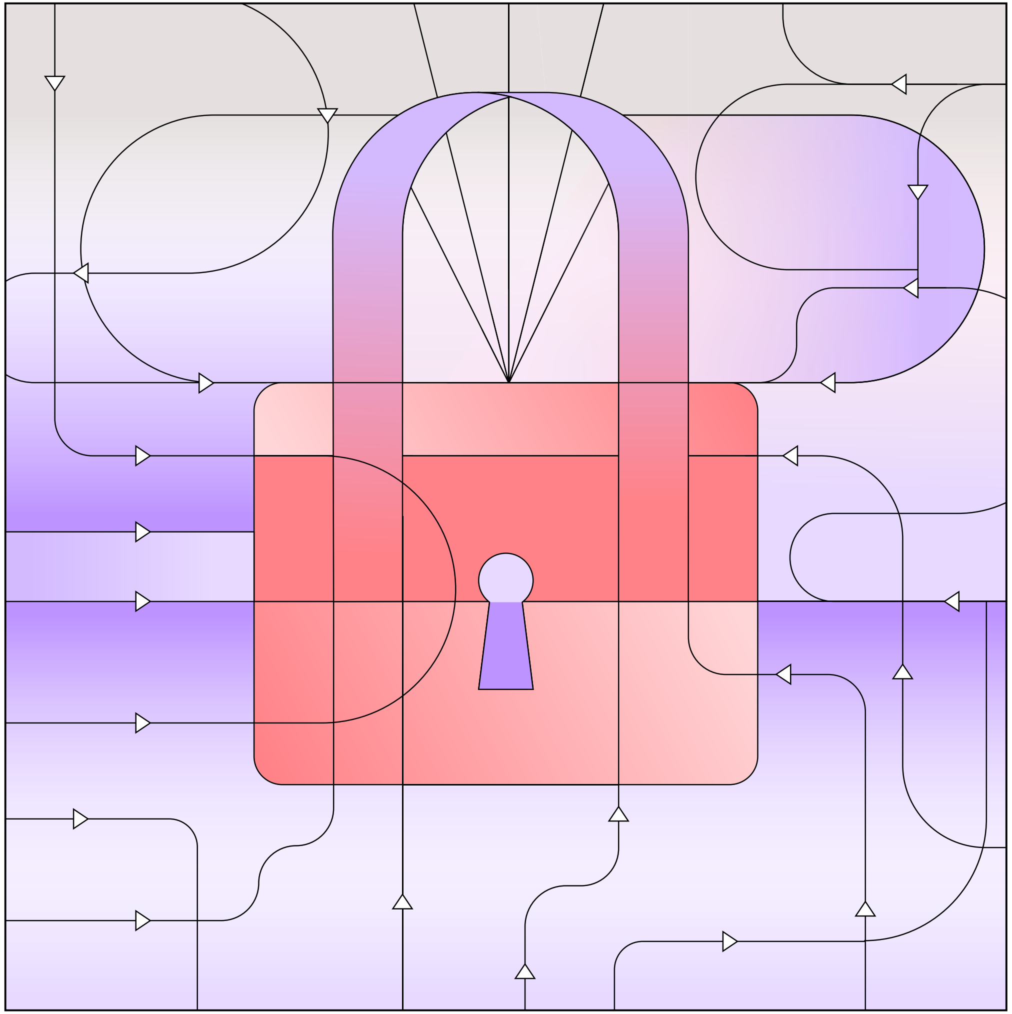
IBM Institute for Business Value | Research Brief

Unify your fragmented security

Accelerate transformation with platformization



IBM | paloalto NETWORKS

Introduction

Building a new foundation for cybersecurity resilience

From the C-suite to security operations centers (SOCs), the growing scope and scale of cyberattacks is raising security concerns to new heights. With the total annual economic impact of cybercrime estimated to exceed $10.5 trillion by 2025, CEOs are looking for more effective approaches to navigate the threat landscape.[1] And with SOC operators reporting that they no longer have time to review 51% of daily alerts, cybersecurity professionals are looking to AI, automation, and more seamless security architectures to detect, deflect, and deter threats.[2]

