively is helping to eliminate the costs and time associated with basic detection. Another 65% say that reducing false positives and noise has reduced the need for human analyst inspection. And 65% state that use of behavioral analytics is supporting prediction of future threats, an important step in becoming more proactive.

FIGURE 3

AI advantage

AI Adopters improve performance by using AI solutions for critical capabilities



Q: Which of the following AI applications has had the greatest impact on your security operations (select the top 5)?

AI investments pay off

One source estimates that by 2025, cybercrime will cost the world economy an average of $10.5 trillion every year.[7] In 2021, according to the annual Ponemon Institute and IBM Cost of a Data Breach report, the average cost of a data breach reached an all-time high, while the number of data breaches jumped an alarming 68%, magnifying those costs.[8]

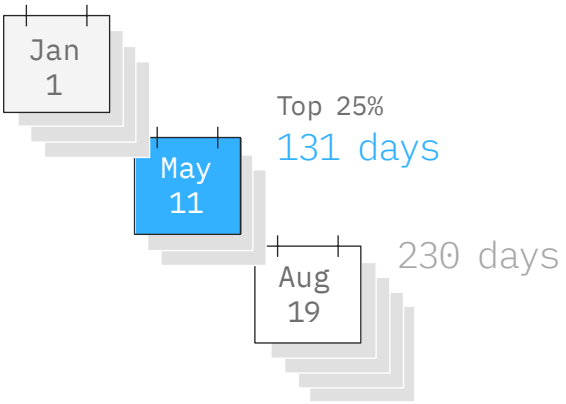
The results of our research reveal that initial AI investments across the security lifecycle are helping organizations more efficiently combat cybercrime, as reflected by security cost performance measures. In fact, the top 25% of Adopters—those that perform in the 75th or 25th percentile on each metric—credit AI plus automation with significant improvements in 3 key performance metrics, resulting in a fundamental improvement in the performance and effectiveness of their security functions. (For more information about top performer measurements, see Study and research methodology on page 32.) They have:

- Reduced their total cybersecurity costs by at least 15%, indicating efficiency and productivity gains across security lifecycle processes for protection and prevention as well as detection and response
- Reduced data breach costs by at least 18%, indicating an improvement in the efficiency of their detection and response processes. This is reflected in a reduction—or avoidance—of associated operational and reputational costs, including potential lost business (customers and suppliers), investment, and future business opportunities
- Improved their return on security investment (ROSI) by 40% or more, indicating a reduction in and avoidance of cyber risk and the associated operational and reputational costs.

Our research is consistent with other studies that have found AI delivers similar benefits. The Ponemon Institute and IBM reported that the combination of AI and automation was found to be the single greatest factor in reducing the overall costs of a data breach.[9] Similarly, an IBV study on zero trust security found that 61% of leading organizations used security automation and orchestration to reduce security capital and operational costs.[10]

These results offer compelling evidence for why security leaders are embracing AI and automation across the security lifecycle. Next, we'll explore how leaders are driving performance across two critical areas: protection and prevention and detection and response.

If an organization takes 230 calendar days to detect, respond to, and recover from cyber incidents without the use of AI, it could cut that time by up to 99 days by applying AI.



Chapter 2

AI drives performance across the security lifecycle

Along with the shared responsibility model inherent in cloud security and the IT integration inherent in a zero trust approach, AI plus automation represents a fundamantal capability for security operations going forward.

Security AI plus automation can generate meaningful insights enriched by context and historical data, then facilitate greater coordination and collaboration with partners inside and outside the organization. This frees skilled resources to investigate threats before they have a chance to mature. By improving performance across both protection and prevention and detection and response processes, AI plus automation can have a significant impact on the organization's overall cyber resilience.

To better understand this influence, we examined how Adopters are using AI and automation across the security operations lifecycle, in both their protection and prevention as well as detection and response processes. These insights helped us assess how the combination of these technologies is driving greater operational efficiency and effectiveness. They also helped us explain how improved performance can deliver downstream business benefits, such as greater productivity and a better employee experience.

By improving operations performance, AI plus automation helps strengthen overall cyber resilience.

Protect and prevent: Using AI to mitigate risk, control costs, and build trust

The challenges

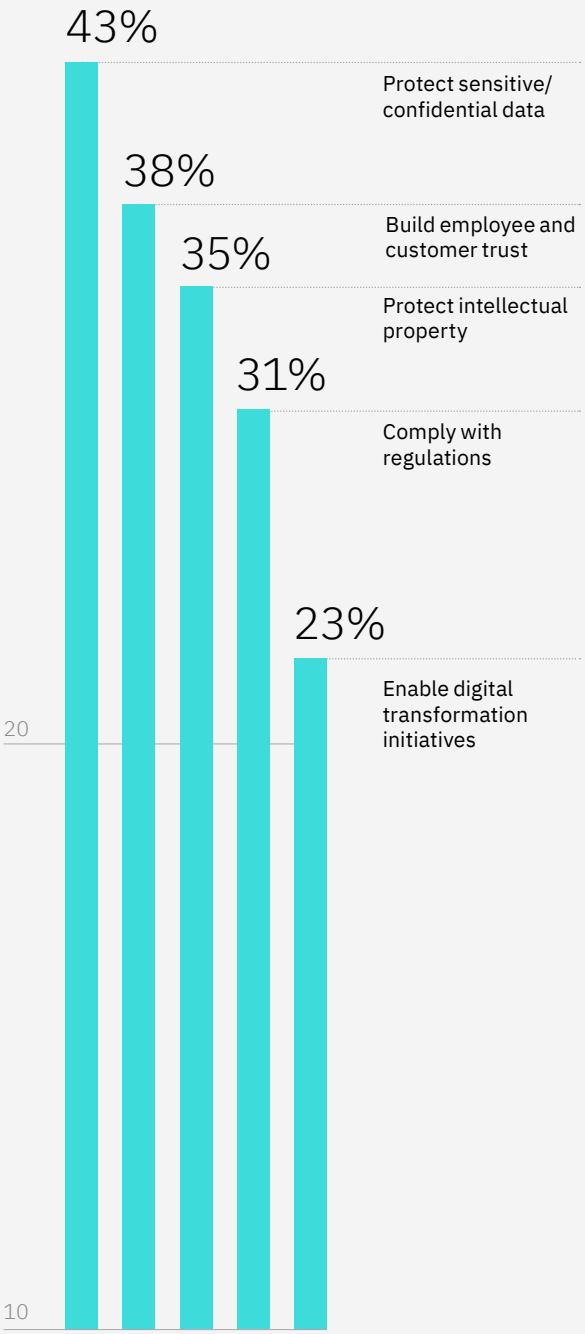
As the number of remote workers and cloud-based applications and servers has expanded in recent years, so has the number of endpoints and applications that must be monitored. Cybercriminals are exploiting connected services to create new threat vectors, with attacks evolving from opportunistic phishing to coordinated ransomware campaigns—where a business is essentially held hostage until it pays. Ransomware ranked as the top attack type observed by IBM X-Force® in 2021, while phishing operations were the top pathway to compromise—occurring in 41% of attacks.[11]

This increasing sophistication of cybersecurity threats impacts both businesses and their customers. To earn and grow the trust of customers, partners, and employees, AI Adopters are proactively prioritizing reducing risks, protecting sensitive data, and preserving intellectual property y (see Figure 4).

FIGURE 4

AI on guard

AI Adopters aim to protect business and customer data and preserve trust



Q: What are the primary drivers of AI in your organization? (Objectives focused on protection and prevention.)

The AI value proposition

Perhaps the most significant business advantage comes from combining AI plus automation with a zero trust model. For protection and prevention, these capabilities break down operational silos and improve visibility across the organization's digital estate—data, devices, users, network, workloads, applications, and partner interactions across the ecosystem.

