Capturing the cybersecurity dividend in telecoms

How security platforms generate business value

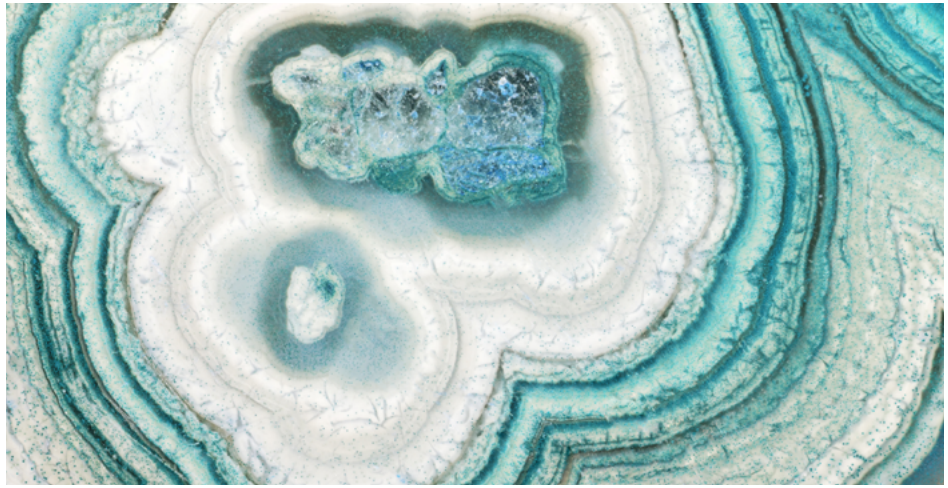
IBM | paloalto NETWORKS

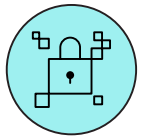
How IBM and Palo Alto Networks can help

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

More than half—57%—of telecom executives say complexity is the biggest impediment to security operations.





Security fragmentation is now the unhappy norm.

Communications service providers (CSPs) juggle an average of 107 different security solutions from 39 vendors. More than half—57%—of telecommunications executives say complexity is the biggest impediment to security operations.

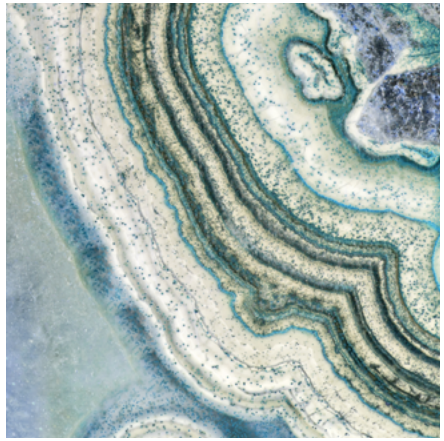
Security platforms bring faster response times and higher ROI.

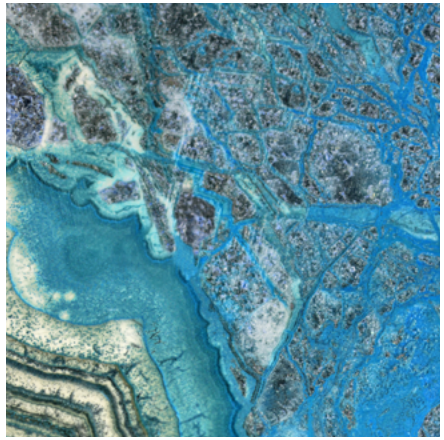
It takes platformized CSPs 43 days less, on average, to detect a security incident and 36 days less to contain one. They also reap an average ROI of 108%, compared to 43% for those that are not yet embracing platformization.

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

All of the telecommunications executives in our survey who have adopted platformization say security is a source of value, compared to just 10% of those who haven’t.

Cybersecurity should boost the bottom line





As the digital landscape continues to change, communications service providers (CSPs) face a daunting reality: cybersecurity complexity is eating away at their bottom line.

CSPs juggle an average of

107

different security solutions from

39

vendors.

Our most recent research shows that CSPs juggle an average of 107 different security solutions from 39 vendors, creating a tangled, expansive mess that frustrates security professionals and hinders overall effectiveness. A majority of telecommunications executives (57%) say complexity is the biggest impediment to their cybersecurity operations.

In addition, cybersecurity is more expensive than ever; the average cost of a breach involving more than 50 million records is $375 million.[1]

CSPs have added more security solutions to manage a growing threat landscape. But this approach has caused their overall security costs to rise significantly. Telecommunications executives estimate their cybersecurity spending has grown 41% from 2023 to 2025. Meanwhile, 87% of telecom executives agree they face pressure to reduce the cost of security.

The good news is, CSPs that platformize (move toward a single integrated security platform) to reduce complexity are seeing better cybersecurity and better ROI.

