IBM Institute for Business Value | Research Brief

Capturing the cybersecurity dividend in banking

How security platforms generate business value

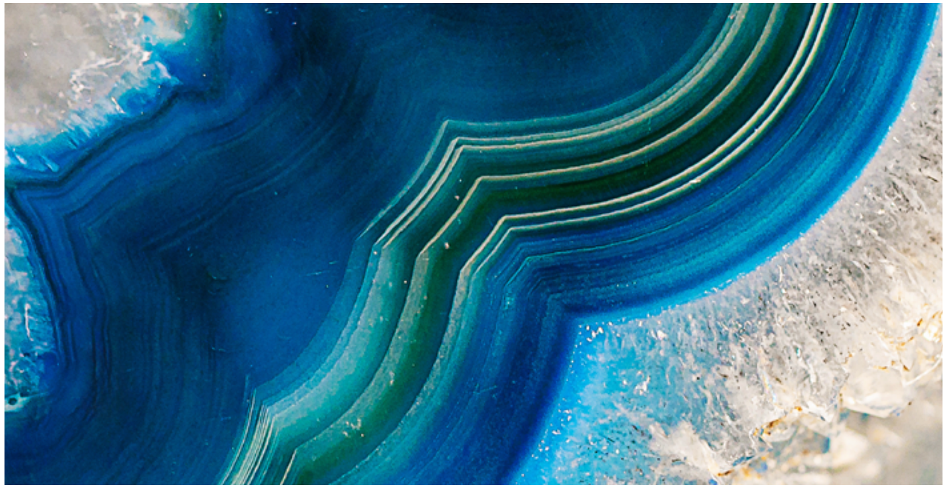
IBM | paloalto NETWORKS

How IBM and Palo Alto Networks can help

IBM Consulting and Palo Alto Networks have joined forces to deliver AI-powered, fully integrated, open, end-to-end security solutions to enterprises. From consultation through execution, we can help you modernize your cybersecurity program, saving time, money, and resources as well as enhancing your organization's resilience against today's complex threats. For more information, visit ibm.com/consulting/palo-alto.

Key takeaways

Almost half—47%—of banking executives say complexity is the biggest impediment to security operations.



Security fragmentation is now the unhappy norm.

Banks juggle an average of 114 different security solutions from 42 vendors. Almost half—47%— of banking executives say complexity is the biggest impediment to security operations.

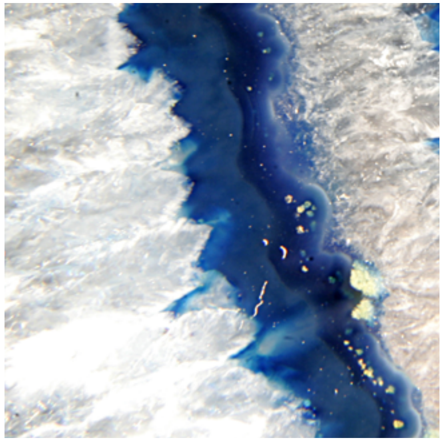
Security platforms bring faster response times and higher ROI.

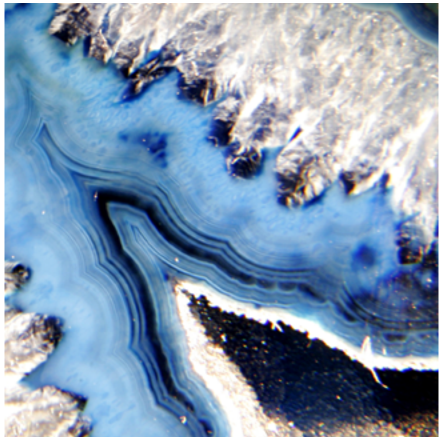
It takes platformized financial institutions 53 days less, on average, to detect a security incident and 55 days less to contain one. They also reap an average ROI of 118%, compared to 45% for those that are not yet embracing platformization.

Platformization moves the security function from "necessary cost" to value generator.

97% of banking executives in our survey who have adopted platformization say security is a source of value, compared to just 43% of those who haven't.

Complexity is the enemy of cybersecurity





As the digital landscape continues to change, financial institutions face a daunting reality: cybersecurity complexity is eating away at their bottom line.

Our research shows that banks juggle an average of

114

different security solutions from

42

vendors.

In today's interconnected world, complexity is the enemy of security, and that translates directly into financial exposure. This isn't just an IT problem; it's a business issue.

