Trellix

The Mind of the CISO:

The Future of Cyber Resilience

How CISOs and their organizations strategically leverage hybrid infrastructures and AI innovation to navigate regulations, compliance, and the evolving threat landscape.

Contents

Introduction

The cybersecurity landscape is evolving faster than ever. As digital transformation accelerates and hybrid infrastructure models cement themselves as the backbone of enterprise operations, CISOs face a growing web of risks, responsibilities, and expectations. What was once a technical leadership role has become a strategic command post, balancing innovation with resilience, agility with control, and compliance with constant change.

This edition of Mind of the CISO explores how organizations are building resilience through hybrid infrastructure, and how operational technology (OT), such as the systems that run production lines, energy grids, and other physical processes, is converging with IT security. It also examines how organizations are preparing for the next generation of intelligent, AI-driven threats, while the CISO role itself continues to expand in scope and influence. As these operational environments become more digitized and connected, they are also becoming more exposed to cyber threats, adding new complexity to the security landscape CISOs must navigate.

Inside this report:

- Hybrid infrastructure: The foundation of modern resilience
- The convergence of OT and IT security
- Evolving threats and the rise of intelligent defense
- The expanding role of the CISO

Across every dimension, one theme stands out: resilience is no longer static. It's dynamic, distributed, and deeply tied to an organization's ability to evolve. Hybrid infrastructure is redefining continuity and control; OT and IT convergence is uniting once-disparate systems; and intelligent defense, powered by AI and automation, is giving CISOs new ways to anticipate, not just react to, emerging threats.

Yet even as technology advances, the human dimension of cybersecurity remains critical. CISOs are under increasing pressure to manage regulatory complexity, limited resources, and rising expectations to deliver security at the speed of business. Their success depends not only on the systems they secure but on the organizational support, alignment, and investment that enable them to lead effectively.

This report explores what it takes to lead with resilience in an era defined by convergence, intelligence, and constant change, and what must evolve for CISOs to stay ahead of an ever-shifting threat landscape.

Key Findings

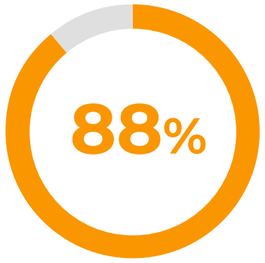
Hybrid infrastructure: The foundation of modern resilience

Nearly all (97%) respondents agree hybrid infrastructure provides greater resilience and risk management capabilities than relying solely on cloud or on-premises environments.

Almost all CISOs (96%) say adopting a hybrid model is essential for meeting evolving regulatory and compliance requirements.

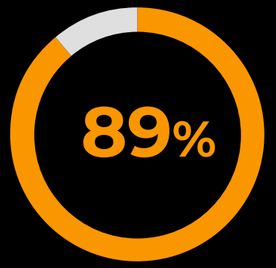
The convergence of OT and IT security

96% agree the convergence of OT and IT security is essential for protecting critical infrastructure from emerging threats.

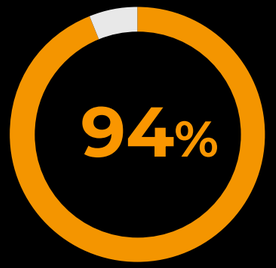


88% agree the convergence of OT and IT security exposes new challenges that many organizations are not yet prepared to address.

Evolving threats and the rise of intelligent defense

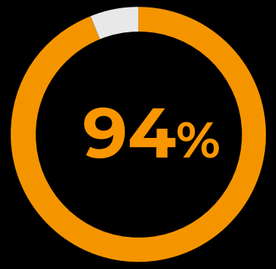


89% agree AI-driven and autonomous ('agentic') cyberattacks represent a major new risk to their organization.

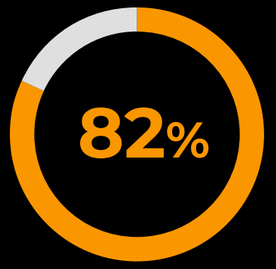


94% agree emerging threats are forcing them to rethink and reprioritize their cybersecurity and infrastructure strategy.

The expanding role of the CISO



Nearly all (94%) agree balancing compliance, security, and innovation is one of the most challenging aspects of their role.

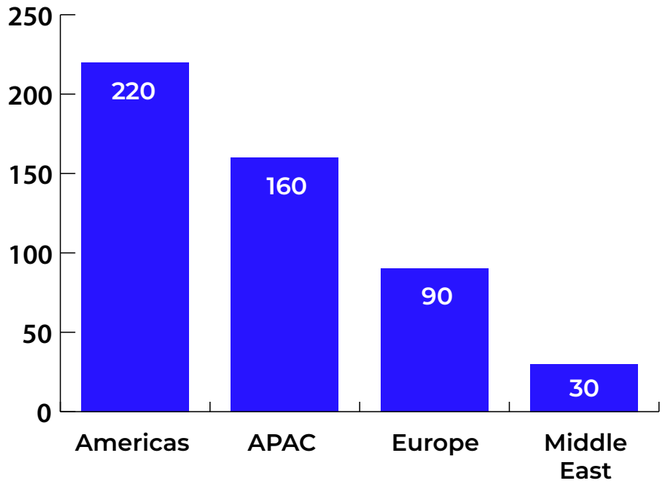


Around eight in ten (82%) agree the time and effort it takes to keep pace with regulatory change is not sustainable for them in their role as a CISO.