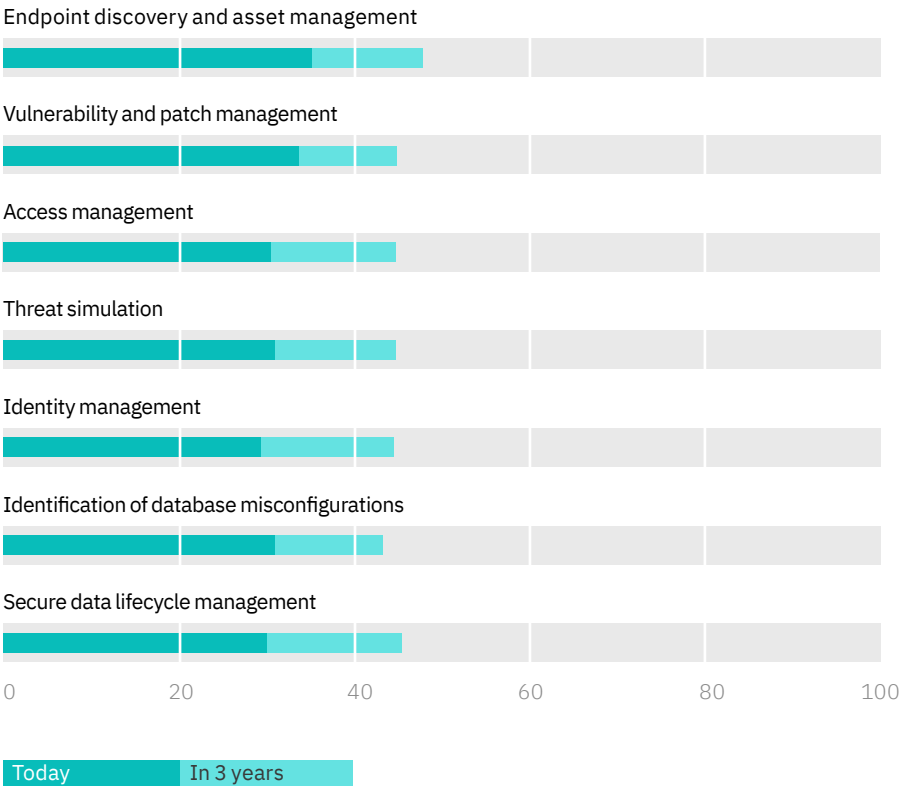
AI plus automation can facilitate this view by regularly performing sensitive data discovery and classification—on premises, at the endpoint, in transit, and in the cloud. The technologies allow companies to use source data and metadata to recreate the full context for any given interaction as well as to understand where the most sensitive data resides, who has access to it (and how), who is accessing it (and when), and what they're doing with it. This can help meet standards for data privacy and regulatory compliance, as well as support monitoring and control of access to highly sensitive data repositories.

In pursuit of this more holistic view of their digital landscape, AI Adopters have identified endpoint discovery and asset management as their top AI use case. 35% are currently applying AI and automation to this capability with plans to increase usage to almost 50% in 3 years (see Figure 5). This application is followed closely by vulnerability management, at 34%. AI Adopters expect to increase their use of AI for protection and prevention by around 40%, on average, in the next 3 years. (See Perspective "How AI helps protect and prevent.")

FIGURE 5

Applying AI for protection and prevention

Adopters are using AI to extend their view across an expanding digital estate



Q. What use cases for AI automation are being implemented today? And in 3 years? (Use cases focused on protection and prevention.)

Perspective

How AI helps protect and prevent

With these top 5 use cases, AI Adopters are investing in protecting the underlying value of their businesses with a focus on reducing risks, preventing attacks, and, in turn, building trust.

AI for endpoint discovery and asset management. Unauthorized devices operate under the radar of organizations' traditional security policies, making them difficult to detect. AI can learn the context, environment, and behaviors associated with specific asset types, network services, and endpoints, and companies can then limit access to authorized devices and prevent access for unauthorized and unmanaged devices.

AI for vulnerability management. AI-powered vulnerability assessments can help identify improperly configured devices so administrators can remove or re-configure them. While active vulnerability scanning in operational technology (OT) environments can destabilize systems, organizations can use AI plus automation to perform passive monitoring. AI can also help prioritize vulnerability patching by providing information about weaponized exploits so clients can take a risk-based approach to vulnerability management.

AI for access management. Companies can use AI to audit access to data and services by users and applications. Once entitlements to sensitive resources are established, AI can coordinate activities across the control plane—monitoring behaviors, flagging anomalies, generating contextual insights, sending alerts, and initiating remedial actions.

AI for threat simulation. Threat simulators can connect to software endpoints across an organization's network to emulate the lifecycle of a cybersecurity incident. This tests live security defenses without interacting with production servers or endpoints, allowing companies to identify and address gaps in their defenses without impacting their operations.

AI for identity management. Zero trust security operations place greater demands on IT infrastructure and security authentication capabilities, notably the need to resolve identity in near real time. While zero trust can represent a significant enhancement in operational capabilities, it also presents new challenges in operations capacity and coordination (for example, supporting remote workers using multiple devices from multiple locations). AI can enhance authentication services by creating a unique user profile based on a combination of historical behaviors, contextual data, and role-based policies.

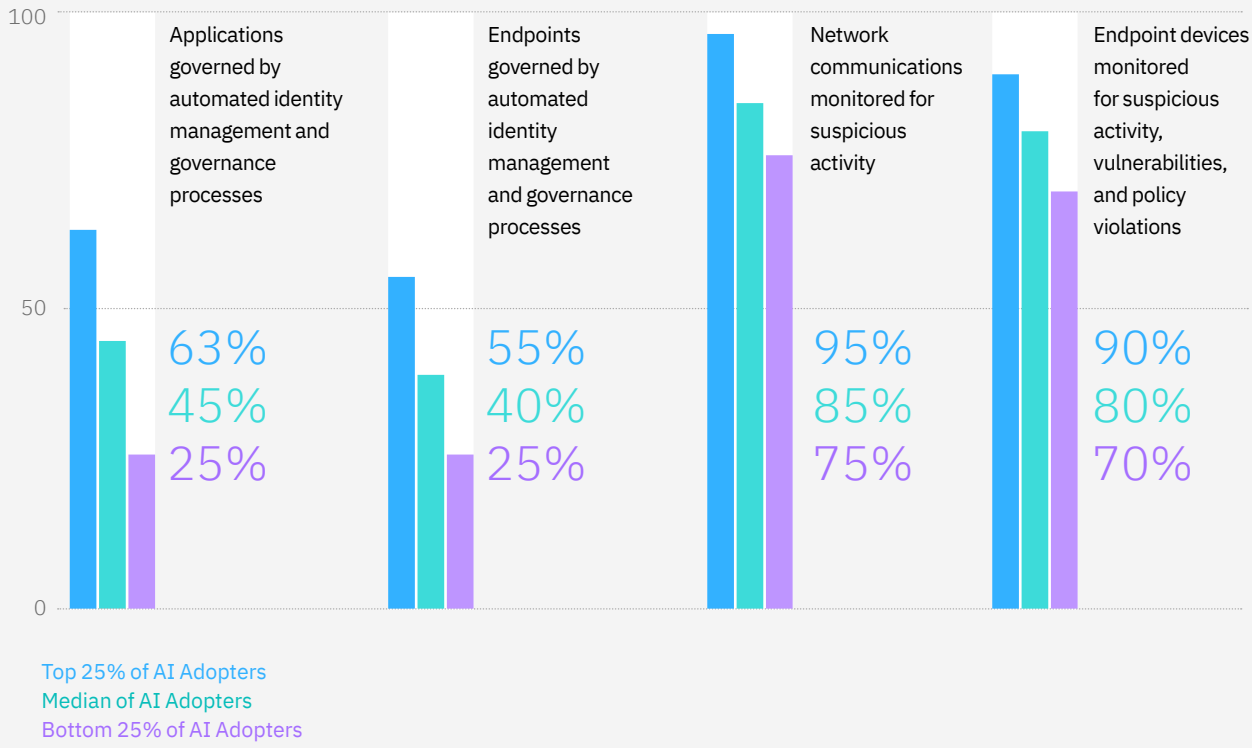
AI-enabled automation is improving the ability of organizations to protect more of their endpoints and applications as well as increase monitoring of network communications (see Figure 6). Top-performing AI Adopters report they are applying automated identity management and governance to 63% of their applications and 55% of their endpoints. These percentages represent an increase of 67% more applications and 50% more endpoints gained through AI. This provides broader visibility over an expanding operations footprint that relies on services spanning multiple clouds.