Why? Because cybersecurity complexity not only obscures financial institutions' ever-important risk exposure, it actually elevates the cost of their risk. Yet, the banking industry's ability to navigate financial and economic uncertainties hinges on effective risk management and security capabilities that update continuously; a faulty security posture brings increased risk.

Financial institutions that use integrated security platforms (platformization) to reduce that complexity are seeing better security and better ROI. But first, let's take a closer look at the state of cybersecurity in banking—and how it's impacting balance sheets.

Every customer touchpoint is a security conversation

The pandemic accelerated the digitalization of financial services, sweeping clients into a new wave of digital banking and open finance. Banks' architectures, though, were not built for this digital tsunami. And the gap has widened further, touching on the very core foundations of banking trust–ensuring client funds are secured. Every customer touchpoint, therefore, is not just a business conversation—it's also a security conversation.

The challenge (and the opportunity) for financial institutions is that cybersecurity is more expensive than ever. The banking sector now ranks second—only behind healthcare—in the cost of data breaches, with each incident averaging nearly $6.1 million.[1] However, it's the mega data breaches, involving over one million records, that have a truly devastating financial impact. Costs range from an average of $42 million for one million compromised records to $375 million for breaches of 50-60 million compromised records.[2]

A typical response to a growing threat landscape is more security solutions—which can lead to security sprawl. With this approach, a financial institution's security costs rise significantly, with cybersecurity spending in the banking industry expected to grow 47% from 2023 to 2025. Meanwhile, 95% of banking executives agree they face pressure to reduce the cost of security. Against this backdrop, new cybersecurity regulations around the world are adding to the pressure on financial institutions, with increased responsibilities for reporting, customer reimbursement, and more.

Banks' tech legacy is holding them back

The industry's resilience against financial uncertainties is being tested by its own technological legacy. Financial institutions have accumulated security products and services over time on a tool-by-tool basis. Each has its own dashboards, data models, training needs, and more. This creates a tangled, expensive mess that frustrates security professionals and hinders overall effectiveness.

118%

Average security investment ROI for banks that platformize

45%

All others

> "We value our customers and understand how important cybersecurity is to enable them to enjoy our services with peace of mind."
>
> —Maximiliano Damian Rodrigues, General Manager SME Business, Nubank[6]

What integrated security platforms can do for security and ROI

The illusion that more solutions equate to more security is just that—an illusion. Every integration is a potential point of entry for bad actors. If banks instead consolidate their security into an integrated platform, our research with 1,000 executives across 21 industries (including 140 in banking) and 18 countries shows it would improve cybersecurity. It takes platformized banks 53 days less, on average, to detect a security incident and 55 days less to contain one. And that's just the beginning of the benefits for platformized organizations. From ROI to relief for overloaded security operators, organizations that platformize are seeing much better results than those who don't.

Amidst this complexity, a unified security framework emerges as the most valuable investment for driving business outcomes, according to 45% of CIOs and CTOs.[3] Yet, a stark paradox emerges: while 84% of banks boast meticulously crafted security strategies, only 39% can claim to truly wield them effectively.[4] The chasm between ambition and execution needs to be bridged successfully and platformization can help financial institutions do just that.

This report sheds light on how platformization can help banking executives deal with the pressing issue of cybersecurity, using platforms for simplification and integration. We offer insights and recommendations tailored for banking's C-suite and security technology executives—the architects of change in a volatile financial security landscape.

> "A change of mindset—of culture—is paramount [to succeed with embedded finance]. All colleagues must understand the reason for what we do, how to constantly do it, and how to do it with security."
>
> —Maria Cristina Arrastia Uribe, former Business Vice President, Bancolombia[7]

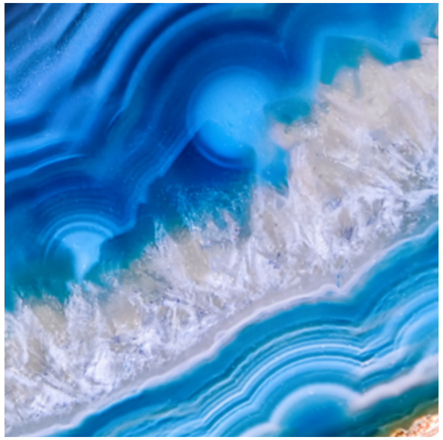
Cybersecurity has always been important. Here's why it matters to banks more than ever right now.

Cracks in the system. Once bastions of impregnable security, banks now face new online banking operational complexities, exacerbated by imperfect cloud migrations and burgeoning vulnerabilities in AI-based systems. Additionally, multiple SaaS vendors and an increasingly complex financial services supply chain increase a bank's attack surface--adding to breach vulnerability. And as open finance throws the doors wide open, the interconnected web of dependencies grows ever more tangled. This combination of circumstances has elevated cybersecurity to a top-tier priority in many banking C-suites.