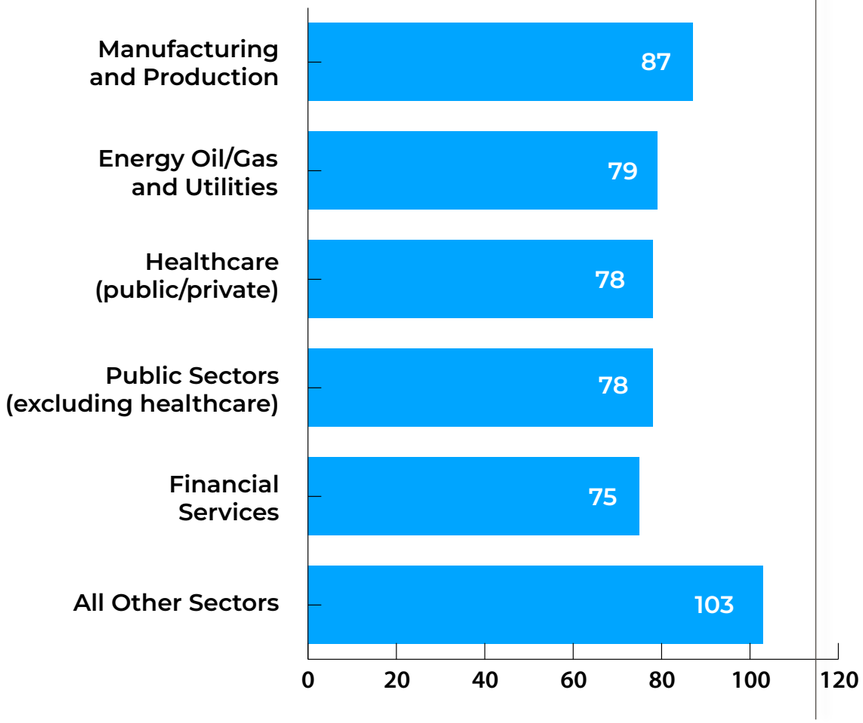
Quantitative respondents

500 CISOs (or equivalent) were surveyed in October 2025, split in the following ways:

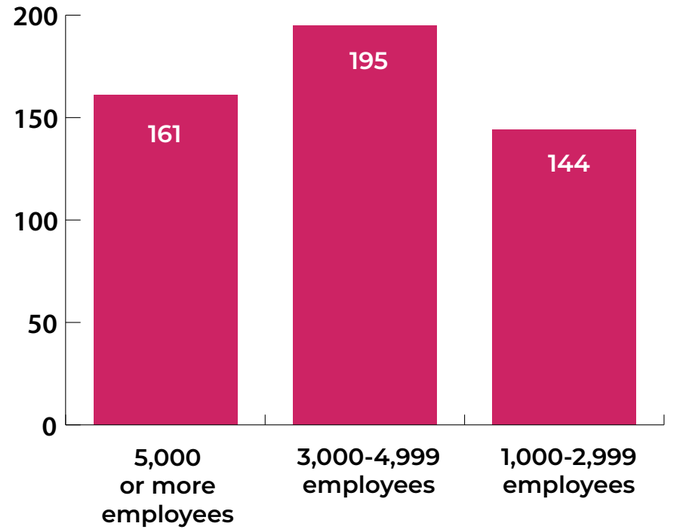
1. In four regions: America, Europe, Middle East, APAC



2. Across a number of sectors: including Finance, Healthcare, Public sector, Energy, Manufacturing etc.



3. Were from organizations with more than 1,000 employees



All interviews were conducted using a rigorous multi-level screening process to ensure only suitable candidates participated.

Qualitative respondents

We conducted seven qualitative interviews with CISOs (or equivalent) in October 2025, split in the following ways:

... by region

In the UK, US and Singapore...


x 2


x 2


x 3

... by organizational sector

- Public sector x 2
- Retail x 1
- Financial Services x 2
- Chemicals/Pharm x 1
- Technology x 1

... by organizational size

- 1,000 - 2,999 employees x 4
- 5,000+ employees x 3

All interviews were conducted using a rigorous multi-level screening process to ensure only suitable candidates participated.

Section 1

Hybrid infrastructure: The foundation of modern resilience

The rising need for hybrid infrastructure

In a world of constant threats and expanding digital operations, no organization can afford to depend on a single environment. Hybrid infrastructure has become the foundation of modern resilience, giving organizations the flexibility to operate securely across multiple platforms. Nearly nine in ten (89%) CISOs say their organizations already operate in a hybrid model, distributing workloads across public and private clouds, on-premises systems, and air-gapped or isolated networks. What began as a practical bridge between legacy and modern IT has evolved into standard architecture for continuity and control.

Organizations currently run their applications across ...

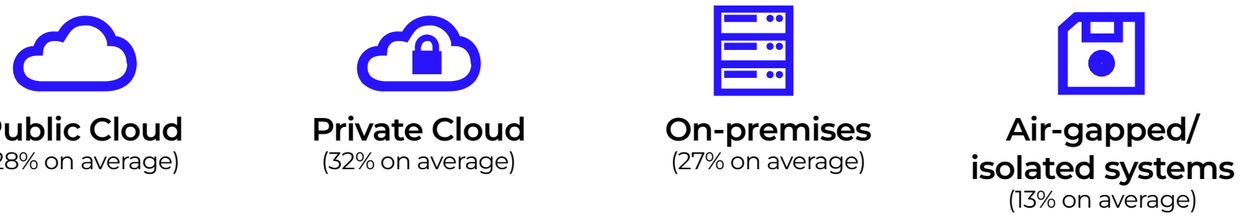


Figure 1. Approximately what percentage of your organization's workloads are currently hosted in each of the following environments? Base: 500

At its core, the shift toward hybrid infrastructure is a response to risk. Organizations are using it to strengthen continuity and safeguard operations in an environment where disruption is inevitable.

97%

Nearly all (97%) respondents agree hybrid infrastructure provides greater resilience and risk management capabilities than relying solely on cloud or on-premises environments.

> **"Building a strong cyber resilience strategy ensures your organization can withstand and recover from advanced attacks. It is a critical component of your broader operational resiliency, which ensures your organization can withstand and recover from all disruptions."**
>
> – Michael Green, CISO, Trellix

Section 1

Hybrid infrastructure: The foundation of modern resilience

Improving resilience and business continuity (36%) remains the leading driver for hybrid environments, followed closely by enhancing cybersecurity (31%) and reinforcing supply-chain integrity (26%). By distributing workloads across different environments, organizations can minimize the impact of localized failures or attacks and maintain critical operations even under pressure. It's this ability to contain disruption, not simply recover from it, that makes hybrid so valuable.

The rising need for hybrid infrastructure

The advantages of hybrid infrastructure extend beyond operational resilience. Regulations are no longer just compliance guardrails; they are actively shaping how organizations design and manage their infrastructure.

Almost all CISOs (96%) say adopting a hybrid model is essential for meeting evolving regulatory and compliance requirements, while a similar number (97%) see it as key to managing data sovereignty and residency obligations. For organizations operating under multiple or fast-changing frameworks, the ability to control where data is stored and processed makes hybrid infrastructure an increasingly compelling choice.

The Cyber Resilience Act (CRA) and ISO 27001 are among the most influential forces behind this shift. Both are strongly influencing hybrid infrastructure strategies, cited by 44% and 40% of CISOs, respectively. These frameworks are driving CISOs to design systems that not only meet compliance expectations but also embed resilience and accountability at their core. The CRA, in particular, has had a significant impact on highly regulated sectors such as financial services, where 63% of CISOs say it strongly influences their hybrid strategy. For these organizations, hybrid infrastructure offers the flexibility to adapt to new mandates without compromising performance.

For many CISOs, this marks a shift in mindset. Regulation is no longer something to keep pace with; rather, it is driving long-term infrastructure design. Those able to align compliance with agility will be best positioned to move faster than competitors, expand confidently into new markets, and demonstrate resilience to both regulators and customers. In this way, hybrid infrastructure not only supports compliance but transforms it into a strategic advantage.