FIGURE 6

Expanding visibility

Automation allows AI Adopters to govern and monitor more assets

Percentage of assets being governed and monitored using AI



Even the median percentages reported for these areas reflect solid numbers of applications and endpoints being governed with automation, with substantially more upside available as performance improves. AI Adopters report even better progress in using AI plus automation to watch network communications and endpoint devices for suspicious activity. Top-performing AI Adopters say they are using AI to monitor 95% of network communications and 90% of endpoint devices.

The true value of protection and prevention is rooted in something inherently difficult to measure: avoidance. Given more relevant and timely performance insights from across all digital assets, security teams can more effectively avoid threats, mitigate risks, and protect and preserve their organizations' bottom lines and brand reputations.

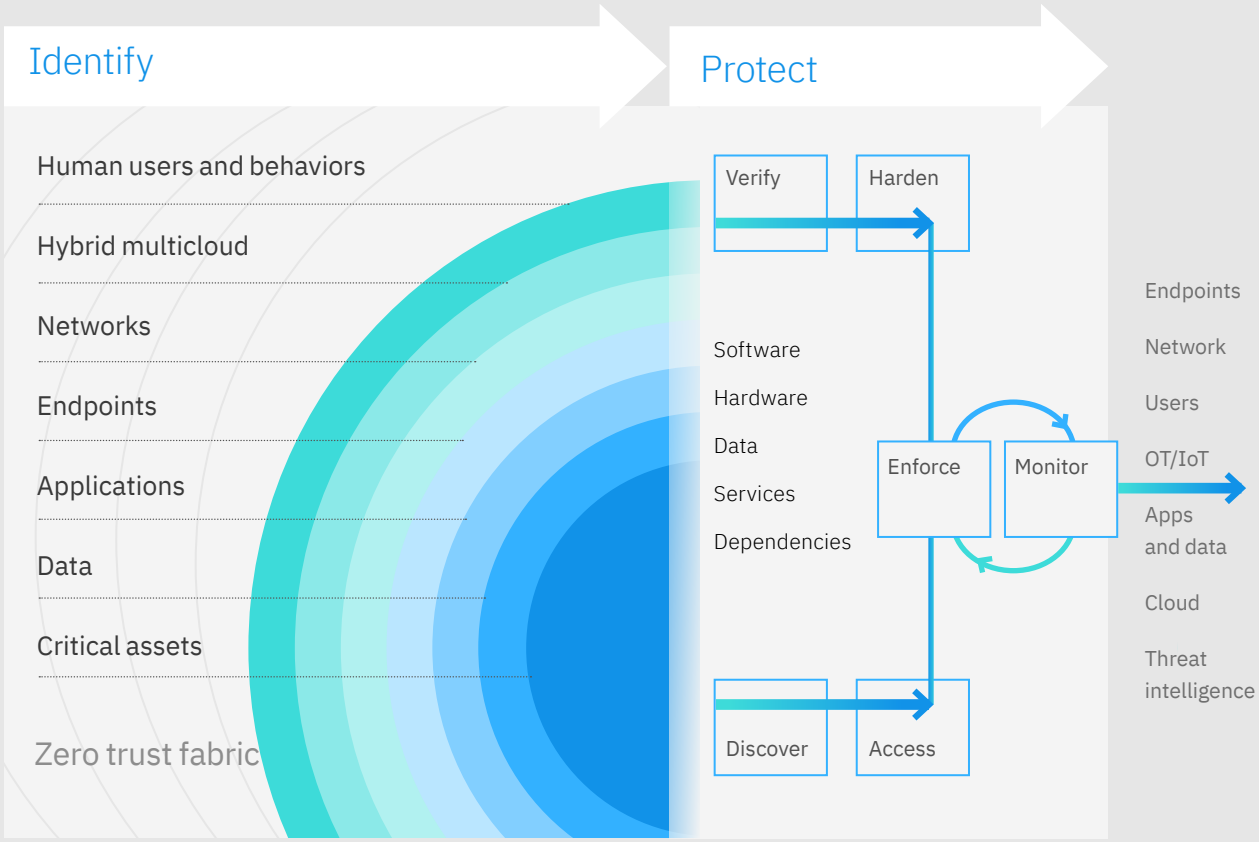
Leading AI Adopters are using automation to govern 63% of their applications and 55% of their endpoints.

Perspective

The combination of AI and automation enables better security controls

Protection and prevention

AI supports monitoring multiple layers across multicloud environments

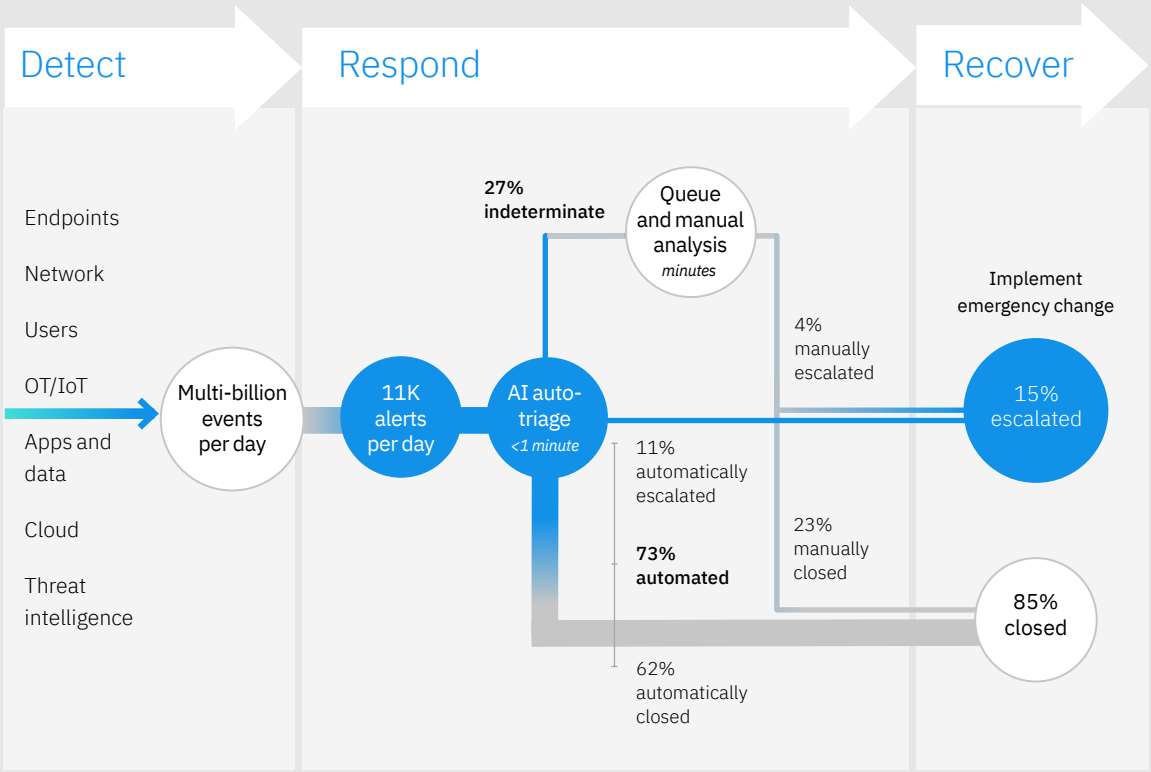


Perspective

The combination of AI and automation improves security operations performance

Detection and response

Using AI and automation can compress performance metrics



The future analyst's experience

Without AI	With AI plus automation
8 tools/screens	1 screen
19 steps	6 steps
Response time in hours/days	Response time in minutes

Source: IBM Security Services based on an analysis of aggregated 2021 performance data.
Note: Performance thresholds depicted are expected to improve on a continuing basis.