As banks venture deeper into cloud platforms and intertwine their operations with external partner networks, their vulnerability to data breaches has never been greater.

The targeting of cloud-based data. But it's the "mega-breaches"—those monstrous attacks compromising over a million records—that truly threaten to incapacitate banks. Complicating the situation, cyber criminals are now meeting banks on the very frontier where the industry is aggressively expanding its digital horizons: 82% of last year's breaches targeted cloud-based data.[5]

Cybersecurity should boost the bottom line



The illusion of "more solutions, more security"

Many organizations have continued to add to their stable of security solutions, hoping to plug holes as they become apparent and as threats increase.

The average cost of security complexity is

6%

of annual revenue for banks.

But our research shows this approach is not a path to success—instead, it adds complexity and inefficiency. There's a limit to how far you can get by adding more security solutions. That strategy gradually dilutes the benefits of each new solution and ultimately reduces security effectiveness.

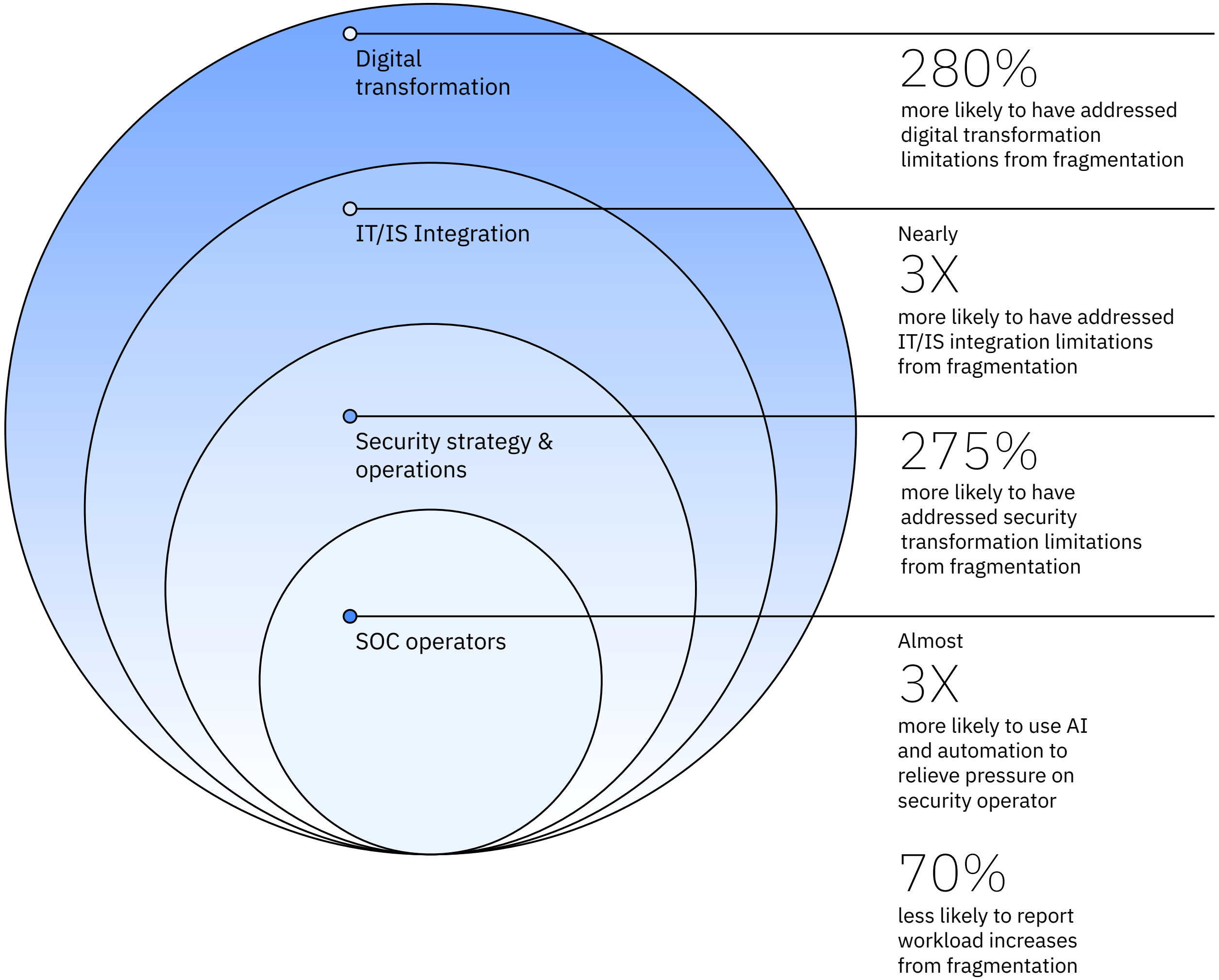
Tellingly, 47% of banking executives say complexity is the biggest impediment to their cybersecurity operations. When asked to estimate the total impact of security complexity to their business, responses from banking executives on the security front line were startling. Based on their responses, the average cost of security complexity is 6% of annual revenue. For a company with $20 billion in annual revenue, that's more than $1 billion in annual cost to the business resulting from security incidents, inefficiencies, failed digital transformation efforts, stalled AI initiatives, loss of customer trust, and reputational damage.