> **"The key benefit to me is business continuity. That is first and foremost, top of the list. If something were to happen, we could resort to our on-premises stuff and continue to work."**
>
> – US, Public Sector

> **"A hybrid environment specifically allows the organization to be much more scalable, much more flexible, much more cost effective. And given that you are in a heavily regulated environment, when the regulations change, when the rules change, when there's any kind of change [...] you definitely want to react really quickly."**
>
> – US, Banking

Section 1

Hybrid infrastructure: The foundation of modern resilience

Navigating the complexities of hybrid infrastructure

While hybrid infrastructure has become central to enterprise resilience, managing it is far from simple. The combination of public, private, on-premises environments, and air-gapped/isolated systems introduces new layers of complexity that can stretch teams and tools alike.

Organizations currently run their applications across

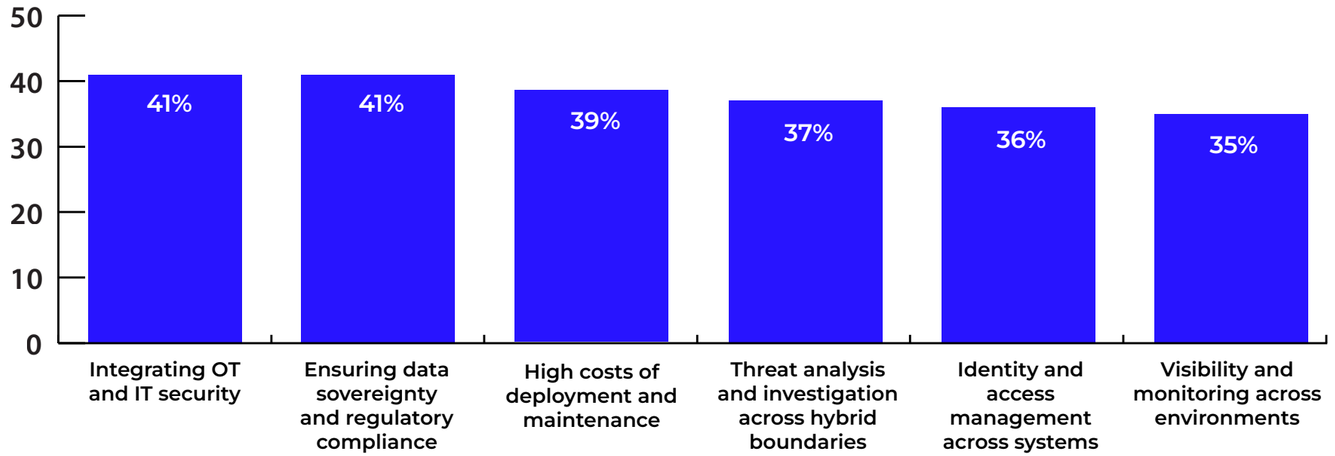


Figure 2. What are the main challenges your organization faces in managing its hybrid infrastructure? Base: respondents' organizations are operating a hybrid infrastructure. Combination of responses ranked first, second, and third (Q5combi3) Base: 445

Integrating OT and IT security is one of the most common challenges in managing hybrid environments. As organizations work to align systems that were not originally designed to operate together, teams must balance performance, protection, and continuity across increasingly distributed networks. At the same time, the task of analyzing and investigating threats across hybrid boundaries is becoming more challenging. The sheer volume and variety of data can make it difficult to identify patterns or isolate incidents quickly, and in an interconnected environment, delays in detection can have far-reaching consequences.

> **"It is challenging to manage hybrid environments - the combination of private and public cloud and on-premises makes security controls more complicated."**
>
> – Singapore, Energy, oil and gas

Section 1

Hybrid infrastructure: The foundation of modern resilience

While regulation is a driving force behind infrastructure design, compliance does add another layer of complexity. Each environment, whether it is public, private, or on-premises, carries distinct regulatory obligations, making it difficult to enforce consistent policies. Even well-resourced teams may struggle to keep pace with shifting requirements across regions, while costs force CISOs to constantly balance what's secure, compliant, and achievable.

Doubling down on hybrid: Investing in long-term resilience

Despite the complexity, CISOs aren't stepping back; they are doubling down. Rather than simplifying their environments, they are investing in making hybrid environments more effective and secure. Having recognized a hybrid infrastructure model is here to stay, organizations are moving beyond short-term fixes and focusing on building the capabilities that will sustain long-term resilience.

The investment priorities for the next 12 months reflect this shift, turning hybrid from a source of complexity into a source of confidence. Cybersecurity sits at the center of this focus, emerging as the top area for investment. This likely reflects the growing recognition that as hybrid environments expand, so too does the attack surface, and that maintaining resilience will depend on having the tools and expertise to detect, respond, and recover quickly.

At the same time, investment in cloud expansion and IT/OT security convergence shows how CISOs are looking to balance growth with control. Expanding cloud capacity supports continued scalability and agility, while convergence between digital and operational systems paves the way for greater integration and visibility. Together, these priorities signal a maturing approach to hybrid infrastructure—one built not on reactive risk management, but on strengthening the systems that underpin long-term resilience.

As these investments take shape, organizations are laying the groundwork for deeper integration across their digital ecosystems. One area coming sharply into focus is the convergence of OT and IT security. The question now is how organizations can bring these traditionally separate domains together to strengthen security and continuity, without introducing new risks.

Top 3 areas of hybrid infrastructure prioritized for investment over the next 12 months

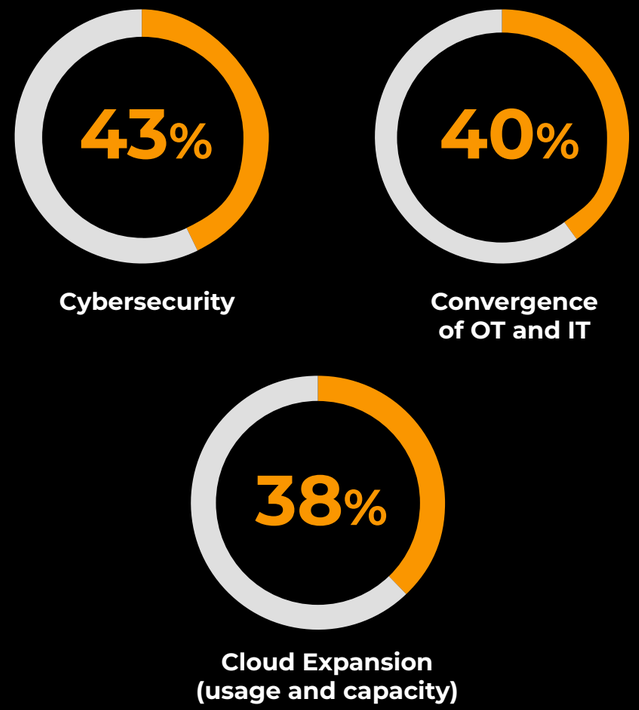


Figure 3. Which areas of your hybrid infrastructure, if any, does your organization plan to prioritize for investment over the next 12 months? Base: respondents' organizations are operating hybrid infrastructure. Base: 445

Section 2

The convergence of OT and IT security

The case for convergence

For many organizations, the next phase of resilience lies in bringing OT and IT security closer together. This includes the operational systems that underpin physical processes, from industrial control and manufacturing equipment to building management systems, access control, and utilities and energy infrastructure—all of which are increasingly connected to digital networks. Yet while the value of convergence is widely recognized, most are still early in their journey. Only 38% of CISOs say their organization has fully converged OT and IT security, with both managed as a single, unified function.