Meanwhile, the growth of cloud, AI, IoT, and edge computing is creating an even more target-rich environment, resulting in more attacks with costlier implications. The latest Threat Intelligence 2024 Report from IBM found a 31% increase in cyberattacks year over year in Europe, while there was a 71% increase in the volume of attacks using valid credentials globally.[3]

This latter trend reflects a worrying shift in security threats—enabling hackers to simply log-in rather than hack-in—which are markedly more difficult to identify and remediate. This may, in part, explain why the cost of each attack is going up. According to IBM research, the cost of the average data breach now stands at $4.45 million globally, up 15% in a year. In the US, the average cost is as high as $9.48 million.[4]

Bad actors seek bigger prizes. In addition to ransomware attacks and data breaches, they have put the core assets of AI—the GPU server infrastructure—in the crosshairs. In fact, researchers recently discovered a hacking scheme to hijack machines and computing power worth $1 billion.[5]

With the clock ticking until the next headlining hack, corporate and cybersecurity leaders must rethink security strategies and restructure for resiliency. This means adopting across-the-board automation to give cybersecurity professionals more time to do their jobs. It means tackling the thorniest security problems that can't be solved with standalone capabilities. It means integrating security solutions up-front, instead of stitching them together later, to deliver security outcomes through systemic integrations that can't be achieved incrementally.

This leap forward into the next generation of security will be built on hybrid by design architecture, accelerated by AI, and delivered through a foundational and far-reaching strategy called platformization.

Corporate and cybersecurity leaders must rethink security strategies and restructure for resiliency.

Fragmentation leads to fragility

In response to the increased velocity and volume of cyberattacks, many enterprises have followed a common playbook for securing networks: add individual solutions as necessary, on an ad hoc basis, to address specific challenges. However, over time, this approach creates a patchwork of protection, comprised of individual solutions that are not necessarily designed to fit into a broader security strategy.

With each new layer, ad hoc systems become more complex and require more resources to operate and update. That's why the average organization finds itself engaged with more than 13 security vendors and paying for 31 different security solutions.[6]

As complexity impacts performance and costs continue to rise, three out of four organizations are pursuing security vendor consolidation, compared to only 29% in 2020.[7] Recent IBM Institute for Business Value (IBM IBV) research also focuses on the issue of complexity, with a lack of common tools across the enterprise identified by executives as a top barrier to making progress on security.[8]

3 out of 4

organizations are pursuing security vendor consolidation.

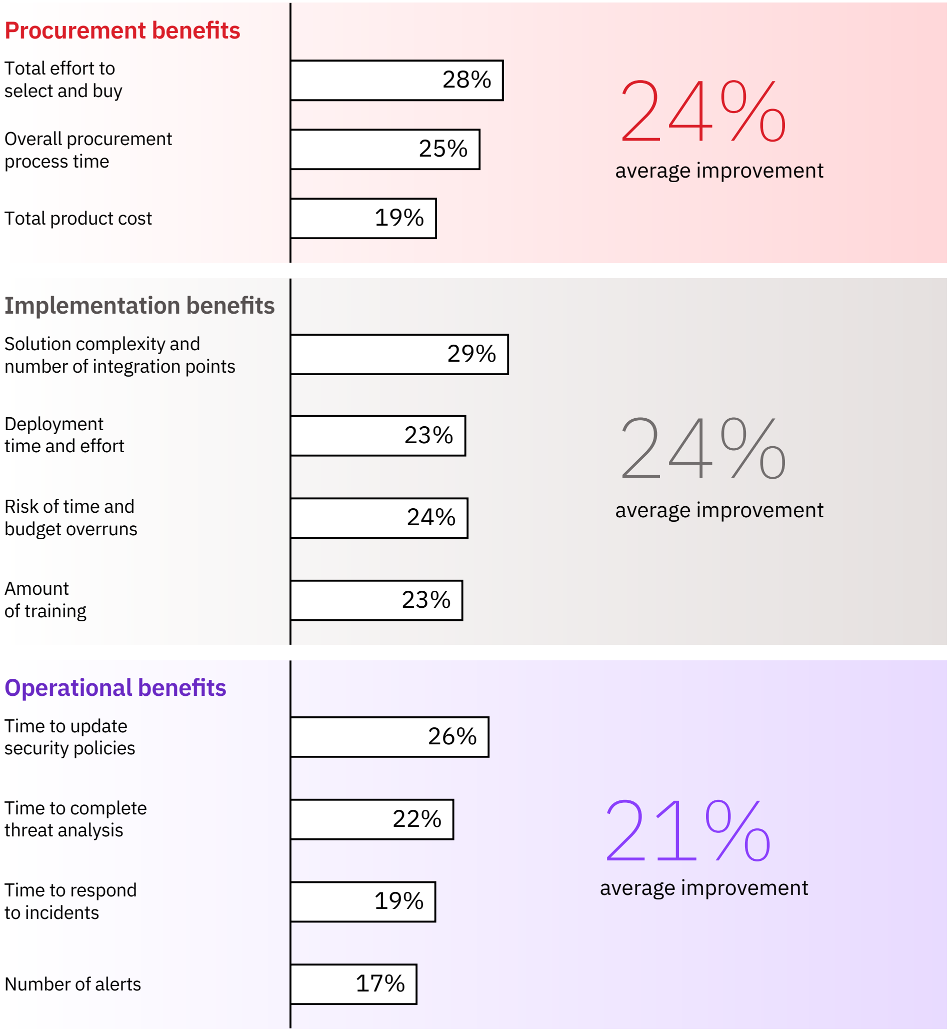
A fragmented solution landscape reflects a more fundamental issue: security is not being approached strategically. Although 86% of organizations have a security strategy, IBM IBV research found that only 35% have started executing on that strategy.[9]