An antidote to the costs of security complexity

By addressing complexity—strategically consolidating and integrating security solutions onto a common platform—organizations can dramatically lower their risk posture, reduce their costs, and unlock improved business opportunities. Our research shows a distinct connection between platformization and positive business as well as security outcomes (see Figure 1).

Figure 1

Platforms bring practical benefits at all levels



280%
more likely to have addressed digital transformation limitations from fragmentation

Nearly
3X
more likely to have addressed IT/IS integration limitations from fragmentation

275%
more likely to have addressed security transformation limitations from fragmentation

Almost
3X
more likely to use AI and automation to relieve pressure on security operator

70%
less likely to report workload increases from fragmentation

How we analyzed the impact of security platforms

To assess the role of security platformization in overall security and business performance, we analyzed the 140 banking organizations in our survey set. We developed an index of security platformization based on four key criteria:

1. **Simplification.** How great a role does consolidation play in security strategy?
2. **Portfolio rationalization.** How consolidated are security tools and technologies?
3. **Proactive housekeeping.** How well and regularly are outdated security solutions identified and removed?
4. **Platforming progress.** To what extent are security platforms adopted?

For each of the four areas, executives answered a scaled question assessing their progress. The platformization index was created as a simple average of their scores on each of the four.

Throughout this report, we illustrate the relationship between platformization index scores and performance by segmenting the survey respondents into quartiles based on their index scores. The top quartile refers to the organizations with the highest platformization index scores, while the bottom quartile consists of the organizations with the lowest platformization index scores.

Key takeaways from the analysis

Our analysis reveals a strong correlation between the platformization index and key security performance metrics. Organizations with higher platformization scores demonstrate:

- **Faster incident response.** Platformized organizations take 53 days less, on average, to detect a security incident, and 55 days less to contain one.
- **Improved ROI on security investment.** An average ROI of 118% compared to 45% for those that are not yet embracing platformization.

In short, the data indicates security platformization helps drive improved performance and optimizes the value of security investments.

Security platforms: A business performance boost

Rethinking risk

Think about a financial institution with multiple branches. Each operates independently, using its own strategies, processes, and technologies.

While each branch might be efficient locally, operating without a centralized plan and shared resources leads to a lack of coordination for the larger banking institution. The lack of coordination can create delays, inefficiencies, and security gaps.

Security platformization is the equivalent of unifying the construction under a single general contractor, with standardized equipment and procedures. Platformization eliminates unnecessary repetition of work, simplifies operations, and empowers security teams to focus on strategic initiatives.

> "While embedded finance does necessitate technological innovation, it's not solely about driving technology. It's more about how technology can bolster the strategies of different business units. The real enabler was rethinking our approach with the business lines, figuring out how to be more open, deciding which APIs to expose, and ensuring platform security."
>
> —Jorg Fischer, Group CIO, Standard Bank[8]