Even so, the direction of travel is clear. Nearly all CISOs (96%) agree the convergence of OT and IT security is essential for protecting critical infrastructure from emerging threats, while 82% believe failing to converge will increase organizational risk and compliance exposure. This shared recognition underscores how deeply intertwined digital and physical systems have become, and how vital unified oversight now is to prevent disruption.

Top 5 benefits of OT and IT security convergence

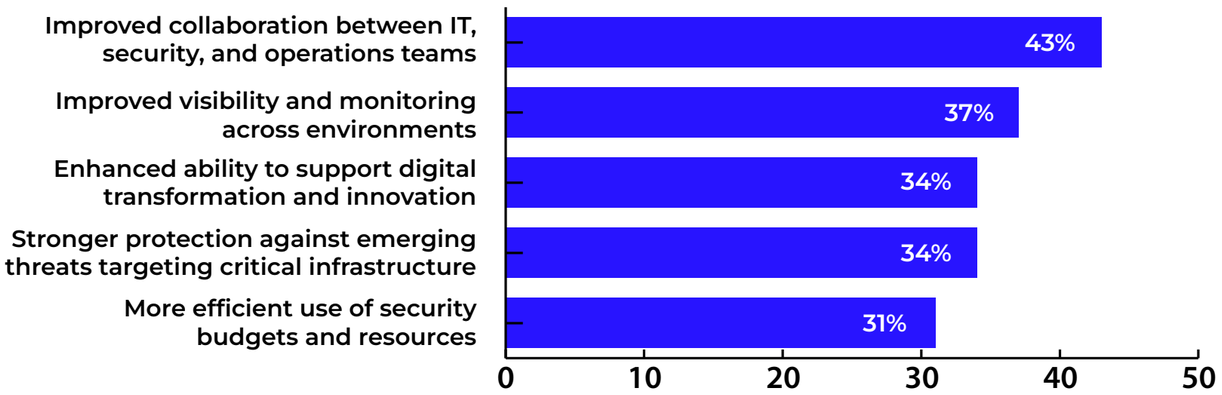


Figure 4. What benefits has/would your organization experience as a result of the convergence of OT and IT security? A combination of responses ranked first, second, and third. Base: 500

Section 2

The convergence of OT and IT security

The benefits of OT and IT security convergence, both realized and anticipated, are becoming increasingly clear. As organizations bring these functions closer together, they are breaking down long-standing silos between security, operations, and technology teams. This improved collaboration can lead to faster, more coordinated responses to incidents and a shared understanding of risk across the business. At the same time, greater visibility across environments gives teams the context they need to detect, contain, and resolve issues before they escalate, reinforcing protection for critical infrastructure and supporting compliance.

However, achieving this level of integration requires more than just technology. It calls for leadership vision, clear strategy, and the readiness to rethink how teams work together. For many, the cultural and organizational shift may be the biggest barrier to full convergence.

“True convergence of OT and IT security is a complex endeavor that demands an intentional, strategic approach driven by strong leadership. While both domains share the goal of protecting critical assets, their priorities, risk profiles, and operational requirements differ significantly. As a result, integration introduces unique challenges, from expanded attack surfaces to interoperability and governance issues. Most organizations still have considerable work ahead to thoughtfully implement and sustain true OT-IT convergence.”

– Michael Green, CISO, Trellix

Balancing convergence and control

Even as organizations realize the benefits of OT and IT convergence, a small degree of separation remains essential. In most cases, convergence means unified strategy and oversight rather than a complete operational integration. Maintaining distinct day-to-day processes helps ensure the unique needs of each environment are respected, allowing organizations to balance innovation, resilience, and risk effectively.

“... you have adequate separation between IT and OT. And you know, you treat OT differently, you understand that the needs are different, and you apply the adequate and appropriate skill set and controls.”

– Singapore, IT/computer

Section 2

The convergence of OT and IT security

Bridging the leadership gap

While the advantages of OT and IT security convergence are widely recognized, progress is often slowed by a lack of readiness, both in terms of resourcing and leadership understanding.

97%

agree the convergence of OT and IT security will **require additional investment** in cybersecurity tools and workforce skills

94%

agree the convergence of OT and IT security **requires new partnerships and collaboration** across IT security and operations teams

88%

agree the convergence of OT and IT security **exposes new challenges** that many organizations are **not yet prepared to address**

Convergence isn't just about connecting systems; it's about creating the conditions for success. It demands sustained investment in the right tools and skills, as well as stronger collaboration among IT, security, and operations teams. Yet many organizations admit they're not fully prepared for the challenges convergence brings. Closing that gap requires more than intent; it calls for a clear strategy, coordinated planning, and leadership capable of turning alignment into action.

Limited leadership understanding of OT may be amplifying these challenges. More than two in five (41%) of CISOs believe leaders have limited awareness of the differences between OT and IT security. Without this awareness, strategies built for traditional IT environments may be applied to OT systems that require very different priorities, risk profiles, and operational demands. The likely result is a disconnect between strategic vision and practical execution, where controls fail to account for how these systems function.

Furthermore, 38% of CISOs say their leadership team lacks focus on resilience and recovery planning for OT environments. This lack of attention leaves organizations vulnerable to longer outages and greater disruption when incidents occur, undermining the very resilience convergence is meant to strengthen. To move forward, leaders must go beyond recognizing the need for convergence; they must understand the distinct realities of OT and embed resilience at every stage of integration.

Section 3

Evolving threats and the rise of intelligent defense

A new age of threats

The cyber threat landscape is evolving rapidly, becoming more sophisticated, targeted, and difficult to anticipate. As hybrid environments expand, the attack surface grows, multiplying the number of potential entry points and raising the stakes for every organization.

Among the most concerning developments are AI-driven and autonomous ("agentic") cyberattacks—threats that use artificial intelligence to operate independently, make decisions, and adapt in real time. These attacks can probe defenses continuously, identify weaknesses, and execute tailored exploits at speed and scale. Nearly nine in ten (89%) CISOs say such attacks represent a major new risk to their organizations, underscoring growing concern about how to defend against adversaries that are dynamic, automated, and increasingly unpredictable.