And even where a cybersecurity strategy is in place, it is not adequately synchronized with wider business and technology needs. Only 52% of executives agree that their security strategy is aligned with their business strategy, and only 48% concur that their security strategy is aligned with IT strategy.[10]

The legacy of fragmentation means that the security posture of many organizations becomes increasingly reactive and tactical rather than proactive and strategic. When the security mosaic is broken into so many shards, no one has an overall view of security risk at the enterprise level. Navigating through a landscape of unknown security threats without clear, overarching insights is becoming an increasingly untenable cyber risk management strategy.

FIGURE 1

Benefits of using a platform-based approach instead of a point-based approach.



Platformization shifts the security paradigm

With the increased cadence and cunning of cyberattacks and escalating costs related to security breaches, there is an urgent need to shift from piecemeal, point-based security to a seamless, platform-based approach.

Platformization enables enterprises to simplify, amplify, and unify security efforts in ways that can’t be done when solutions initially designed for standalone deployment are improvised for integration, often in suboptimal and cost-intensive ways.

Moving forward, a strategically designed portfolio of solutions operating on a common platform is crucial for integration, enterprise-wide visibility, and easy scalability in response to emerging threats. By leveraging automation, machine learning, and AI, a consolidated cybersecurity platform can also help compensate for staff shortages and enhance the efficiency of on-site security teams.

In addition, a platform-based approach can bridge the knowledge gap that often exists when multiple vendors with incompatible products are involved, enabling security teams to focus on high-value tasks such as risk assessment and mitigation. Meanwhile, machines, digital assistants, and bots can handle routine tasks such as monitoring networks and verifying credentials.

Platformization enables enterprises to simplify, amplify, and unify security efforts.

In terms of organizational structure, platformization can demolish security silos and clear the way to deliver improved security outcomes more efficiently. Recent research by IDC finds that organizations that integrate security through a platform-based approach:

- Respond 55% faster to cyberattacks and 58% faster to remediate security events.[11]
- Operate security teams that are 34% more efficient.[12]
- Lower annualized security-related platform costs by 10%.[13]

These benefits could have significant implications for how security, managed on a unified platform, supports business operations more proactively and efficiently. In recent IBM IBV research, organizations with mature security capabilities saw a 43% higher rate of revenue growth over five years and were 69% more likely to see positive impact from security on revenue generation.[14] In pure business terms, platformization can make security an enabler and an accelerator of digital transformation and growth.

Platformization can make security an enabler and an accelerator of digital transformation and growth.