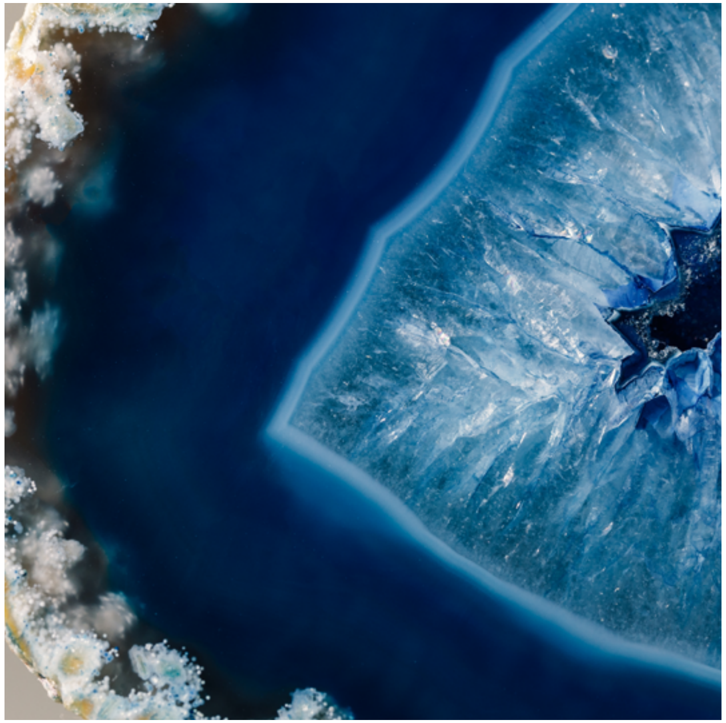
The benefits are compelling. A majority–69%–of platformization adopters in our research say they have full visibility into potential vulnerabilities and threats, versus only 21% of non-adopters.

Revenue generation and efficiency

Security platformization can further business goals. In fact, in our research, more than six out of 10 banking organizations with a high degree of platformization report that cybersecurity investments have helped revenue generation and operational efficiencies. Less than one in 10 of executives from banking organizations that have yet to move toward platformization say the same (see Figure 2).

This advantage comes in part from enhanced agility. Many digital transformation efforts can be derailed by security concerns. Yet among platform users, less than 8% of digital transformation initiatives fail to scale due to security concerns compared to more than 17% for non-platform users.

That helps transform security from a cost center to a value driver. In fact, 97% of banking executives in our survey who have adopted platformization say security is a source of value, compared to just 43% of those who haven’t.



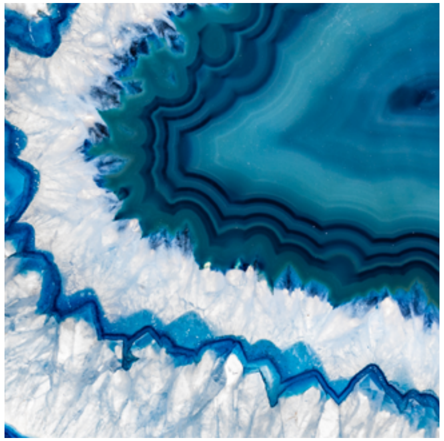
Building a bridge between information technology and information security

Traditionally, information technology (IT) and information security (IS) have operated in separate silos with different priorities and responsibilities.

Platformized organizations take

53 days less, on average, to detect a security incident, and

55 days less to contain one.



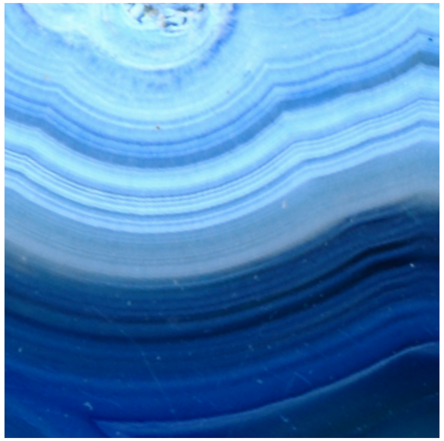
The move to platformization makes security operations an integral part of the broader IT estate—as much a contributor as a consumer.

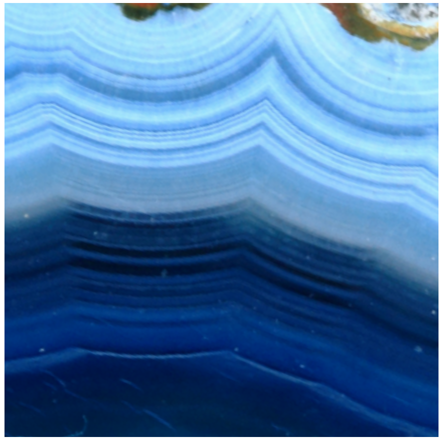
This is where data security comes into play. A platform helps because the more connected your data is, the more visible it is and the easier it is to surface it. This helps boost efficiency because it helps to integrate workflows. And all of these combined factors help a financial institution detect security breaches faster and respond with more speed.

Our research shows that 60% of organizations without a unified platform struggle with fragmentation. The lack of cohesiveness for companies that have not adopted platformization can make them vulnerable to potential threats simply because they lack visibility and awareness.

Bridging the gap between IT and IS with a security platform can shift organizational focus from risk aversion to value creation, transforming potential threats into opportunities for innovation and growth. The more teams embrace the use of common platforms and services, the less time they waste getting everyone on the same page. And leaders can spend less time negotiating standards and governance and devote more energy to achieving goals.