It is understandable, then, why agentic AI and autonomous cyberattacks (39%) top the list of emerging threats causing the greatest concern among CISOs. Yet these are far from the only challenges reshaping the security landscape. Phishing and social engineering campaigns are growing in sophistication (38%), often using AI to imitate trusted users or systems with alarming accuracy. Targeted attacks on operational technology are testing the resilience of critical infrastructure (36%), while exploits targeting cloud and hybrid environments (35%) are also among concerns for CISOs. Each of these threats compounds the challenge of maintaining visibility and control across an increasingly interconnected enterprise.

Top 5 emerging threats causing the greatest concern

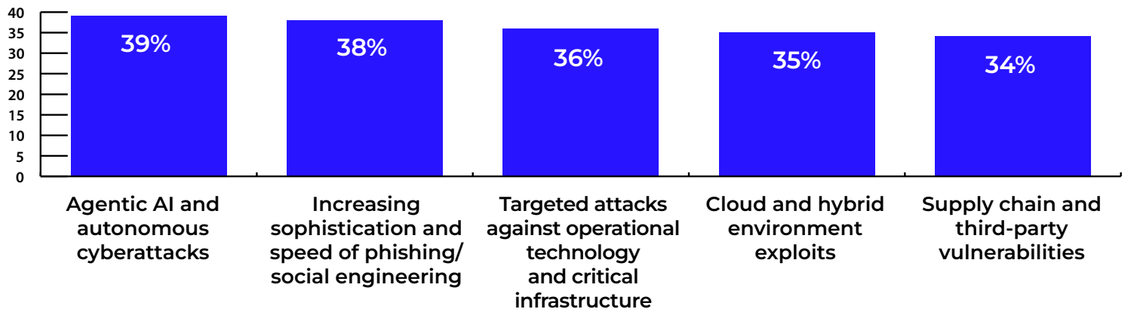


Figure 5. Which of the following emerging threats are of greatest concern to your organization today? Combination of responses ranked first, second and third. Base: 500

> **"These things are always changing, and we have to make sure that we are changing our response and our detection line. I would say at the moment it's probably quite unprecedented the amount of threats that are out there."**
>
> – UK, Financial Services

Section 3

Evolving threats and the rise of intelligent defense

It is unsurprising then that 94% of CISOs agree emerging threats are forcing them to rethink and reprioritize their cybersecurity and infrastructure strategies. The growing sophistication of the threat landscape is not just reshaping defensive priorities; it is redefining what resilience looks like.

The need for improvement

Cyber threats are evolving faster than most organizations can adapt, exposing cracks in even the most mature security strategies. The vast majority of CISOs now recognize that meaningful improvement is needed to keep pace. Ransomware and extortion (89%), agentic AI and autonomous cyberattacks (88%), and targeted attacks on OT and infrastructure (87%) are all seen as areas where defenses must evolve. A clear sign that current measures are struggling to match the scale and sophistication of modern threats.

To strengthen their defenses, CISOs are focused on the areas that would most enhance capability. For many, that begins with visibility, particularly across hybrid and cloud environments (40%). The ability to see and understand activity across every layer of infrastructure is fast becoming the cornerstone of resilience, helping teams detect and contain threats before they escalate.

Top 5 factors that would improve organizations' cyber defense capabilities

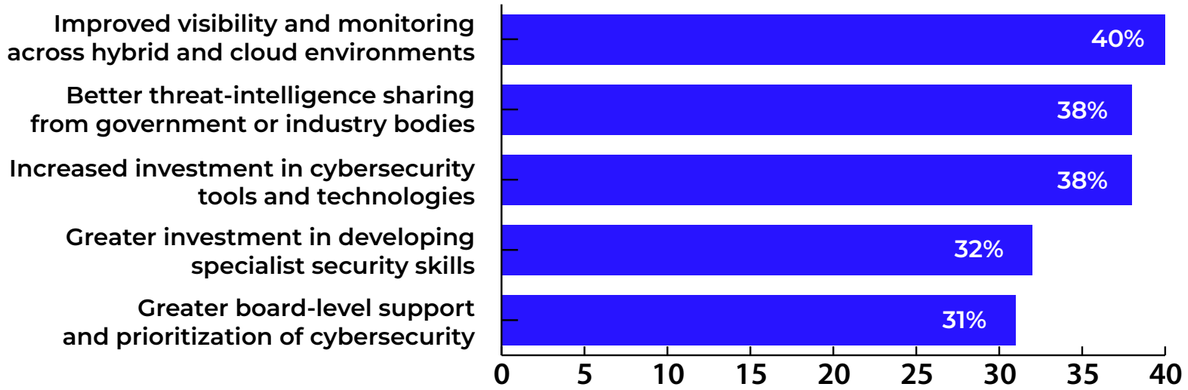


Figure 6. What would improve your organization's ability to defend against cyberattacks and emerging threats? Base: 500

Section 3

Evolving threats and the rise of intelligent defense

CISOs also recognize that lasting progress requires more than visibility alone. Better intelligence sharing between public and private sectors (38%) and continued investment in cybersecurity tools (38%) and specialist skills (32%) are seen as key areas to strengthen defense capabilities. Yet, recognizing what would strengthen defense is one thing; having the means to act on it is another. Progress depends on leadership commitment, sustained investment, and the support to turn plans into action.

AI: From emerging risk to essential defense

While adversaries are exploiting AI to automate and amplify their attacks, organizations are leaning into it to strengthen defenses and keep pace with a rapidly shifting threat landscape. Nearly half of CISOs (47%) say they are completely confident AI-powered security tools can effectively defend against autonomous, AI-driven cyberattacks. A reassuring sign given these threats rank among their top concerns.

That confidence is now being matched by investment. On average, a quarter of security budgets (25%) is dedicated to AI-enabled tools, demonstrating just how central AI has become to modern security strategy. These tools are being used to streamline complex tasks such as threat analysis, intelligence gathering, and incident management, enabling teams to detect and respond with greater speed and precision. In doing so, AI is helping organizations move from reactive protection to proactive defense, anticipating attacks before they strike.

Yet as confidence and investment grow, deploying AI effectively remains a complex task. CISOs recognize that integrating AI effectively is still a work in progress, and one that brings its own set of complexities.

Hybrid foundations power AI success

AI's growing role in cybersecurity brings enormous promise, but also significant complexity. For many CISOs, implementing AI effectively is proving a challenge. High deployment and maintenance costs (46%) and integration difficulties with existing OT and IT systems (42%) are among the most common barriers, compounded by concerns over supply chain dependencies (37%) and compliance requirements (32%).