Detect and respond: Using AI to boost productivity and accelerate recovery

The challenges

The well-being of the business is not only based on protecting against and preventing incidents, but on how rapidly organizations can detect, respond to, and recover from them. Zero trust design principles suggest security professionals should assume their organizations have already been breached and will be breached again in the future.

Multiple issues are feeding the primary drivers for using AI in detection and response activities. As noted previously, the rapidly expanding digital footprints of most organizations, the move to increasingly open business models, and the sharp rise in the number of remote employees are generating a torrent of new security events. Many security organizations simply don't have the capacity to manually monitor, manage, and act on all of them quickly and effectively.

A cyber talent shortage compounds the situation. A lack of skilled employees has a major impact on the organization's security posture—both in terms of applying resources more efficiently to improve response times and leveraging expertise to strengthen the quality of security outcomes.

According to EMSI, a national labor analytics firm, for every 100 cybersecurity roles needed, there are only 68 qualified candidates, many of whom are already gainfully employed.[12] A recent IBV study found organizations need 150 days to fill a cybersecurity vacancy with a skilled candidate.[13] New front-line analysts, who need additional operational support to do their jobs effectively, are not necessarily alleviating the talent shortage. They are often inexperienced in the industry and require time to truly develop the confidence and maturity in their threat assessment and investigation skills.

AI plus automation can support these analysts with knowledge management, case management, and operational support capabilities (for example, front-line chatbots and natural language knowledge repositories). The net result is groundbreaking: an augmented intelligence capability made possible by the combination of human judgement and AI plus automation. (See Perspective "AI plus automation—a talent revolution.")

Perspective

AI plus automation– a talent revolution

Cybercultural awareness and cybersecurity talent play a critical role in delivering security and business outcomes. Successful AI programs don't make talent obsolete. They enhance the efficiency and effectiveness of security analysts and the reach of security knowledge workers. By opening the door to a more flexible engagement model, AI alleviates some of the resource and skill constraints that play a decisive factor in positive and negative security outcomes.[14]

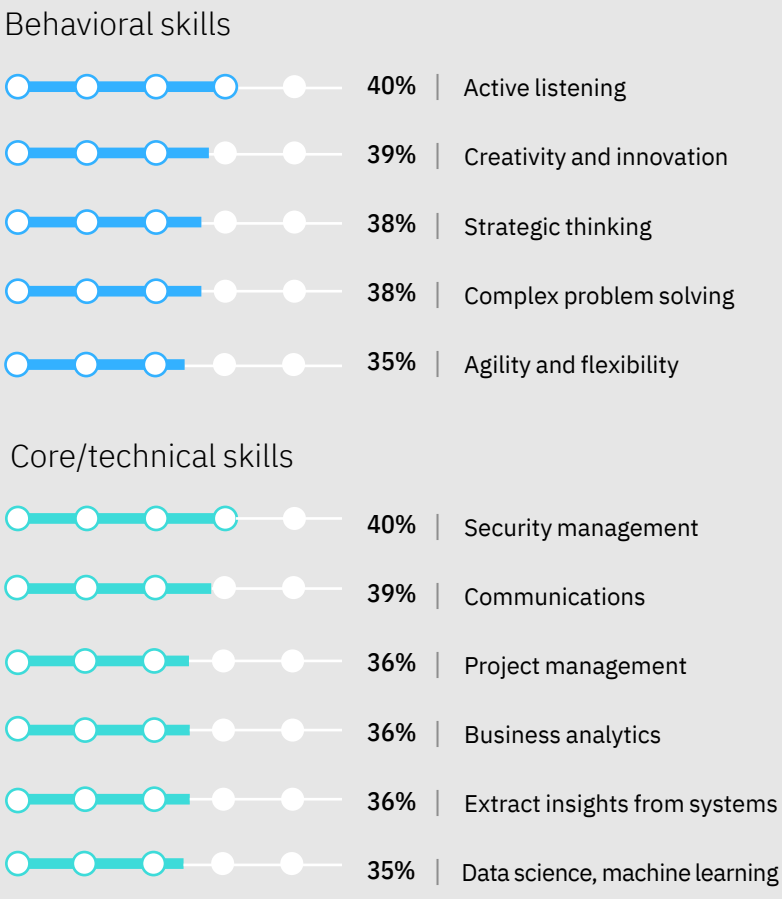
AI Adopters are experiencing an acute demand for new talent. Over the past 12 months, they added 15% net new cybersecurity employees and attribute 40% of this change to their adoption of security AI. Respondents told us 34% of security roles had skills requirement changes, 35% of which were driven directly or indirectly by the adoption of AI.

By combining human factors with technology, AI Adopters can address the resource gap directly by reinvesting in their cybersecurity workforce. Organizations can grow talent natively by making automation less about cost optimization and more about specialization and a better work experience, helping employees to expand their skills.

AI Adopters prioritize a combination of behavioral and technical skills in their employees. From a behavioral perspective, 40% cite active listening as the most important skill employees need as a result of AI; 39% say the same for innovation and creativity. On the technical side, 40% consider security management skills to be most important, while 39% are focused on communication skills (see Figure). This greater flexibility in integrating soft and hard skills is one of the most promising areas for new AI value propositions.

AI demands a skills mix

Cybersecurity employees need both hard and soft skills to succeed with AI



Q. What skills do/will your cybersecurity staff need to develop/enhance as a result of AI?

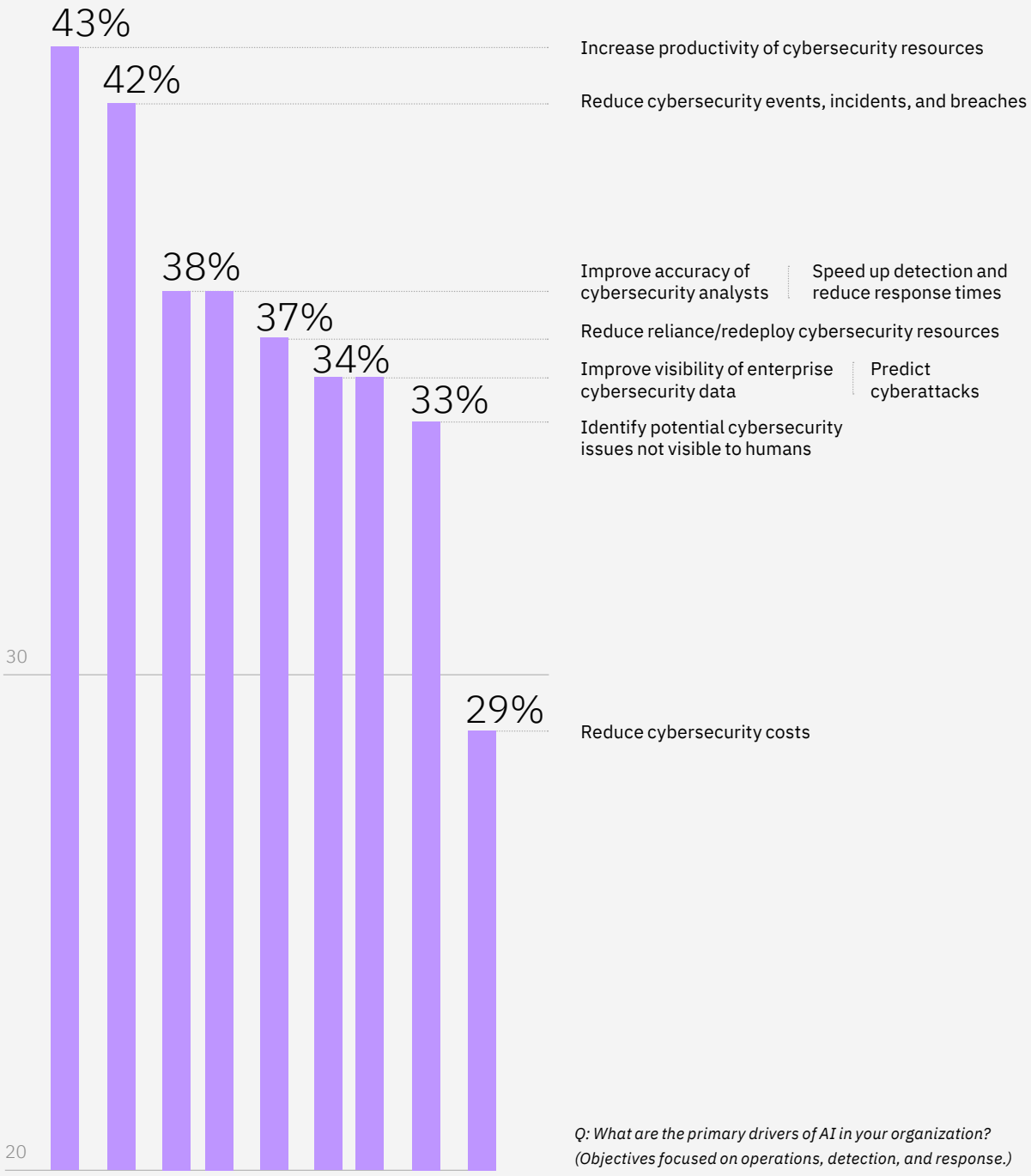
In response to the staffing challenges, AI Adopters are deploying AI plus automation to improve the productivity and work experience for overstretched resources. In fact, 43% cite increasing the productivity of cyber resources as a top driver for using AI. 42% report that reducing security events, incidents, and breaches is a goal, and 38% are focused on using AI to improve the accuracy of cybersecurity analysts (see Figure 7).