Streamlined security strategy and operations





The security operations center (SOC) is the beating heart of cybersecurity, but only 59% of banking organizations believe their current security operating model is effective.

By reinforcing better ways of working, platforms can drive efficiency and visibility. In fact, all banking organizations with a mature approach to platformization agree their security processes are efficient and clear.

Banking organizations that tap platformization also spend less on cybersecurity as a percentage of their IT budget than others. But they achieve much greater impact with their spend, seeing an average ROI 159% higher than non-adopters.

Platforms can aid efficiency by easing workload demands on security operators and freeing up human capital for transformation efforts and other digital advances. While four out of five non-platform users agree their security operators cannot deal effectively with the sheer quantity of threats and attacks, only one in five platform users think the same.

While 4 out of 5 non-platform users agree their security operators cannot deal effectively with the sheer quantity of threats and attacks, **only one in five** platform users think the same.

Case study

Australian bank jettisons legacy tech for zero-trust platform

The challenge

A Fortune 500 Australia-based multinational bank relied on a complex mix of outdated technologies that made it vulnerable to cybersecurity threats—an untenable situation for a highly regulated financial institution with more than 1,100 branches and 55,000 users worldwide. This caused unnecessary frustration for the IT team, as well as end users; it took up to 12 hours to resolve basic app issues. The bank also struggled to support remote work when the pandemic hit, specifically around user access to applications.

The solution

The enterprise embarked on a zero-trust journey to strengthen security and optimize user experience. Zero trust is essentially security wrapped around every user, every device, and every connection—every time. Based on the concept of "never trust and always verify," zero trust is a cybersecurity model that verifies each connection between users, devices, applications, and data, instead of trusting the network perimeter.

The platform the bank adopted as part of its zero-trust journey empowers the bank to provide customers quality financial services and confidence their assets are secure.

The bank deployed a network-security platform to transform zero-trust principles into solutions and put the organization at the forefront of digital innovation. The bank started with physical firewalls at branch offices for segmentation and financial compliance. When the pandemic hit, the company rapidly deployed Secure Access Service Edge (SASE—a cloud-based network architecture that combines security and networking services) to protect users working from anywhere and deliver quality app performance. Finally, it layered on security services for deeper traffic inspection and data loss prevention.

Now, the bank's productive workforce can serve more customers globally with the assurance that their personal and financial data is protected. The IT team can easily identify and secure digital transactions involving General Data Protection Regulation (GDPR) data and personally identifiable information (PII), troubleshoot issues from a centralized console, and scale capacity up or down as needed—all without sacrificing zero-trust security controls.

As the next step, the bank is expanding its use of branch firewalls with a zero-trust framework to strengthen security with further segmentation.

Results

Nearly

50%

increase in internal app scores based on performance, troubleshooting time, and user ratings.

>40%

decrease in trouble tickets raised due to performance issues.

97%

increase in detection accuracy of sensitive data.