What integrated security platforms can do for security and ROI

As the threat environment grows more complex (see “The digital tightrope” on page 6), transitioning from reactive to proactive security is crucial. Leading-edge CSPs are adopting cloud-based and AI-powered solutions that enable continuous threat monitoring.

When CSPs infuse proactivity by using an integrated security platform, they see dramatic improvements in performance and cost. Our research findings from 1,000 executives across 21 industries and 18 countries—including 60 telecommunications leaders—shows security platforms improve cybersecurity key performance indicators (KPIs) and ROI.

Platformized CSPs take 43 days less, on average, to detect a security incident, and 36 days less to contain one. They also reap an average ROI of 108% compared to 43% for those that are not yet embracing platformization.

Security is no longer just about protection—it is a strategic asset that underpins innovation, customer trust, and regulatory compliance—the essential drivers of growth in the digital era.

43

days less, on average, to detect a security incident

36

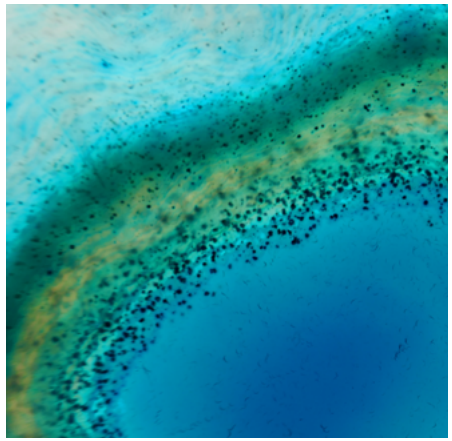
days less to contain one

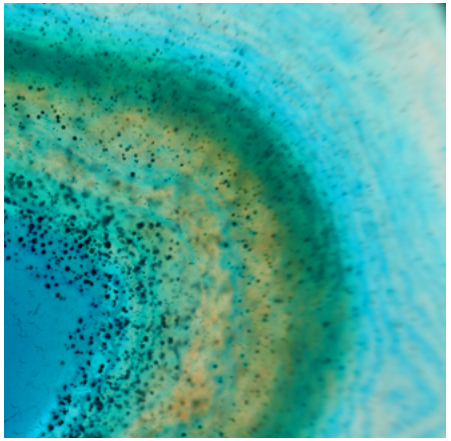
108%

average ROI for platformized CSPs

43%

all others





The digital tightrope
Telecom's high-stakes efforts against cyber threats

CSPs are the guardians of vital infrastructure, but this crucial role makes them prime targets.

The chilling reality is the threats are increasing: in late 2024, US officials disclosed that nine US telecommunications companies had been targeted by a nation-state sponsored hacking campaign of unprecedented scale and sophistication.[2] More than half of CSPs (55%) experienced a breach over the past year.[3]

In 2024 alone, telecom operators across the US, Europe, and Asia experienced high-profile security breaches that exposed regulatory gaps and operational vulnerabilities.[4]

Indosat's Senior Vice President of Technology Strategy Enterprise Solutions, Amit Kumar, described the actions his company is taking to address today's security challenges, in a recent interview with the IBM Institute for Business Value (IBM IBV): "Over the past two years, cybersecurity has become a significant focus, driven by public data breaches like the Optus incident and similar issues in Indonesia, which negatively impacted customer trust NPS [net promoter satisfaction] scores. Previously, our cybersecurity was decentralized, with each division managing its own needs.

Following these events, Indosat has implemented a centralized cybersecurity pillar, ensuring a unified approach to detection, response, and backup security. This shift has led to increased cybersecurity spending and a more coordinated strategy. Additionally, the introduction of PDP [personal data protection] regulations by the Indonesian government has heightened the focus on protecting customers' identifiable data, requiring stricter measures for database security and internal processes. The combined impact of global data leaks and local regulations has put cybersecurity under the spotlight, driving ongoing improvements."

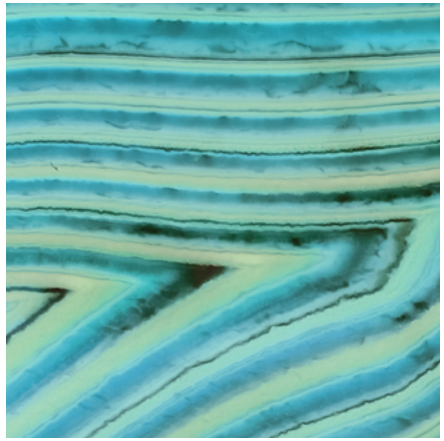
The impact of 5G and cloud on cybersecurity

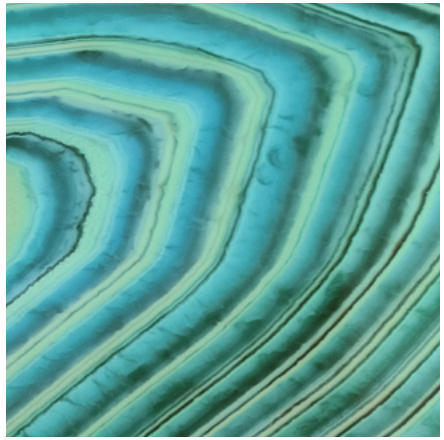
5G's speed and reach, along with highly distributed cloud-native architectures, have revolutionized connectivity, but also blown up the old cybersecurity playbook. The combination of connected devices, increased digitization, and complex networks creates a breeding ground for vulnerabilities, demanding a new security paradigm built on collaboration and shared responsibility.