Considered as a whole, AI and automation can have a dramatic positive impact on the ability to address the sheer volume and tempo of security events, a key factor in improving the security analyst's work environment. By better understanding which threats require greater attention, analysts can shift from routine triage to higher-value threat investigation activities. The ultimate outcome: gains in both capacity and specialization across the cybersecurity workforce.

FIGURE 7

Boosting productivity

AI Adopters aspire to improve analysts' efficiency in detection and response



Q: What are the primary drivers of AI in your organization? (Objectives focused on operations, detection, and response.)

The AI value proposition

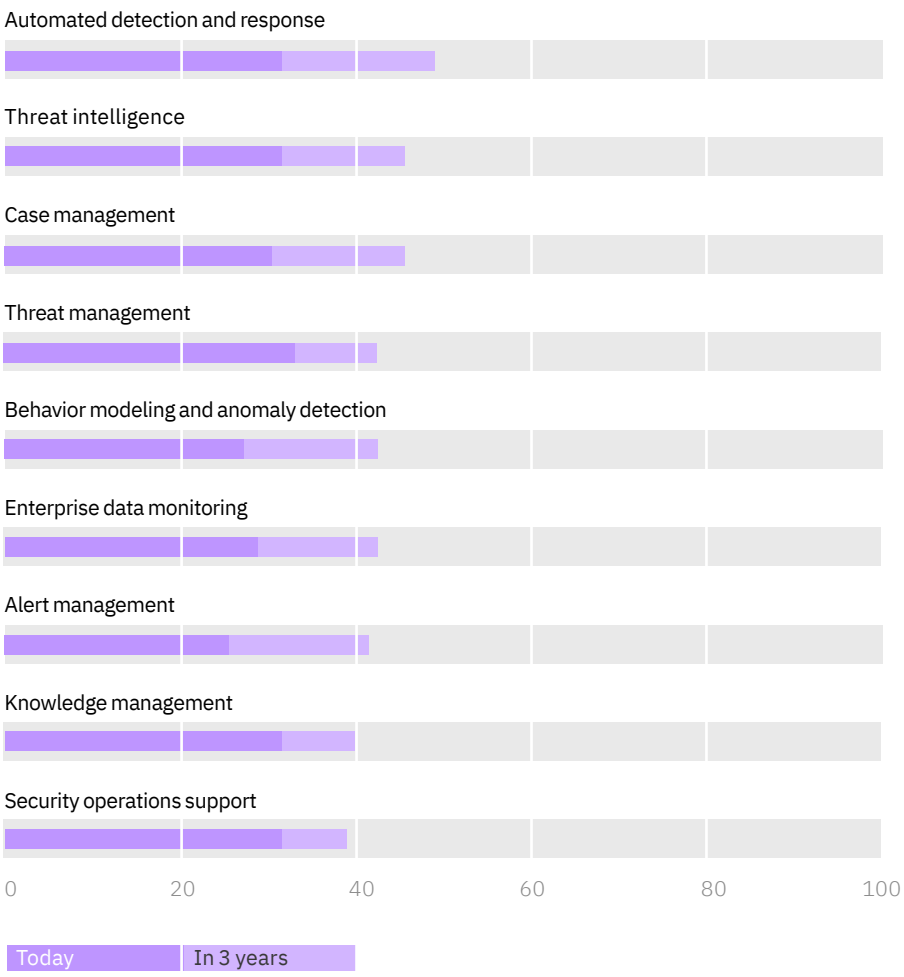
The secret to improving productivity is supporting the workforce by applying technology where it can be most effective. For example, threat detection is an ideal use case for reducing manual methods and gaining efficiencies through AI plus automation. Automated, AI-driven investigation processes can selectively protect high-value data and assets, network segments, and cloud services. By providing greater visibility into network communications, traffic, and endpoint devices, AI plus automation helps improve the ability to identify potential threats, allowing cyber resources to consistently make better, more informed decisions.

AI Adopters recognize the potential of using AI plus automation for threat management. 34% indicate this is their top AI use case for detection and response activities (see Figure 8). This is closely followed by automated detection and response, which will become the most widely implemented in three years, according to 49%. And, as with the protect and prevent use cases, Adopters expect to increase their use of AI for detect and respond use cases by an average of around 40% within the next 3 years. (See Perspective “Using AI to detect and respond faster.”)

FIGURE 8

Applying AI for detection and response

Adopters are using AI to identify threats faster and respond proactively to cyberattacks



Q. What use cases for AI automation are being implemented today? And in 3 years? (Use cases focused on detection and response.)

Perspective

Using AI to detect and respond faster

AI Adopters are using AI plus automation to significantly improve the productivity of their cybersecurity workforce, as measured by several key performance indicators. These 5 use cases demonstrate how.

Automated detection and response. Security AI plus automation automates the collection, integration, and analysis of data from hundreds and even thousands of control points, synthesizing system logs, network flows, endpoint data, cloud API calls, and user behaviors. Together with threat management and alert prioritization, organizations can complement existing telemetry solutions with endpoint detection and response (EDR) and cross-layer detection and response (XDR) capabilities. These allow security operations teams to fully understand the context of security exceptions, establish priorities, and devote sufficient resources to investigating high-impact threats.

Threat intelligence. AI-enabled security intelligence enables organizations to analyze live data streams to detect abnormal behavior in real time. Combining security information across domains—by integrating internal telemetry signals with external intelligence sources—provides actionable intelligence in an actionable window, improving the effectiveness of security policies, especially those associated with emergent threats. In addition, log capture capabilities can be extended by applying the same procedures across cloud environments—scanning for irregular configurations that may point to more elusive attack signatures like zero days and advanced persistent threats (APTs).

Case management. Security case management functionality allows a security team to gather information on suspicious activity and escalate investigations with detailed, case-related information and logs. Applying AI can increase the speed and volume of data processed and integrate data science techniques, allowing for automated identification and classification of data in documents. Because AI can understand context, it can group data by topic without prior classification, helping security teams use data recognized as related to make inferences and find similarities that are not readily apparent.

Threat management. AI helps analysts triage alerts effectively by focusing on the most critical ones first, helping distinguish between false negatives and false positives and greatly reducing the chances of missing critical incidents. It also classifies and prioritizes threats to trigger alerts based on attack signatures, indicators of compromise (IOC) and indicators of behavior (IOBs).