AI-fueled security platforms are supercharging security teams

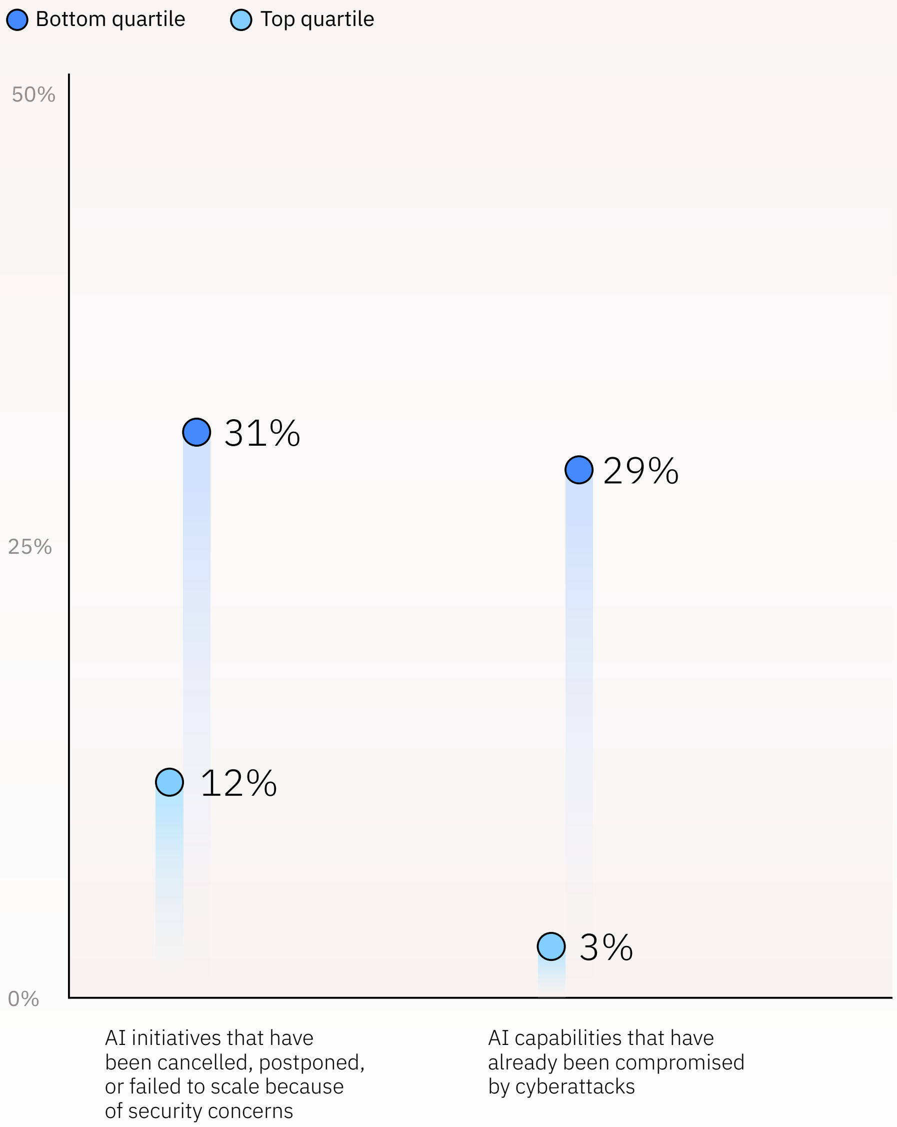
Today’s cyberthreats are too complex and too fast-moving for reactive security. To stay ahead, organizations need a proactive, intelligent, AI-fueled defense.

“We are trying to establish a strategy connecting our cloud, AI, and security operations. We have to design for cybersecurity from the beginning. Using automation helps our analysts focus on higher-value work. We can use AI to deliver better security outcomes.”

—Javier Torres Alonso, Chief Information Security Officer, Allfunds

Figure 2

Banking organizations that move to platformization are better able to secure their AI and execute on their AI agenda



Our research shows security platformization users are better able to tap this potential. It unifies data to help uncover the source of emerging threats and provides operators with near-instantaneous visibility and responsiveness. Our analysis reveals that organizations using platformization are far less likely to report fragmentation and lack of transparency among their security teams. In contrast, 69% of organizations with low platform adoption indicate their security analysts' performance is hindered by a lack of visibility and transparency.

A security platform can also help protect and advance additional AI business initiatives throughout the organization. Approximately nine out of 10 executives in our research agree that adopting security platforms will improve AI operations across the enterprise.

> "The more the market grows [with embedded finance], the more security, compliance, and high-quality accessibility become key and differentiating attributes. And that is what we target."
>
> —Fernando Freitas, Head of Innovation, Bradesco

Action Guide

The next systemic crisis might not be financial in nature—but originate from the very systems that keep our money moving.

Think cyberattacks, data breaches, and the chaos that ensues when technology fails.

As banks increasingly rely on tech-savvy startups and nontraditional partners, their digital defenses are one of their most valuable assets.

Instead of just trying to avoid disaster, imagine a future where security actually fuels innovation.

Here are six key actions to take to use platformization to your best advantage:

1

Reduce complexity by rationalizing your security toolset. Establish a working group with your security, technology, and business leaders to evaluate the impact of security complexity on key performance metrics. Conduct a comprehensive security toolset assessment, including a cost-benefit analysis of each tool. Identify redundancy, gaps, and opportunities for consolidation or replacement.

2

Pivot to a platform-first approach. Engage the right partner to build a business case for security platformization. Prepare a board-level briefing on operational benefits and cost savings to gain C-suite buy-in. Create a roadmap for scaling your security platform. Stage incident-response drills to assess where a unified platform can deliver the greatest impact.

3

Build a unified security framework. Implement a unified security controls framework to streamline interoperability across monolithic systems, public clouds, private clouds, and hybrid architecture.

4

Update regulatory compliance approaches. Revamp the risk and control framework, integrating AI into all risk and compliance policies, to build a trusted operational environment both within the bank and beyond banking borders.