Network security? A top concern. Security audits? Infrequent.

Despite 42% of executives ranking security as a top concern, surprisingly few (36%) conduct quarterly audits, and 21% do so just twice per year, leaving critical infrastructure vulnerable for extended periods.[6]

The illusion of “more solutions, more security”





Many organizations have continued to add to their stable of security solutions, trying to plug holes as they become apparent and as threats increase. But our research shows this approach is not a path to success—instead, it adds complexity and inefficiency.

> The average cost of security complexity for a CSP is more than
>
> 6%
>
> of annual revenue.

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.

So what is the solution? Where is there opportunity, what models exist, and what lessons can they teach? The results of our research provide some clear opportunities and actionable lessons.

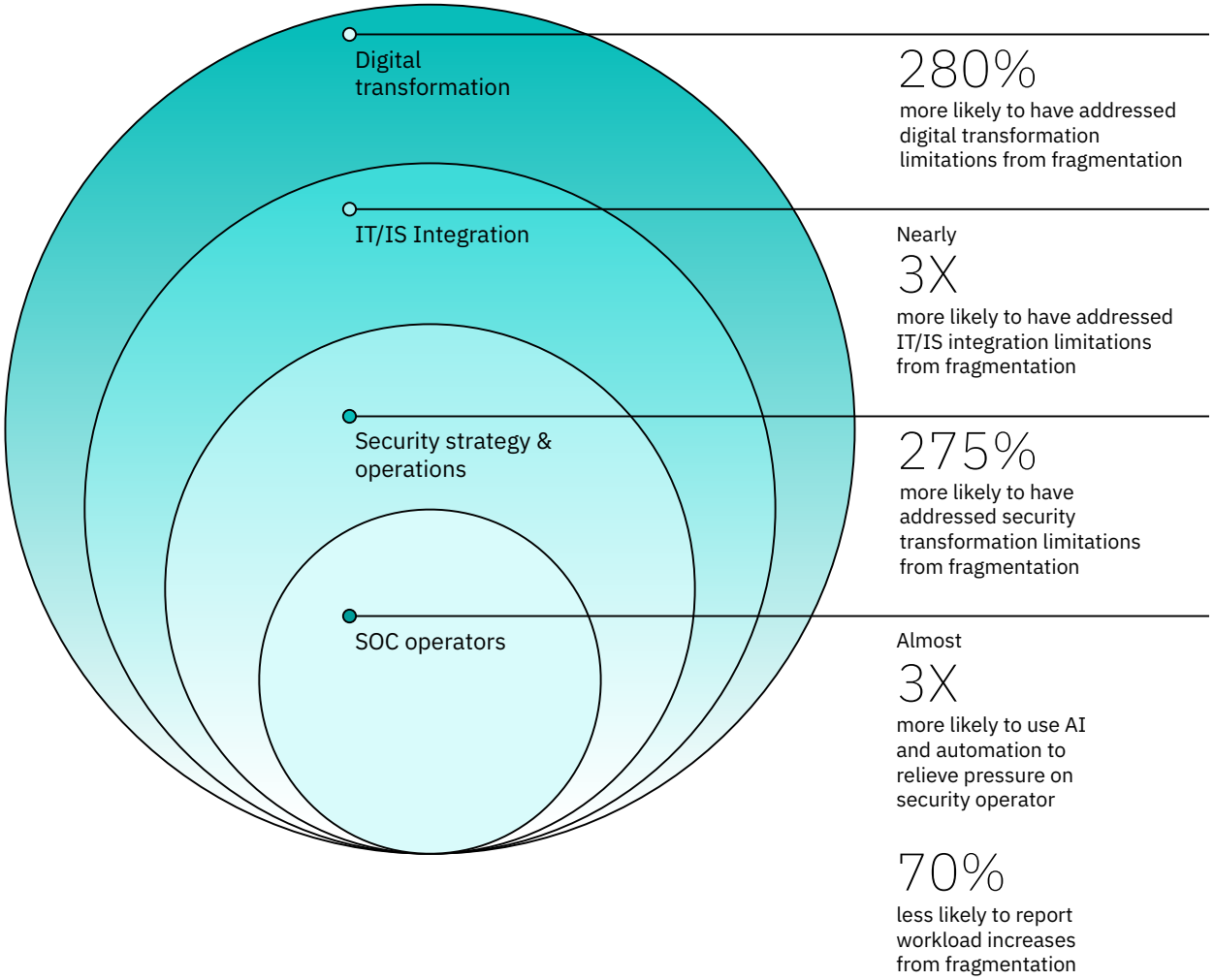
When asked to estimate the total impact of security complexity to their business, responses from telecom executives on the security front line were startling. Based on their responses, the average cost of security complexity for a CSP is more than 6% of annual revenue. For a company with $20 billion in annual revenue, that’s more than a $1-billion 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. We call this security platformization—and our research shows a distinct connection between platformization and positive business and security outcomes (see Figure 1).