Behavior modeling and anomaly detection. Automated AI security models can recognize abnormal behaviors, assess vulnerabilities dynamically, and flag anomalous activity—all potential indicators of compromise. Then, machine learning can suggest remediation options based on a broad spectrum of factors like situational variables, historical precedents, or threat intelligence sources—followed by updates to policy administration at specific control points.

AI Adopters report successfully reducing the time to detect and respond to incidents (see Figure 9). Compared to performance estimates before they implemented AI, the Adopters report the median days to detect incidents decreased by 12%, while the median days to respond to and recover from incidents declined by 11%. When looking at the leading performers, we see the real opportunity for AI plus automation to deliver significant improvements. The top 25% of AI Adopters report they have used AI to cut the time to investigate incidents by nearly one third and the time to respond and recover by nearly a quarter. They have also reduced dwell times by 45%.

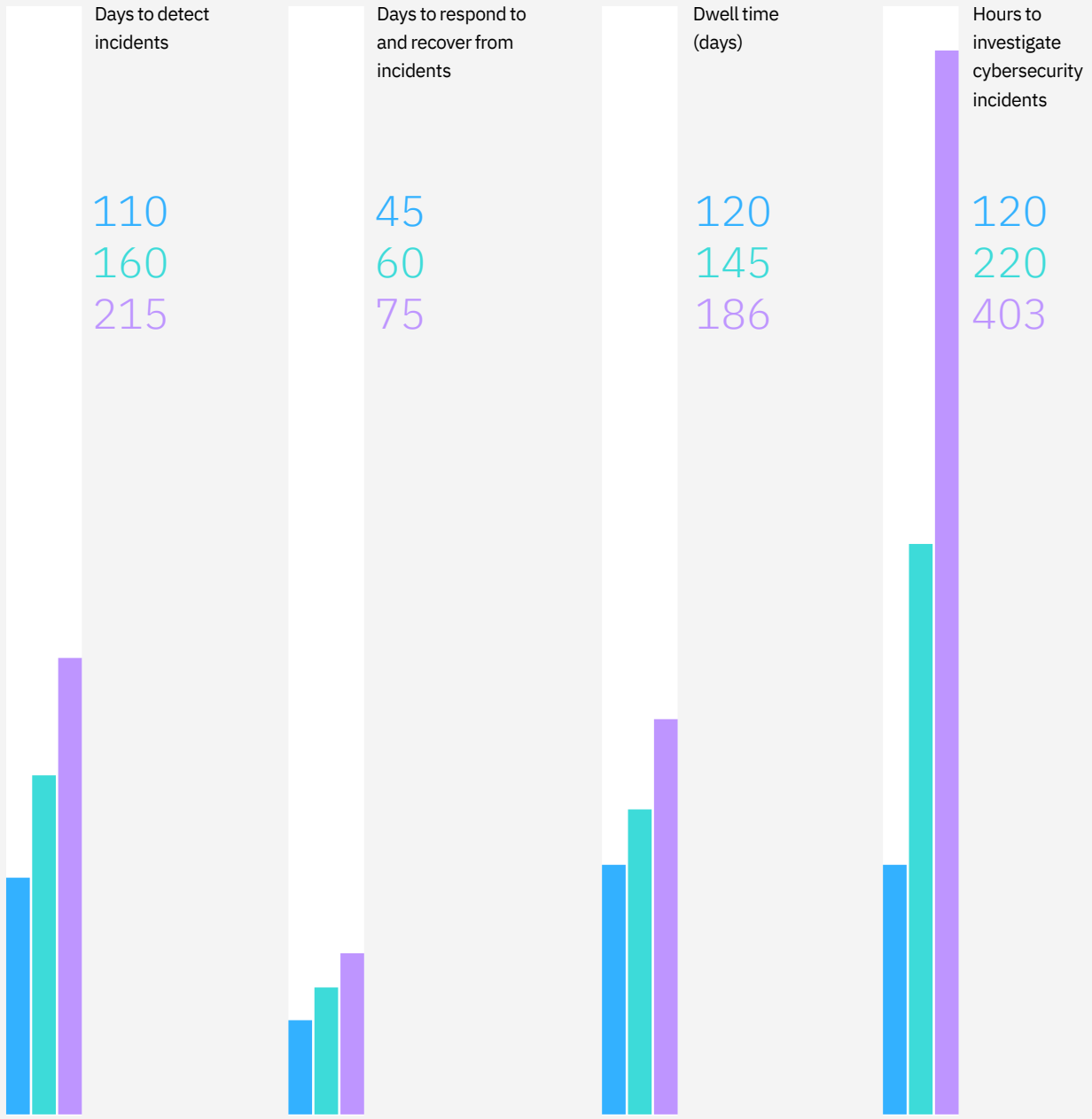
AI Adopters are demonstrating that deploying AI plus automation across the entire security operations lifecycle enhances protection and prevention capabilities while improving their detection and response performance. Their success reveals how organizations can potentially use AI to greatly enhance overall cyber resilience during challenging times. (See case study “AI plus automation—Better work environment, better performance.”)

Top-performing AI Adopters cut the time to investigate cybersecurity incidents by nearly 30%.

FIGURE 9

Speeding recovery

Top performers have markedly better detection and response times for security incidents



Top 25% of AI Adopters
Median of AI Adopters
Bottom 25% of AI Adopters

Shorter bars represent better performance

Case study

Global managed security services provider

AI plus automation – Better work environment, better performance

A managed security services provider serving hundreds of global clients from across industries was encountering recurring capacity issues, despite having modernized security operations with hybrid cloud and zero trust capabilities. “The attack surface is only getting bigger,” said one of the client’s lead security analysts. “We see both sides of the issue: either too much information from too many sources or a lack of relevant information at the right moment, when it matters most.”

Making matters more challenging, skills and specialization were in short supply. “We are competing for hard-to-find talent and any advantage can give us an edge,” said the lead client executive. Using design thinking and IBM Garage™ collaboration methodologies, client leaders started by framing the opportunity in terms of business outcomes. “We wanted to create a better work experience for our analysts. We were also interested in seeing how greater automation might improve the team’s performance,” the client executive said.

An integrated development and operations team articulated four primary goals:

- Reduce noise for analysts so they can focus on high value alerts
- Reduce triage time by compiling contextual data, metadata, and service logs to faithfully re-create the threat environment
- Speed investigations through greater context and enriched data/metadata
- Supplement pinpoint recommendations with explanation and reasoning

After nearly a year, the client has dramatically improved operational efficiency by:

- Automating the triage of 73% of alerts—up from 40%—at a confidence level greater than 90%
- Reducing the total attack surface—and associated risk—by an estimated 50% using workload-specific zero trust controls
- Reducing attacker dwell time and windows of vulnerability by 50%
- Reducing security incidents by 75% and doubling mean-time-to-breach performance

While AI powers automation, the solution’s impact on the human side of the equation is perhaps even more powerful. The combination of AI and automation frees analysts to focus on higher-impact threats, such as zero days, APT detection, threat hunting, and forensics. Security analysts provide ongoing feedback to make the solution smarter but also more human-friendly. The client executive sums up the impact to the business: “For us, the ability to combine automation with a better work environment for our team made all the difference.”