5

Focus on collaborations that drive simplicity. Enhance your security strategy by forging strong partnerships with trusted vendors and advisors. Critically assess current and potential partners based on technology offerings, as well as services and capabilities.

6

Visit a cyber range to assess how AI threats are evolving and use it to support the transformation of your security operating model with platformization. Engage a preferred managed security services partner (MSSP) to accelerate your AI transformation.

Banks and cybersecurity: A critical crossroads

In conclusion, while banks acknowledge the growing importance of cybersecurity, many struggle to translate strategy into effective execution. This is due in part to the ever-increasing complexity of the cybersecurity landscape, which is further exacerbated by security sprawl. The answer lies in platformization: consolidating security tools into a unified framework that simplifies operations, reduces detection and containment times, and delivers a significantly higher return on investment. By embracing a platform-based approach, banks can continue to bridge the gap between ambition and execution to achieve their cybersecurity goals.

> "As a financial institution, our regulations are strict, probably more than most industries. It's better if we can cover our risk and regulatory requirements using a single platform. Here in Europe, we have new regulations like the Digital Operational Resilience Act (DORA). Our teams need more time to understand how we should address these new requirements."
>
> —Javier Torres Alonso, Chief Information Security Officer, Allfunds

Authors

Leah Generao

Partner, IBM Security Consulting

Leah.Generao@ibm.com

https://www.linkedin.com/in/leah-gregorio-generao-27050a13/

Paul Leonhirth

Managing Director, Global Financial Services Industry, Palo Alto Networks

pleonhirth@paloaltonetworks.com

https://www.linkedin.com/in/pleonhirth/

Research methodology

New data and findings in this paper are from a recent survey conducted by IBM Institute for Business Value in collaboration with Oxford Economics. From July through September 2024, 1,000 executives across 21 industries (including 140 from banking and financial markets) and 18 countries were surveyed. In addition to descriptive analysis, we analyzed data from the executives to facilitate the creation of a "platformization index." This index measures the extent to which an organization has moved toward security platformization. Based on the index, regression analysis was conducted to ascertain the relationship between security platformization, and security and business outcomes. In addition, moderator and mediator analysis was conducted to understand how platformization interacts with other capabilities in supporting security outcomes. To facilitate the presentation of our data analysis, we segmented results from the platformization index into quartiles showing the extent of security platformization progress. These quartiles were used to further understand differences in performance as well as practices and approaches for enabling next generation cybersecurity.

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 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

Unify your fragmented security: Accelerate transformation with platformization

IBM Institute for Business Value. May 2024.

https://ibm.co/next-gen-platform-cybersecurity

Architecting for AI agility: How hybrid by design can help tech architectures accelerate business outcomes

IBM Institute for Business Value. July 2024.

https://ibm.co/hybrid-by-design-agiletech- architecture

***6 blind spots tech leaders must reveal: How to drive growth in the generative AI era* (Tech CxO study)**

IBM Institute for Business Value. August 2024.

https://ibm.co/c-suite-study-ceo

2025 Global Outlook for Banking and Financial Markets: Elevate banking performance in the age of AI

IBM Institute for Business Value. January 2025.

https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-banking-financial-markets-outlook

Notes and sources

1. *Cost of a Data Breach Report 2024*. IBM Security. July 2024. https://www.ibm.com/reports/data-breach
2. Ibid
3. Ramamurthy, Shanker, John J. Duigenan, Hans Tesselaar, and Paolo Sironi. *Foundations for banking excellence. Practices and priorities to accelerate digital transformation*. IBM Institute for Business Value in collaboration with BIAN. October 2022. https://ibm.co/foundations-banking-excellence
4. McCurdy, Chris, Shlomi Kramer, Gerald Parham, and Jacob Dencik, PhD. *Prosper in the Cyber Economy: Rethinking cyber risk for business transformation*. IBM Institute for Business Value. November 2022. https://ibm.co/security-cyber-economy
5. *Cost of a Data Breach Report 2024*. IBM. July 2024. https://www.ibm.com/reports/data-breach
6. Sironi, Paolo, Diane Connelly, and Connor Loessl. *The voice of the makers: Banking for small and medium enterprises*. IBM Institute for Business Value. October 2024. https://ibm.co/sme-banking-makers
7. Sironi, Paolo, Diane Connelly, and Connor Loessl. *The voice of the makers: Embedded finance*. IBM Institute for Business Value in partnership with BIAN. October 2023. https:// ibm.co/embedded-finance-makers
8. Ibid
9. Ibid

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | February 2025

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.

1227cc9cfb4b9c3a-USEN-01