Figure 1

Platforms bring practical benefits at all levels



"Indosat manages a vast network of 56,000 sites, hundreds of thousands of routers, and various endpoints such as laptops, iPads, and devices in data centers. Each of these endpoints is treated as a potential entry point into the network, ensuring that all are carefully monitored and observed as part of the comprehensive cybersecurity strategy."

Amit Kumar, Senior Vice President
Technology Strategy Enterprise Solutions, Indosat

How we analyzed the impact of security platforms

To assess the role of security platformization in overall security and business performance, we analyzed the 60 CSPs 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 criterion, 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 criteria.

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.

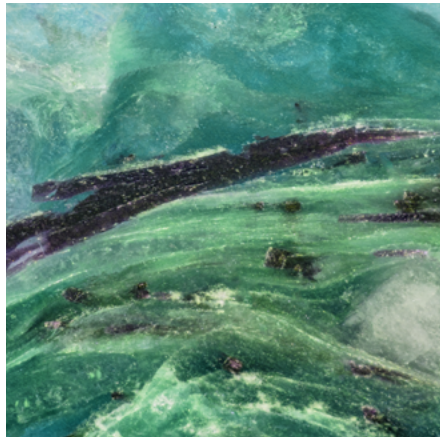
Key takeaways from the analysis
Our analysis reveals a strong correlation between the platformization index and key security performance metrics.

Organizations with higher platformization scores demonstrate:

- **Faster incident response.** Platformized organizations take 43 days less, on average, to detect a security incident, and 36 days less to contain one.
- **Improved ROI on security investment.** An average ROI of 108% compared to 43% for those that are not yet embracing platformization.

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

Security platforms
A business performance boost



Rethinking risk

Think about a large construction project with multiple contractors, each using their own tools, materials, and blueprints.

While each contractor might be skilled, coordinating their efforts without a unified plan and shared resources can lead to delays, inefficiencies, and potential safety hazards.

The current state of cybersecurity is similar. Organizations 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. Our research shows that CSPs juggle an average of 107 different security solutions from 39 vendors, creating a tangled, expansive mess that frustrates security professionals and hinders overall effectiveness.

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.

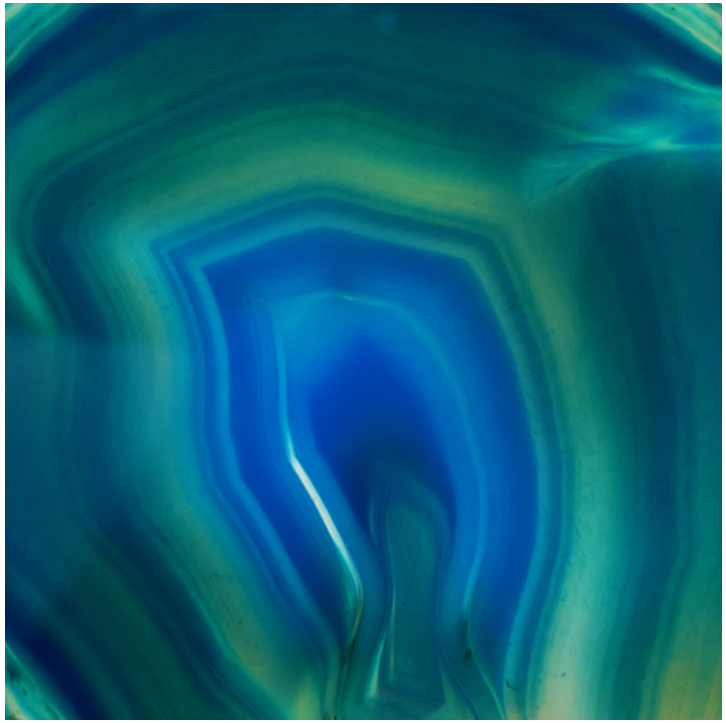
The benefits are compelling. Organizations in our study that have made strides toward platformization report substantially fewer incidents and data breaches. And, as mentioned earlier in this report, their mean time to identify and contain security incidents is significantly shorter.