Case study

Digital-first homeownership organization adopts platformization strategy to integrate and automate security operations

Founded in 2016, Better has funded more than $100 billion in home loans, furthering its mission to transform the mortgage industry and make owning a home simpler and faster. However, along with rapid growth and the launch of new services, Better also experienced an increased tempo of cyberthreats, which increased the manual burden on security employees. And with thousands of remote employees logging in every day, the firm also had to protect an increased number of attack surfaces.

In the financial services industry, highly sensitive data and management of customer and employee accounts must be kept secure. Data security is key to building customer trust and managing compliance with state and federal regulations.

To adopt a more mature approach to threat detection and response—and automate processes to make its SOC team more effective and efficient—Better deployed an integrated platform of Palo Alto Networks solutions for network, cloud, endpoints, and security operations. Each security solution was configured to reduce friction and increase collaboration between business and engineering teams.

Today, instead of managing security solutions piecemeal from several different security vendors, Better now benefits from a unified Palo Alto Networks security platform—a scalable platform that can provide secure access from virtually anywhere, facilitate visibility and control over cloud security, and deliver substantially lower costs than its previous multivendor approach.

By decreasing incident response time, automating 90% of responses, and reducing investigation times from hours to minutes, Better’s IT team now has significantly more time to focus on security strategy and manage more complex, future-facing issues.

Turning generative AI from a security risk into a security asset with a platform-powered approach

It’s rare for 96% of executives to agree on anything, but that’s the high percentage of business leaders that see generative AI as a potential security threat.[15] They say that adopting this technology will make a security breach likely in their organization within the next three years. Consequently, 94% of executives indicate that it’s important to secure AI solutions before deployment. However, only 24% say that, within the next three months, their generative AI projects will also include a cybersecurity component. In fact, 69% of these executives prioritize innovation over cybersecurity when it comes to deploying generative AI.[16]

But what if the perception of AI changes from a security risk to a security asset? Can AI drive greater security and can security enable AI-driven innovation?

Platformization provides a more secure and efficient way to roll out new AI applications

In fact, AI can give security professionals capabilities they never had before. When coupled with a platform, AI provides a holistic and dynamic view of the entire security posture, with insights and recommendations derived from endpoints, networks, servers, cloud workloads, and security information and event management systems (SIEMs). Through historical analysis, visualizations of threat chains of events, and automated root-cause analysis, AI automates and integrates response recommendations into more streamlined workflows.

Recent research by IBM IBV found that combining AI with automation for security can increase visibility and productivity across security operations, with leading AI adopters monitoring 95% of network communications and cutting time to detect incidents by 33%. Through automation, these organizations can increase their return on security investment (ROSI) by 40% or more and can reduce data breach costs by at least 18%.[17] These cost savings provide the potential to free up funding to reinvest in the cybersecurity workforce.

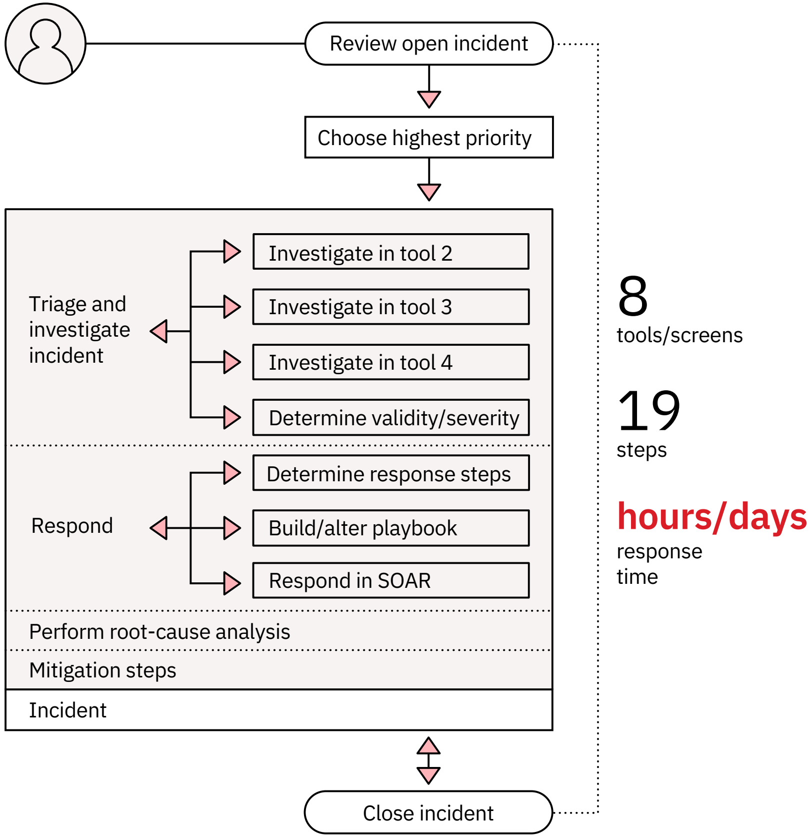
Platformization provides a more secure and efficient way to roll out new AI applications that tackle emerging threats, such as adversarial AI. Taking a platform-wide approach with AI also reinforces cyber defenses, enhances security postures, and bolsters resilience through improved threat detection and faster mitigation.