Chapter 3

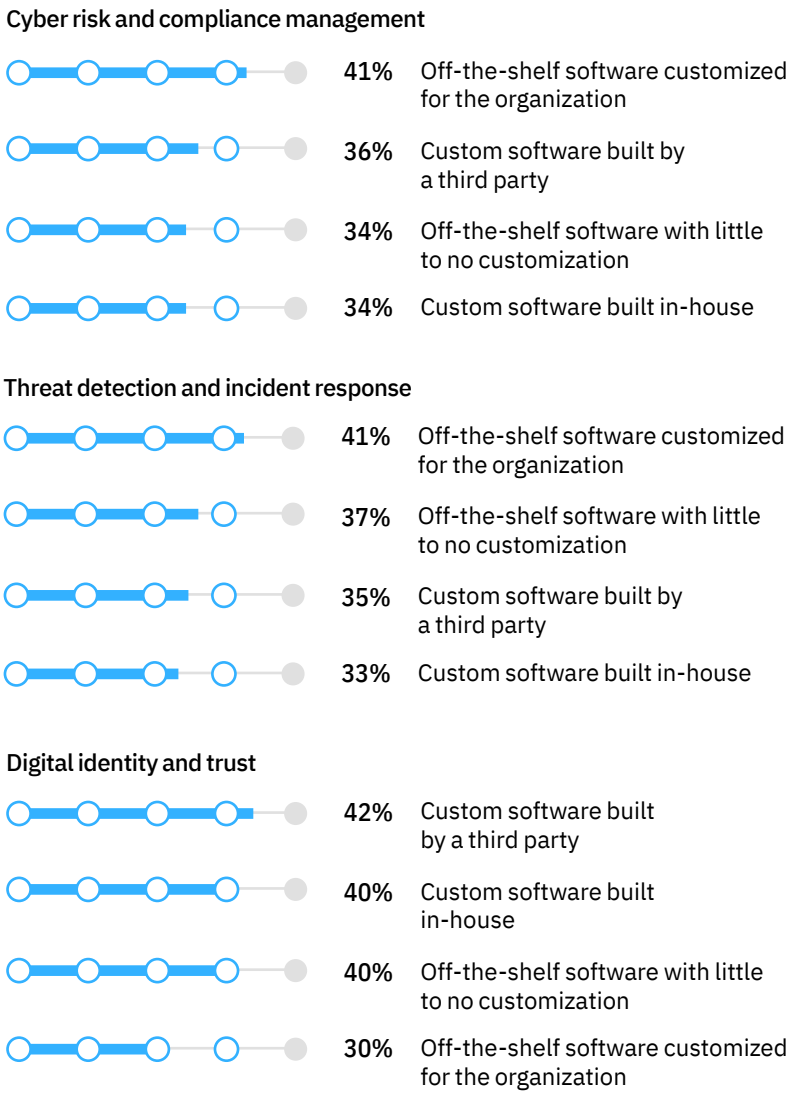
Planning your roadmap for security AI adoption

As you look at integrating AI insights and automation into your security operations, consider what a successful deployment might look like. AI Adopters are using a mix of off-the-shelf solutions and custom-built tools. For cyber risk and compliance as well as threat detection and incident response, more AI Adopters report configurable, off-the-shelf software is the most successful deployment type (see Figure 10). But for digital identity and trust management, AI Adopters say that custom software built either in-house or by a third party has led to more successful outcomes.

FIGURE 10

Security AI enablement

The most successful deployments typically involve some form of customization



Q. How would you describe your organization's deployment of AI technology for cyber risk and compliance management? (Select the top 3.)

Q. How would you describe your organization's deployment of AI technology for threat detection and incident response management? (Select the top 3.)

Q. How would you describe your organization's deployment of AI technology for the management of digital identity and trust? (Select the top 3.)

Highly configured and custom-developed security solutions can deliver greater capabilities—and greater benefits, yet the continuing costs associated with development and support must be factored into your security operations budget.

While some industries may benefit from specialized AI security applications (for example, banking and financial markets), ongoing support costs, staffing requirements, and patch schedules must be considered carefully, particularly for maintenance and vulnerability management. The decision to customize a solution should reflect a compelling business rationale based on the organization's evolving risk posture and potential security vulnerabilities.

A custom AI solution should factor in ongoing support costs.

Action guide

Applying security AI and automation to deliver business value

Even the most successful security organization is a work-in-progress. The dynamic nature of operations and the continuous emergence of new threat vectors require you to prioritize readiness and resilience. It is not a matter of if your organization will be breached, but when and to what extent.

Similarly, recognize that AI models must continue to learn, and your security teams must keep feeding them with new performance insights. This commitment to constant learning influences the outcomes you can achieve.

For AI Adopters, security performance is impacting both operational efficiency and business value, while creating a more empowered, more adaptable work environment for security analysts. Taken together, these factors can have a significant impact on the organization's overall cyber resilience.

Whether you are piloting these capabilities for the first time or expanding the functionality of existing applications, three recommendations can guide these efforts.

01

Benchmark your performance across key security metrics

Identify the drivers of security improvement

- Understand the pressing strategic rationale for deploying AI and automation capabilities to your security operations; then update your cyber risk and cybersecurity strategy to reflect this change in priorities. Is it to reduce cybersecurity incidents and breaches or to reduce costs through operational efficiencies? Or perhaps to improve customer, employee, or partner trust?

Identify areas for improvement based on benchmark comparisons

- Examine key risk and security metrics—for protection and prevention as well as for detection and response—and compare your organization's performance with peers. Gaps represent areas where you can focus improvement initiatives, targeting areas where AI plus automation can help the most.
- To perform comparisons, some organizations offer formal benchmarking services. Alternatively, you can find security metrics through online sources such as the Ponemon Institute, Gartner, Forrester, IDC, SANS Institute, the Cloud Security Alliance (CSA), and others.

02

Prioritize security improvements that deliver the most value and align with your top security goals

Set priorities based on impact and target improvements across key performance measures

- Evaluate the potential benefits that can be realized from improving performance on each of your key performance metrics. This helps you see which areas can deliver the greatest value in terms of operational factors like cost, efficiency, quality, and time. Assuming the potential areas align with your security strategy, their measures should contribute the most to achieving your strategic objectives.

Identify the AI applications that are most likely to improve performance

- Understand the performance measures most closely associated with protection and prevention and detection and response. For example, for protection and prevention, a key measure is the number of applications and endpoints governed by automated identity or endpoint management. For detection and response, dwell time is an important metric.
- Consider the AI applications in both areas that are most likely to deliver the performance improvements and business benefits you have determined are most important. Use these priorities to define your organization's security AI and automation roadmaps. Determine your strengths and identify where you can leverage partners to extend your expertise. Lastly, select the AI deployment model that is most likely to be successful—whether configuring an existing solution or developing a specialized solution—and to what extent you wish to rely on third parties for development and support.

03

Develop key enablers for security improvement initiatives

Define a security AI strategy and a corresponding operations plan

- Implement, govern, and manage your AI applications in line with your organization's broader cyber risk and security strategies. Make sure these are reflected in operational policies, controls, and processes.

Determine and develop the behavioral and technical skills your organization needs to be successful

- Consider the impact of automation on your cybersecurity workforce. Will they perceive automation as a threat or as an opportunity? What is the right way to engage in this conversation?
- When considering what makes security AI plus automation successful, factor in development and retention components like work environment, the demand for specialization and expertise, and associated upskilling or reskilling. What mix of skills is required in an AI-plus-automation environment?
- Determine where AI plus automation can provide the greatest benefit to your cybersecurity workforce. Identify gaps and provide role-based training to build and enhance the required behavioral and technical skills. Consider human factors like experiential learning and cybersecurity simulations to build skills while providing real, practical experience, using either in-house or external workforce partner services.
- Finally, monitor your progress. As new AI applications and functionality are deployed, validate your actual performance against target benchmarks to determine the relative efficiency of various investments.

About
the authors

Sridhar Muppidi

Chief Technology Officer
IBM Security
linkedin.com/in/smuppidi
muppidi@us.ibm.com

Sridhar is an IBM Fellow and CTO for IBM Security. He is responsible for driving the technical strategy, architecture, and research for the IBM Security portfolio of products and services to help clients manage defenses against threats and protect digital assets. He is a results-oriented technical thought leader with 25 years of experience in building security products, delivering solution architecture for clients, driving open standards, and leading technical teams.

Lisa Fisher

Global Benchmark Research Leader,
IT, security, and cloud
IBM Institute for Business Value Leader,
Middle East and Africa
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

Lisa is responsible for producing benchmarking research, for all industries and regions, to envision and articulate the impact of technologies on business from cyber risk and cybersecurity perspectives. Lisa is based in South Africa.