Revenue generation and efficiency

Security platformization can further business goals. In fact, in our research, almost nine out of 10 CSPs with a high degree of platformization report that cybersecurity investments have helped revenue generation, and six out of 10 say it has contributed greatly to operational efficiencies. None of the executives from CSPs that have yet to move toward platformization say the same.

This advantage comes in part from enhanced agility. Many digital transformation efforts can be derailed by security concerns. Yet among platform users, 8% of digital transformation initiatives fail to scale due to security concerns compared to more than 16% for those that don't use a platform.

In advancing digital transformation, security shifts from a cost center to a value driver. In fact, in our survey, all telecom executives who have adopted platformization say security is a source of value, compared to just 10% of those who haven't.



Who sees security as a source of true value?

100% of platform adopters

10% of non-adopters

"Indosat has transitioned to a centralized cybersecurity structure, consolidating network security management under a single team. ... This centralized approach enhances the ability to detect, respond to, and manage cybersecurity risks effectively."

Amit Kumar, Senior Vice President, Technology Strategy Enterprise Solutions, Indosat

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.

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

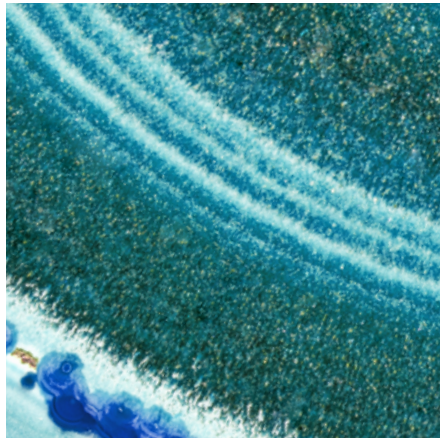
Our research shows that two-thirds of organizations without a unified platform struggle with fragmentation. The lack of cohesiveness for companies that have not adopted platformization can make them vulnerable to potential threats simply because they lack visibility and awareness.

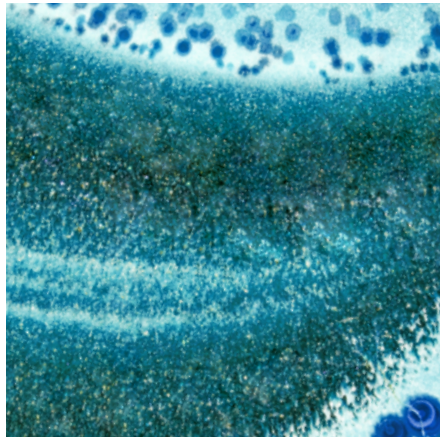
Bridging the gap between IT and IS with a security platform can shift organizational focus from risk aversion to value creation, transforming potential threats into opportunities for innovation and growth. The more teams embrace the use of common platforms and services, the less time they waste getting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

Two thirds

of organizations without a unified platform struggle with fragmentation.

Streamlined security strategy and operations





The security operations center (SOC) is the beating heart of cybersecurity, but only 52% of telecom executives say their current security operating model is effective.

CSPs that tap platformization 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 that is 153% higher than nonadopters.

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

CSPs 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 153% higher than nonadopters.

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 organizations who don't use platforms agree their security operators cannot deal effectively with the sheer quantity of threats and attacks, only one in five platform users say the same.