FIGURE 2

AI simplifies the user experience and accelerates security incident response

Without AI

Security analysts typical workflow complexity



Review open incident

Choose highest priority

Triage and investigate incident

- Investigate in tool 2
- Investigate in tool 3
- Investigate in tool 4
- Determine validity/severity

Respond

- Determine response steps
- Build/alter playbook
- Respond in SOAR

Perform root-cause analysis

Mitigation steps

Incident

Close incident

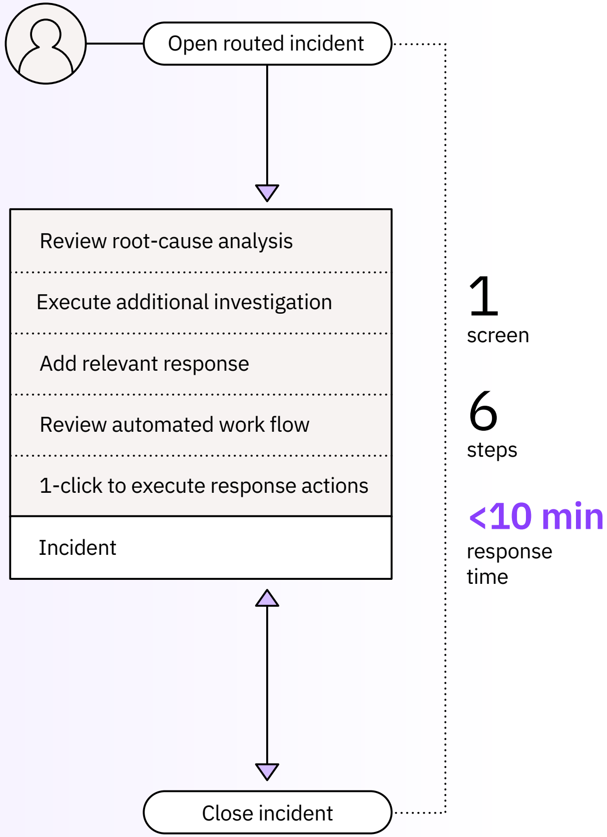
8 tools/screens

19 steps

hours/days response time

With AI

Simplified workflow with AI based XDR



Open routed incident

Review root-cause analysis

Execute additional investigation

Add relevant response

Review automated work flow

1-click to execute response actions

Incident

Close incident

1 screen

6 steps

<10 min response time

Building a hybrid and secure-by-design foundation for digital transformation

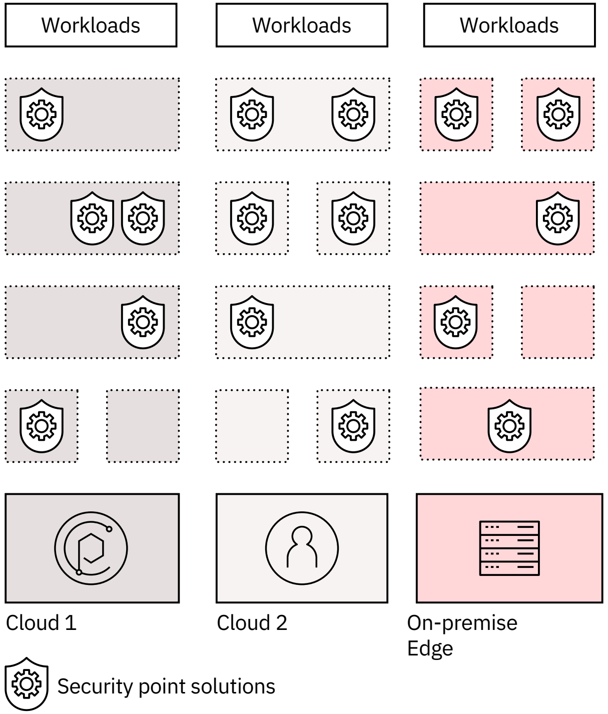
When built on a hybrid cloud infrastructure and powered by generative AI, platformization makes security a fundamental part of business transformation. As organizations pursue an open and hybrid cloud approach, they need to safeguard data across different environments without compromising the user experience. Security must be unified within a consistent posture across the entire cloud estate, as well as on-premises or edge computing, without adding layers of complexity that could bog down operations.

By weaving security seamlessly into hybrid cloud and generative AI, security platformization allows enterprises to exploit the full value of digital transformation. Platformization can encompass end-to-end, ubiquitous security, with consistent security policies maintained across all environments in a simplified manner. For example, platformization expedites the scaling of firewall onboarding and the deployment of emergency change orders across thousands of firewalls.