> **"The cyber risk is forever growing... and you can do so much with a certain size of team, certain size of budget."**
>
> **– UK, Retail**

Section 3

Evolving threats and the rise of intelligent defense

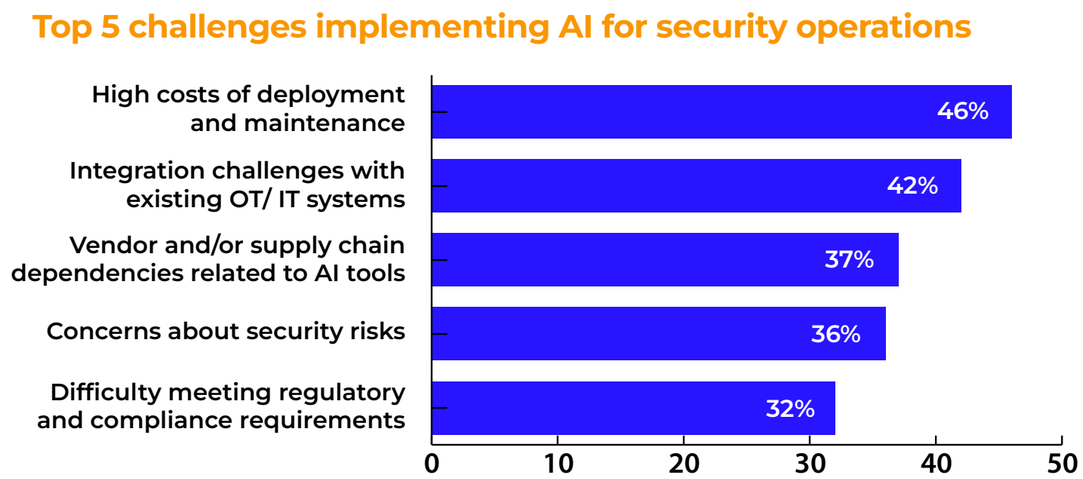


Figure 7. What are the main challenges your organization faces when implementing AI for security operations? Base: 500

Yet, not all organizations face these hurdles equally. Those operating in hybrid environments appear better equipped to manage AI deployment, as they are less likely to report challenges than their non-hybrid counterparts. This advantage reflects the broader trend seen throughout the cybersecurity landscape: hybrid models, with their flexibility and scalability, create stronger foundations for innovation, visibility, and resilience.

Confidence in AI must be balanced with caution. Around nine in ten (92%) CISOs agree managing AI's benefits alongside its security and compliance risks is a key challenge for their organization. This balancing act captures the reality of modern security leadership: navigating rapid technological change while ensuring defenses remain robust and trusted.

As AI becomes more deeply embedded in security operations, the CISO's role is evolving with it. The next frontier isn't just about adopting new tools, but about leading teams, strategies, and cultures that can adapt as fast as the threats they face.

High deployment and maintenance costs

43%	64%
Hybrid Users	Non-Hybrid Users

Integration challenges with existing OT/IT systems

42%	49%
Hybrid Users	Non-Hybrid Users

Vendor and/or supply chain dependences related to AI tools

36%	47%
Hybrid Users	Non-Hybrid Users

Section 4

The expanding role of the CISO

Redefining the CISO

The role of the CISO has never been broader or more demanding. The greatest challenges they currently face include managing increasingly complex hybrid and multi-cloud environments (41%), balancing security with business agility (39%), and maintaining resilience and continuity in the face of disruption (39%). Yet these challenges not only sit with the CISO, they affect the entire organization.

And the pressure is only set to grow. As organizations embrace hybrid environments and accelerate digital transformation, CISOs are finding their remit broadening again. In the year ahead, many expect to devote more time to managing data sovereignty and residency (44%), securing complex hybrid infrastructures (43%), and enabling business innovation (41%), all while staying ahead of an increasingly volatile threat landscape. These expanding responsibilities mirror the wider forces reshaping cybersecurity today: the rise of AI-driven attacks, tightening regulatory demands, and the constant need to balance protection with progress. In this context, it is no surprise addressing emerging threats (38%) remains a focus area.

Areas where responsibilities will increase over the next 12 months

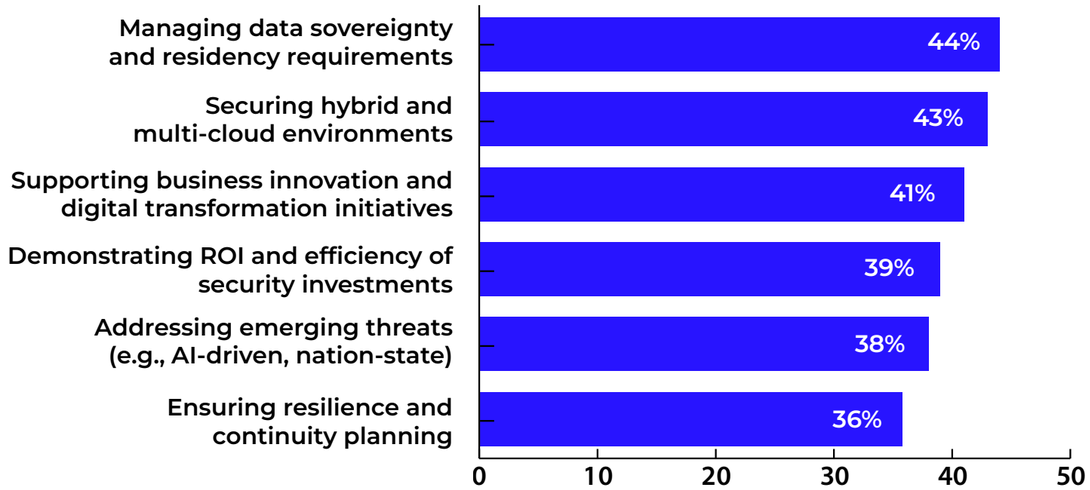
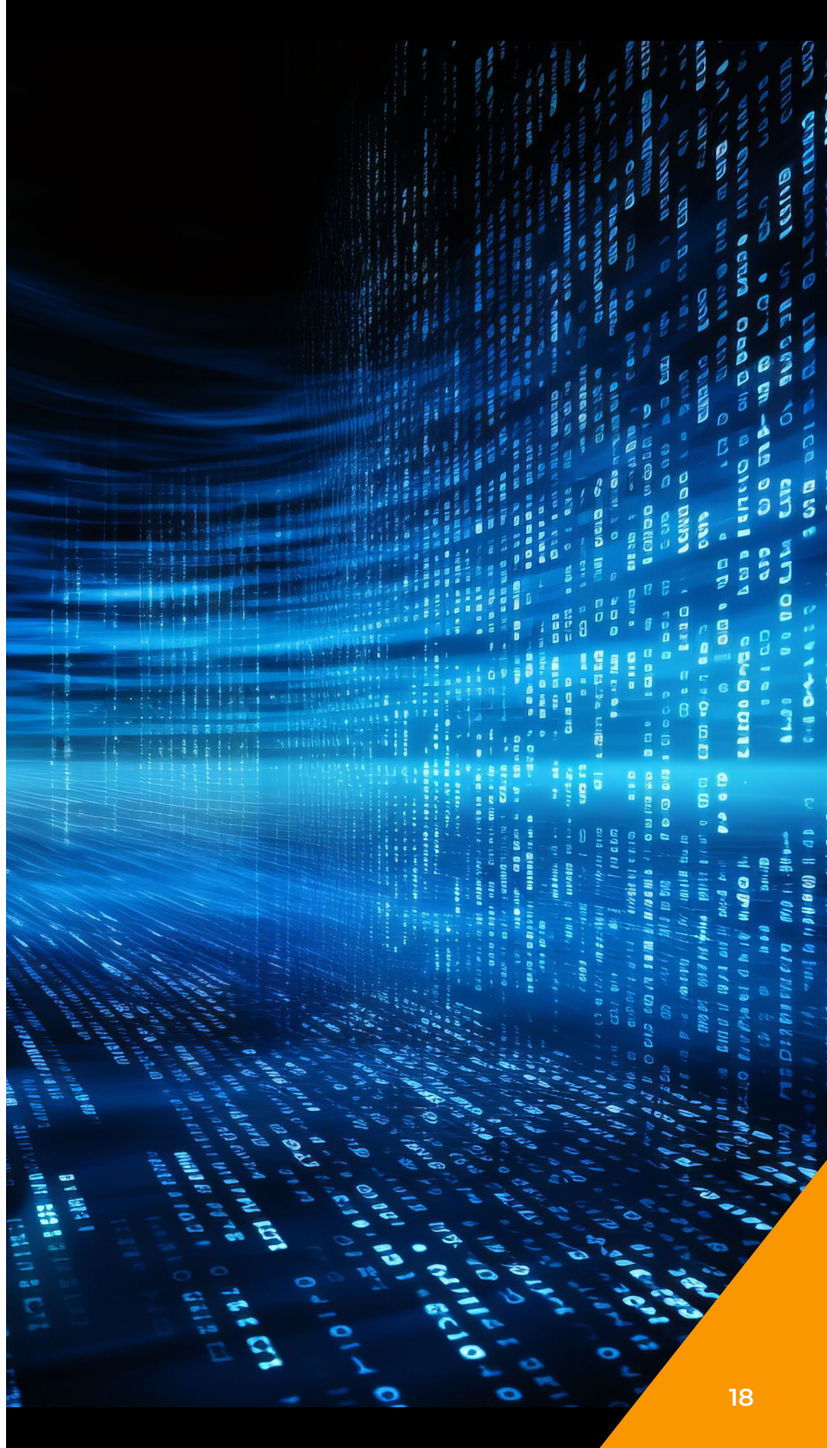