AI-fueled security platforms are supercharging security teams

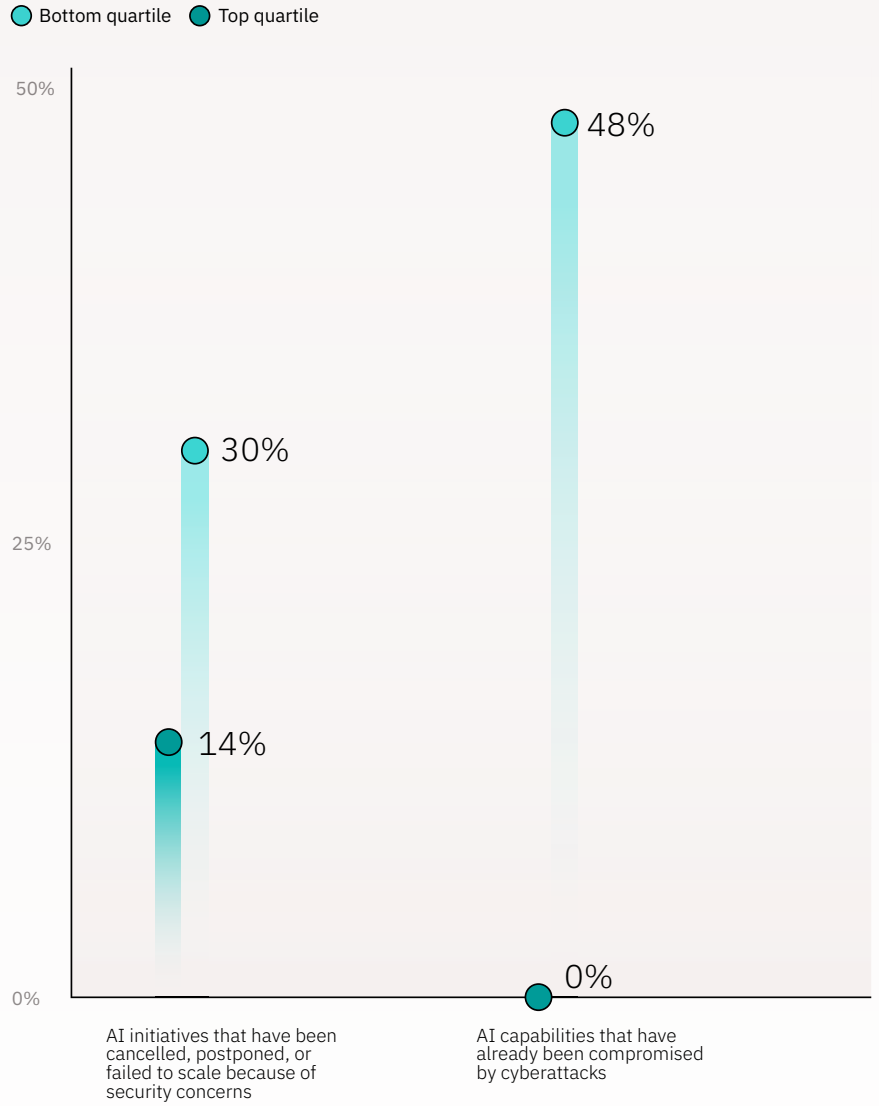
Today's cyberthreats are too complex and too fast-moving for reactive security. To stay ahead, organizations need a proactive, intelligent, AI-fueled defense.

Our research shows security platformization users are better able to tap this potential. A platform 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 a lack of transparency among their security teams. In contrast, 86% of CSPs 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. Eight out of 10 telecom executives in our research agree that adopting security platforms will improve AI operations across the enterprise.

Figure 2

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



Where to begin

Five key actions
to take to use
platformization
to your best advantage:

1

Rationalize 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 regular network security audits and penetration tests—at least quarterly—to reduce blind spots, given that 55% of CSPs have faced breaches in the past year.[7] Do a 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 greatest impact.

3

Strengthen your security with a hybrid-by-design approach. The transition to a security platform can help seamlessly integrate cloud, AI, and security solutions across your network. Adopting a hybrid-by-design approach and incorporating advanced AI-driven threat detection and zero-trust principles at the outset, you create a resilient environment capable of adapting to evolving threats while safeguarding critical data. Update regulatory compliance approaches.

The transition to a security platform can help seamlessly integrate cloud, AI, and security solutions across your network.

4

Make zero trust your security platform starting point. Safeguard your own critical infrastructure using network segmentation and principle-of-least-privilege practices. Enforce strict access controls for IT/IS solutions using robust identity and access management.

5

Drive outcomes using automation and augmentation. Regularly evaluate where automated tools plus human supervision yields the most effective operational and security results. Evaluate how the security platform should interact with operations support systems (OSS) and business support systems (BSS) support services to enable greater integration and greater IT/IS interoperability.

By implementing these strategies and moving to platformization, CSPs can streamline their security operations, reduce costs, improve threat detection and response, and ultimately build a more resilient and secure network. This proactive approach is essential for navigating the evolving cyber threats of today and tomorrow.