In short, platformization can make organizations better at security and facilitate converting opportunities into real growth. It generates greater efficiency, speed, and scale—attributes required of a better performing and more resilient organization. Organizations that understand and implement the platformization paradigm can be hybrid and secure by design and potentially have a head start on capitalizing on future opportunities.

FIGURE3

Point security architecture: Siloed and fragmented

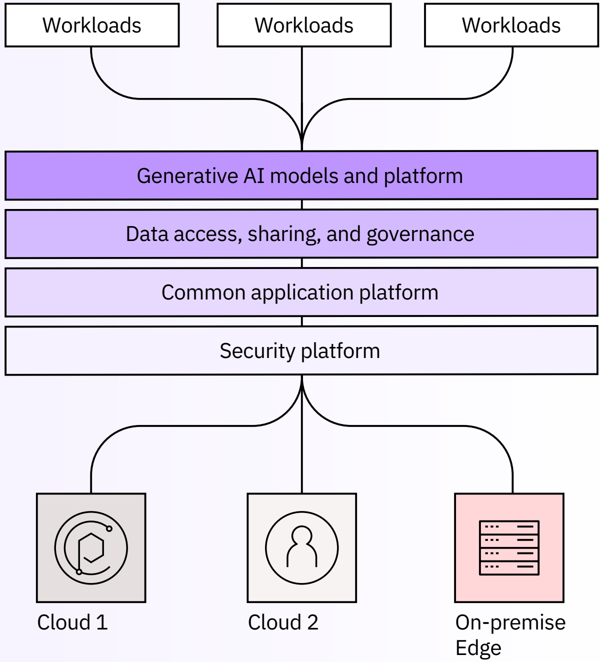


The current state

- ▷ Siloed organizations and uneven innovation
- ▷ Inefficient resource usage
- ▷ Difficult alignment across businesses
- ▷ Constrained generative AI deployment

FIGURE 4

Hybrid platform architecture: Secure by design


Workloads
Workloads
Workloads
Generative AI models and platform
Data access, sharing, and governance
Common application platform
Security platform
Cloud 1
Cloud 2
On-premise
Edge

The future state

- ▷ Secure and trusted generative AI at scale
- ▷ Rapid and secure innovation enabled by tighter IT/ IS integration
- ▷ Streamlined operations through automation and standardization
- ▷ Accelerated decisions and faster time to value

Case study

One of the world’s largest airlines reduces cybersecurity risks by modernizing cloud security architecture

When one of the world’s largest airlines decided to move applications to the cloud, it knew it would be operating in a fundamentally different cyber threat landscape. To make this digital transformation a success, the airline moved aggressively to bolster resilience against cyberattacks.