Figure 8. Thinking about the next 12 months, in which areas do you believe your responsibilities as a CISO will increase? Base: 500



Section 4

The expanding role of the CISO

It is little wonder then nearly all CISOs (94%) agree that balancing compliance, security, and innovation is one of the most challenging aspects of their role. The weight of these competing priorities is fueling deep concern among leaders themselves. Over two-thirds (70%) are worried about their future in the role, citing expanding responsibilities and unsustainable workloads. And as these pressures mount, the growing burden of regulatory change is only adding to the strain. CISOs need the support of the wider organization to help them navigate and manage this ever-increasing burden.

Regulatory complexity demands enterprise-wide alignment

As the CISO remit continues to expand, regulatory demands are emerging as key pressure points. The sheer pace of change—between new data protection laws and tightening compliance frameworks—is leaving many leaders struggling to keep up. In fact, more than four in five (82%) CISOs say the time and effort required to stay aligned with evolving regulations is not sustainable in their current role.

Main challenges for complying or aligning policies with cybersecurity regulations

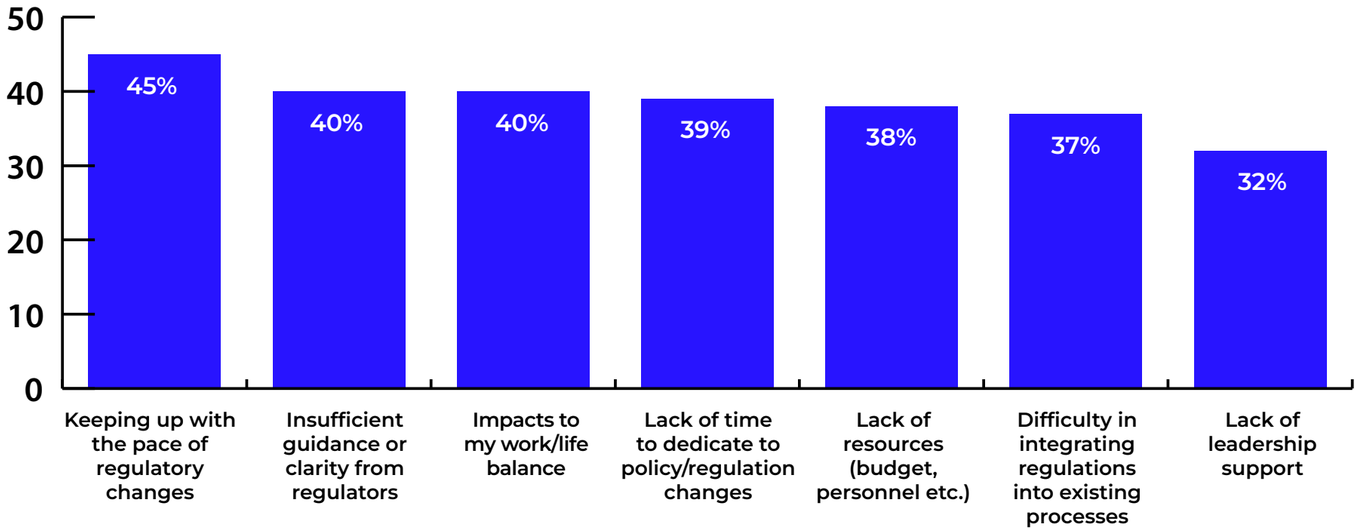


Figure 9. What are the main challenges you as a CISO (or equivalent) face in complying with or aligning policies with cybersecurity regulations? Base: 500

Section 4

The expanding role of the CISO

Keeping pace with this complexity often comes at a personal and organizational cost. Nearly half of CISOs (45%) cite the pace of regulatory change as their main challenge, while others point to a lack of time, clarity, and resources to manage compliance effectively. CISOs operating in non-hybrid environments are particularly affected, being more likely to struggle with the pace of regulatory change (51% vs. 44% of hybrid users). This again highlights how hybrid models can provide greater flexibility and responsiveness in adapting to evolving compliance demands.