Gerald Parham

Global Research Leader—Security & CIO
IBM Institute for Business Value
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald leads the Security and CIO research areas within the IBM Institute for Business Value. He focuses on cyber strategy, board advisory, and ecosystem-level security—in particular the relationship between strategy, risk, open security, trust, and business value. He has more than 20 years of experience in executive leadership, innovation, and intellectual property development.

About Benchmark Insights

Benchmark Insights feature insights for executives on important business and related technology topics. They are based on analysis of performance data and other benchmarking measures. For more information, contact the IBM Institute for Business Value at global.benchmarking@us.ibm.com.

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights.

To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also follow @IBMIBV on Twitter or find us on LinkedIn at https://ibm.co/ibv-linkedin.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

Related reports

Getting started with zero trust security

McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. "Getting started with zero trust security." IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

The new era of cloud security

Thompson, Shue-Jane, Shamla Naidoo, Shawn Dsouza, and Gerald Parham. "The new era of cloud security: Use trust networks to strengthen cyber resilience." IBM Institute for Business Value. April 2021. ibm.co/cloud-security-cyber-resilience

AI ethics in action

"AI ethics in action: An enterprise guide to progressing trustworthy AI." IBM Institute for Business Value. April 2022. ibm.co/ai-ethics-action

Study and research methodology

The IBM Institute for Business Value partnered with APQC (American Productivity and Quality Center) to survey 1,000 executives with overall responsibility for IT and operational technology (OT) cybersecurity and information security at their organizations. Respondents represent 16 industries, including banking and financial markets, electronics and software, government, insurance, media and entertainment, retail, and services. They are distributed among 5 global regions: Africa and Middle Easter, Asia Pacific, Central and South America, Europe, and the US and Canada. Companies not applying AI in their security function processes are included.

Respondents were asked to provide information about the current and planned application of AI in their cyber risk and cybersecurity processes, as well as the performance of their security functions. Because many factors influence performance, we asked AI Adopters—the 637 companies that are piloting, implementing, operating, or optimizing AI in at least one security process—to provide their own estimate of how AI had influenced performance on common cyber risk and security function KPIs. This allowed us to calculate the range of performance on each KPI as well as the range of impact that AI has had on each KPI.

The KPIs in this report are defined as follows:

Dwell time is the time between a successful incursion/compromise and its discovery/detection.

Average time (in calendar days) to respond to and recover from cybersecurity incidents begins when an incident has been detected and its scope has been established. It includes activities to remove the threat and restore the affected systems to their pre-incident condition; testing, monitoring, and validating affected systems; and restoring operations.

Average time (in hours) to investigate cybersecurity incidents starts from the time a security alert is escalated for investigation until the investigation is complete.

Cybersecurity cost as a percentage of IT cost includes IT costs related to application, cloud and data security, identity access management, infrastructure protection, integrated risk management, network security equipment, other information security software, security services, and consumer security software. It includes all costs for processes to support enterprise operations and excludes depreciation/amortization (that is, based on cash flow) and "resold IT."

Return on security investment (ROSI) is expressed as a percentage and is equal to {[the estimated total loss in USD x total cost of cybersecurity (the percentage mitigation afforded by cybersecurity solution(s) or efforts)] – total cost of cybersecurity (the total cost of cybersecurity solution(s) or efforts)} / total cost of cybersecurity (the total cost of cybersecurity solution(s) or efforts)

Cost of a data breach includes direct and indirect expenses incurred for the detection, escalation, notification, and post data breach response activities. The average cost of a data breach is: (annual number of breaches multiplied by all cost factors) / (annual number of breaches).

The performance ranges used in this report are defined as follows:

Top performers are AI Adopters performing in the 75th or 25th percentile on each metric, dependent on whether it is better to have a higher or lower value for a given measure. If, for a particular metric, it is better for a value to be higher, then top performers—the top 25% of AI Adopters—are organizations performing in the 75th percentile. 75% of respondents perform below and 25% perform at or above this level. If it is better for a value to be lower, then top performers are AI Adopters performing in the 25th percentile. 25% of respondents perform at or below this level and 75% perform above. The median is the midpoint value in the distribution of responses; half of respondents perform below this level and half perform above.

Acknowlegments

The IBV would like to extend thanks to the distinguished team of security researchers at IBM Research, who are exploring the impact of new technologies and applied innovations across the security lifecycle. This team includes J.R. Rao, Marc Stoecklin, and Ian Molloy. We would also like to extend thanks to Srini Tummalapenta and Charles Henderson, who graciously shared their expertise in articulating key themes. This report would not have been possible without the generous contributions of these colleagues.

We would like to express our appreciation to Mary O'Brien and Chris McCurdy, who lead a global team of security professionals at IBM Security. Our colleagues in IBM Security have provided valuable, real-world advice based on engagements with hundreds of global clients. Their work provides an essential foundation for much of our research.

Finally, we would like to extend thanks to our fellow IBV colleagues who supported us in creating these materials. This includes Dave Zaharchuk, Kirsten Palmer, Heba Nashaat, Sherihan Sherif, Joanna Wilkins, Angela Finley, and Kathy Cloyd. Every week the IBV publishes new thought leadership reports based on primary research. Each report is supported by a diverse team of research, analytical, and creative professionals who collaborate to bring these materials to life.

Notes and sources

1 Turton, William, and Kartikay Mehrota. “Hackers Breached Colonial Pipeline Using Compromised Password.” Bloomberg. June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password; Holmes, Aaron; “Ransomeware gangs targeted 3 different US water treatment plants this year in previously unreported attacks, according to federal agencies.” Insider. October 16, 2021. https://www.businessinsider.com/3-us-water-treatment-plants-attacked-by-ransomware-gangs-report-2021-10

2 Vigliarolo, Brandon. “Report: Pretty much every type of cyberattack increased in 2021.” TechRepublic. February 17, 2022. https://www.techrepublic.com/article/report-pretty-much-every-type-of-cyberattack-increased-in-2021/; 2022 IBM X-Force Threat Intelligence Index.” IBM Security. February 2022. ibm.com/security/data-breach/threat-intelligence/

3 “SolarWinds hack was ‘largest and most sophisticated attack’ ever: Microsoft president.” Reuters. February 14, 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R; Robertson, Paul. “Best of 2021—Worldwide Hack: Microsoft Exchange Server Zero-Day Exploits.” Security Boulevard. December 27, 2021. https://securityboulevard.com/2021/12/worldwide-hack-microsoft-exchange-server-zero-day-exploits/; Torres-Arias, Santiago. “What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what’s at stake.” The Conversation. https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896

4 “The 2021 CIO Study. The CIO Revolution: Breaking barriers, creating value.” IBM Institute for Business Value. November 2021. ibm.co/c-suite-study-cio

5 Schneier, Bruce. “The Coming AI Hackers.” Harvard Kennedy School, Belfer Center for Science and International Affairs. April 2021. https://www.belfercenter.org/publication/coming-ai-hackers

6 “AI & Cybersecurity: Balancing Innovation, Execution & Risk.” Pillsbury Law and The Economist Intelligence Unit. September 9, 2021. https://www.pillsburylaw.com/en/news-and-insights/ai-and-cybersecurity-balancing-innovation-execution-and-risk.html

7 Morgan, Steve. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” Cybercrime Magazine. November 13, 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

8 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.co/security/data-breach. “Identity Theft Resource Center’s 2021 Annual Data Breach Report Sets New Record for Number of Compromises.” Identity Theft Resource Center. January 24, 2002. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

9 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.com/security/data-breach

10 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

11 “2022 IBM X-Force Threat Intelligence Index.” I BM Security. February 2022. ibm.com/security/data-breach/threat-intelligence/

12 Hatton, Tim. “The Cybersecurity Talent Shortage: An Urgent Threat.” EMSI. March 8, 2022. https://www.economicmodeling.com/2022/03/08/the-cybersecurity-talent-shortage/

13 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

14 Brandenburg, Rico and Paul Mee. “Cybersecurity for a Remote Workforce.” MIT Sloan Management Review. July 23, 2020. https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | June 2022

9NGZA7GK-USEN-01