Authors

Sourav Banerjee

Associate Partner
Americas Security Services
IBM Consulting

sbanerjee@us.ibm.com

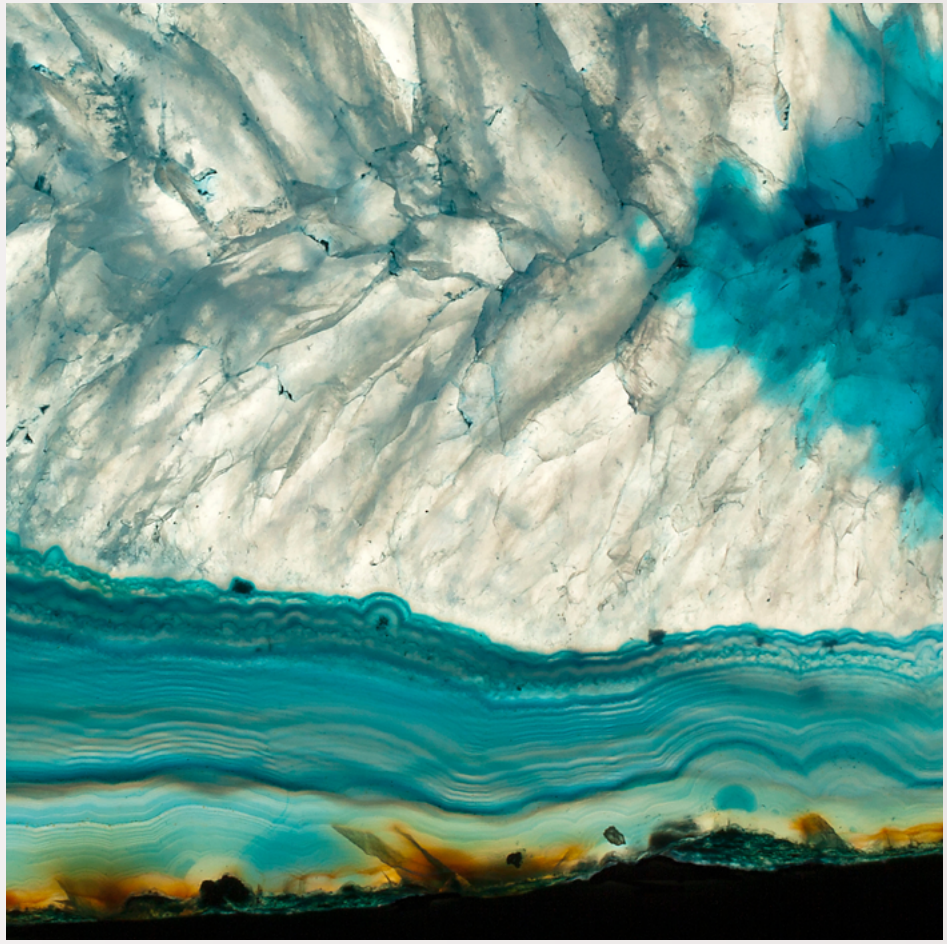
https://www.linkedin.com/in/
sourav-banerjee-b031aa2/

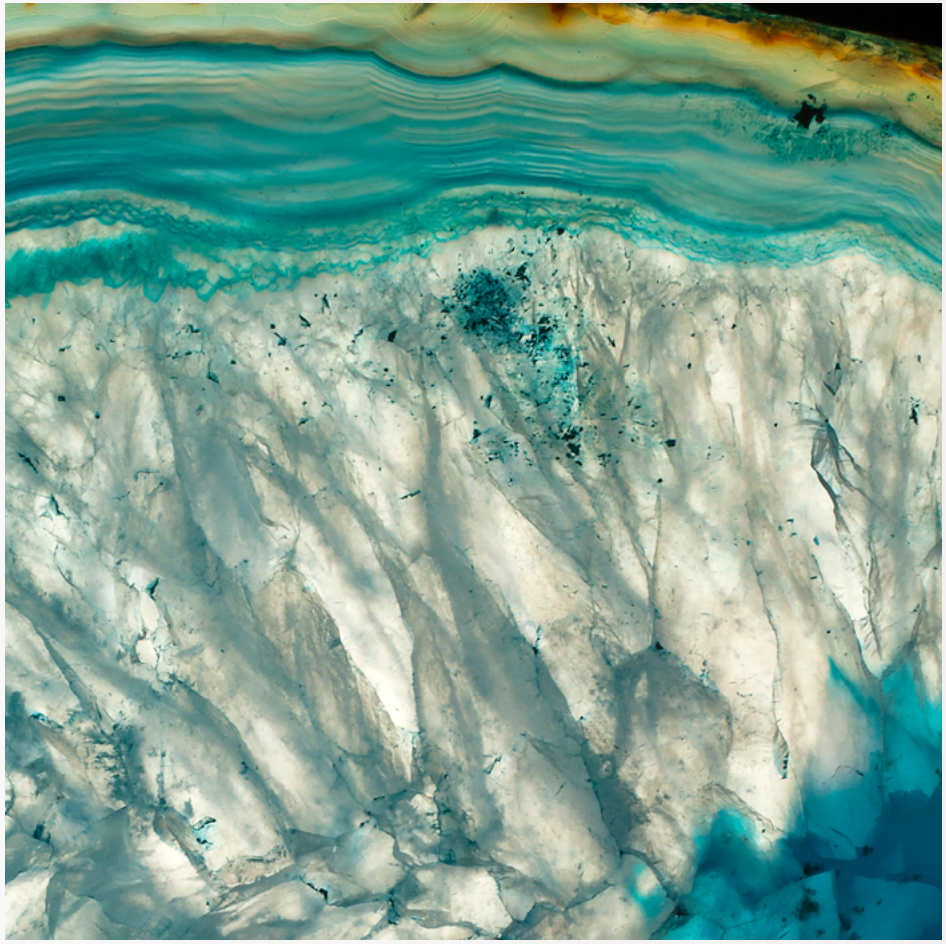
Leonid Burakovsky

Vice President
Product Management
Palo Alto Networks

lburakovsky@paloaltonetworks.com

https://www.linkedin.com/in/
leonid-burakovsky-5795922/





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 (including 60 from telecom organizations) across 21 industries 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 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)**