Yet while technology and structure play a role, the bigger issue is one of support. Many CISOs report being held back by a lack of resources, e.g., limited budgets and understaffed teams (38%) and insufficient leadership alignment (32%), leaving them to shoulder an unsustainable compliance load. Without stronger collaboration between security leaders, boards, and business stakeholders, even the most capable CISOs will struggle to turn strategy into sustained resilience.

To keep pace with the next era of cybersecurity, organizations must evolve alongside their security leaders. That means empowering CISOs with the resources, personnel, and authority needed to act decisively—not only to manage regulatory risk but also to lead innovation securely.

> **“The CISO, for example, shouldn’t necessarily be the risk owner. The CISO, in my view, should be the risk identifier... I think there’s a responsibility on the leadership of the organization rather than just on the CISO.”**
>
> **– UK, Retail**

Conclusion

As this edition of the Mind of the CISO reveals, the architecture of resilience is being rebuilt. Hybrid infrastructure has emerged as the cornerstone of security strategy, enabling flexibility and control in a fragmented world. The convergence of OT and IT security is transforming how organizations manage risk across digital and physical domains. And intelligent defense, underpinned by AI and automation, is becoming essential to stay ahead of threats that evolve faster than human response alone.

But technology is only part of the equation. The pressures facing CISOs—from expanding regulatory demands to rising workloads and board expectations—underscore a growing need for systemic support. Security leaders cannot deliver resilience in isolation. They need the budget, personnel, and executive backing to turn strategy into sustained capability. Without that investment, the very resilience organizations depend on remains fragile.

To thrive in this new era, enterprises must see cybersecurity not as a cost of doing business, but as a catalyst for continuity and confidence. This means empowering CISOs to lead decisively, uniting OT and IT security under a shared vision, and embedding intelligence into every layer of defense.

The message from CISOs is clear: the future of resilience will belong to organizations that act now, investing in the people, processes, and platforms needed to turn security into a source of lasting advantage.

Recommendations:

Based on the findings of this Mind of the CISO report, several priorities stand out for organizations and their security leaders. Together, they reflect the shift from reactive protection to proactive resilience and the need for CISOs to be empowered with the tools, partnerships, and authority to lead that transformation.

Build hybrid resilience as a strategic capability
Hybrid infrastructure is now the foundation of modern resilience, but only when managed cohesively. This means aligning OT and IT systems where appropriate, embedding compliance into design, and using hybrid flexibility to contain disruption rather than react to it.

Converge OT and IT security
Bringing OT and IT security under unified oversight can improve collaboration, accelerate incident response, and strengthen protection for critical infrastructure. Convergence should focus on shared governance and intelligence, while maintaining operational independence to balance performance, resilience, and risk.

Evolve from reactive protection to intelligent defense
Emerging threats, particularly AI-driven and autonomous cyberattacks, demand faster, smarter responses. Organizations should invest in AI-enabled tools that enhance threat detection, response speed, and situational awareness across hybrid environments. The goal is not just automation, but anticipation: using intelligence to identify and act on risk before it escalates.

Empower CISOs with alignment, resources, and authority
The role of the CISO now spans far beyond technical security. To meet growing regulatory, operational, and strategic demands, organizations must strengthen leadership alignment, increase investment in security talent and tools, and establish clear governance frameworks, all to support CISOs in fulfilling their roles.

Develop modern cyber policies for a hybrid and AI-driven future
As CISOs increasingly rely on hybrid operating models, it is essential policymakers reflect this reality when shaping cybersecurity policy and funding, particularly for government agencies. This means policymakers need to diversify their investments in IT environments, not just investing in cloud, but investing in a holistic manner to ensure government agencies get the full benefits of hybrid environments. Likewise, given the use of AI by cyber hackers, policymakers should prioritize investments in defense cyber AI solutions to meet the growing threat of cyber hackers leveraging AI at machine speed.

Additional Resources

Mind of the CISO Research Series

- **Closing the Gap between Reaction and Readiness:** Over 500 CISOs worldwide share their views on the evolving threat landscape, the role of AI and automation in combatting threats, and the value of peer communities in navigating complexities and driving clarity.
- **CISO Crossroads:** Over 500 security leaders worldwide share their views on cybersecurity regulation, the CISO role, and their interactions and challenges when reporting to their organization's board.
- **Decoding the GenAI Impact:** Trellix engaged with 500 security leaders across North America to understand how GenAI and AI are evolving the threat landscape and the CISO role to reshape the future of cybersecurity in the workplace.
- **Behind the Breach:** To shed light on the challenges CISOs face in the aftermath of a breach, Trellix surveyed over 500 security leaders worldwide who have managed a major cyber incident, revealing strategic insights, enlightening stats, and learnings for the best route forward.
- **Understanding the CISO's Struggle:** Trellix engaged with over 500 security leaders to understand what's holding SOC teams back, revealing how they work amidst a tumultuous threat landscape, which business functions hold them back, what tools and support they need to be successful, and how best to move forward.

Trellix Advanced Research Center Digest

Subscribe to get the latest cybersecurity trends, best practices, security vulnerabilities, and more.

Additional Resources

The OT Threat Report: November 2025
Authored by the Trellix Advanced Research Center, this report details an increase in threats targeting operational technology (OT) and industrial control systems (ICS) observed between April 1, 2025, and September 30, 2025. The threat landscape reveals coordinated campaigns by state-sponsored actors and ransomware groups, with the manufacturing, transportation and shipping, utilities, and energy/oil and gas sectors bearing the highest risk.

The CyberThreat Report: October 2025
Authored by the Trellix Advanced Research Center, this report (1) highlights insights, intelligence, and guidance gleaned from multiple sources of critical data on cybersecurity threats and (2) develops expert, rational, and reasonable interpretations of this data to inform and enable best practices in cyber defense. This edition focuses on data and insights captured primarily between April 1, 2025, and September 30, 2025. Notably, this report finds the introduction of new AI-powered malware, the exploitation of vulnerabilities in the software supply chain, and an increased focus on developed economies and critical infrastructure.

Reporting to the Board: CISO Best Practices
As cybercrime and regulatory pressure on cybersecurity grow, the role of the CISO is evolving from a technical expert to a business-focused leader. Many of today's CISOs are being asked to report to their organization's board on a regular basis. How can you make the most of your time in front of the board? Check out this guide from the Trellix CISO Council to learn best practices for presentations.

The CISO's Guide to Ransomware
When it comes to ransomware, every minute counts. Get road-tested guidance for CISOs and cybersecurity leaders to combat ransomware.

Trellix is a global company redefining the future of cybersecurity. The company's comprehensive, open, and native cybersecurity platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through artificial intelligence, automation, and analytics to empower over 40,000 business and government customers with responsibly architected security.

More at *www.trelllix.com*
Follow Trellix on *LinkedIn* and *X*.

VansonBourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit *www.vansonbourne.com*