The airline chose a cloud security architecture designed for agility and a more mature security posture. The initial focus was on micro-segmentation, with a zero trust approach applied across the airline’s IT environment. This was intended to prevent intruders from accessing sensitive data or posing ransomware risks. With this solution in place, the airline gained greater visibility into cyber risks, isolated threats more quickly, and quarantined high-risk systems in real time.

The team also used a DevSecOps model to transform application development processes, increase developer awareness, and enable a more proactive approach to security.

After a year in production, the enterprise-wide security solution has accelerated digital transformation by reducing residual risks across new applications and cloud environments. With security at the core of its transformation, the airline is moving operations to the cloud more confidently and competing more effectively, with more tailored customer experiences and more efficient and cost-effective operations.

Action guide

1

Accelerate your move to next-generation cybersecurity with platformization.

Align leadership at all levels, from the board of directors to line managers, on improving enterprise-wide cybersecurity while reducing complexity, cost, and points of friction. Prioritize cybersecurity infrastructure and processes where platformization will have the most impact.

2

Empower your cybersecurity professionals to work on what matters most.

Automating routine workloads through platformization can free up time for your cybersecurity professionals to focus on high-level, strategic activities instead of manual work. Adopting a platform-first approach transforms the security mindset from reactive to proactive.

3

Adopt your zero trust strategy to support the security lifecycle.

A zero trust approach to cybersecurity is essential in today's threat landscape. This involves adopting a mindset and methodology to build security operation standards, limit threat vectors, and boost resilience. By assuming that all users and devices are potential threats, organizations can implement security measures that are designed to protect against both internal and external threats.

4

Build your case by prioritizing high return on security investment opportunities.

Look to where platformization increases security capabilities while lowering costs—such as consolidating security solutions and vendors, streamlining operations, reducing complexity, and accelerating innovation. These areas can create quick wins and serve as catalysts for larger changes to your security operating model.

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 IBM IBV's email newsletter at ibm.com/ibv. You can also 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.

Notes and sources

[1] Muggah, Robert and Mac Margolis. "Why we need global rules to crack down on cybercrime." *World Economic Forum*. January 2, 2023. https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/#:~:text=Cybercrime%20is%20big%20business.,%2410.5%20trillion%20annually%20by%202025.

[2] *Global Security Operations Center Study Results*. Morning Consult and IBM. March 2023. https://www.ibm.com/downloads/cas/5AEDAOJN

[3] *IBM X-Force Threat Intelligence Index 2024*. IBM. February 2024. https://www.ibm.com/reports/threat-intelligence

[4] *Cost of a Data Breach 2023*. IBM. July 2023. https://www.ibm.com/reports/data-breach

[5] Basu, Suswati. "Massive hack hits AI servers, exploits Ray vulnerability." *readwrite*. March 28, 2024. https://readwrite.com/massive-hack-hits-ai-servers-exploits-ray-framework-vulnerability/

[6] *Unlock the benefits of simplified security*. Palo Alto Networks. Accessed from website on April 25, 2024. https://www.paloaltonetworks.com/why-paloaltonetworks/consolidation

[7] Ibid.

[8] McCurdy, Chris, Shlomi Kramer, Gerald Parham, and Jacob Dencik. *Prosper in the cyber economy*. IBM Institute for Business Value. January 30, 2023. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/security-cyber-economy

[9] Ibid.

[10] Ibid.

[11] Dickson, Frank and Matthew Marden. *The business value of Palo Alto Networks cybersecurity platforms*. IDC. February 2024. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/idc-panw-business-value.pdf

[12] Ibid.

[13] Ibid.

[14] McCurdy, Chris, Shlomi Kramer, Gerald Parham, and Jacob Dencik. *Prosper in the cyber economy*. IBM Institute for Business Value. January 30, 2023. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/security-cyber-economy

[15] *The CEO's guide to generative AI/Cybersecurity*. IBM Institute for Business Value. October 30, 2023. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ceo-generative-ai/cybersecurity

[16] Muppidi, Sridhar, Lisa Fisher, and Gerald Parham. *AI and automation for cybersecurity*. IBM Institute for Business Value. July 20, 2022. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-cybersecurity

[17] Ibid.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | May 2024

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an "as is" basis and IBM makes no representations or warranties, express or implied.