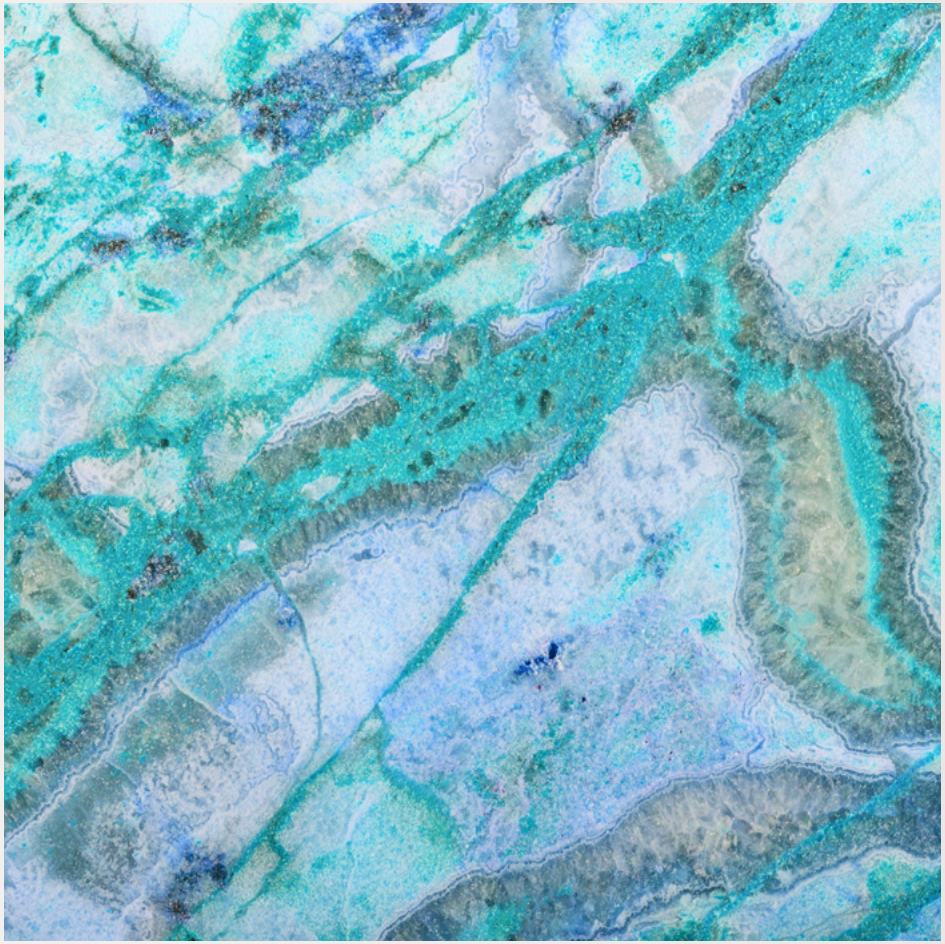
IBM Institute for Business Value. August 2024.

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

Reinventing telecoms with generative AI

IBM Institute for Business Value. June 2024.

https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/telecoms-generative-ai



Notes and sources

1. *Cost of a Data Breach Report 2024*. IBM Security. July 2024. https://www.ibm.com/reports/data-breach
2. Tucker, Eric. “A 9th telecoms firm has been hit by a massive Chinese espionage campaign, the White House says.” AP News. December 27, 2024. https://apnews.com/article/united-states-china-hacking-espionage-c5351ef7c2207785b76c8c62cde6c513
3. Kumar, Rahul, Eoin Coughlan, and Rakhee Chachra. *Rewiring the telecom mindset: How CSPs are gaining a network advantage with cloud and AI*. IBM Institute for Business Value in partnership with GSMA Intelligence. February 2025. https://ibm.co/telecom-networks-cloud-ai
4. Caws, James. “12 recent cyber-attacks on the telco sector.” Wisdiam. July 31, 2024. https://wisdiam.com/publications/recent-cyber-attacks-telcos/
5. Kumar, Rahul, Eoin Coughlan, and Rakhee Chachra. *Rewiring the telecom mindset: How CSPs are gaining a network advantage with cloud and AI*. IBM Institute for Business Value in partnership with GSMA Intelligence. February 2025. https://ibm.co/telecom-networks-cloud-ai
6. Ibid

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | February 2025

1227c12d36b8be12-USEN-00