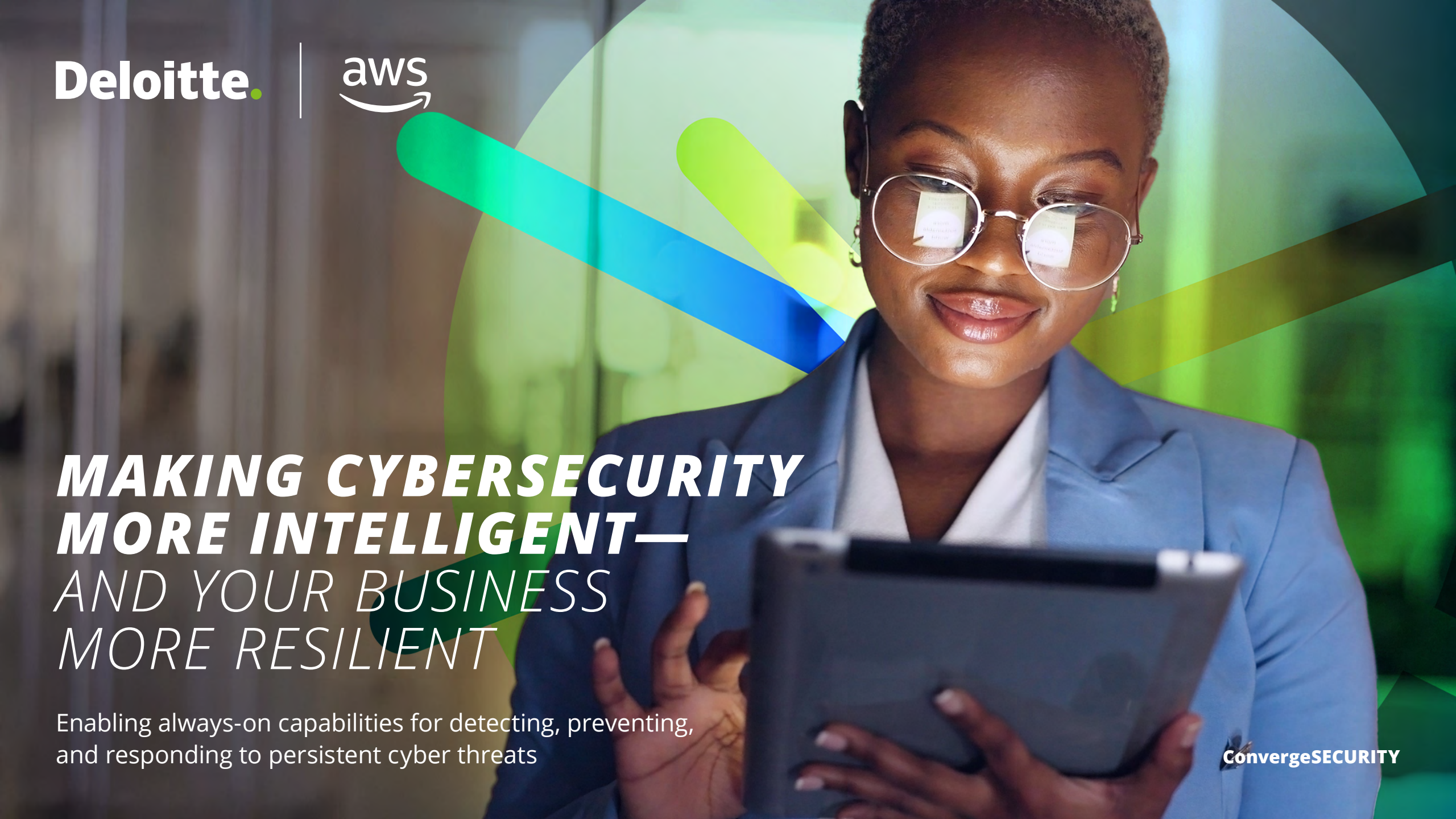
Deloitte. | aws



MAKING CYBERSECURITY MORE INTELLIGENT— *AND YOUR BUSINESS MORE RESILIENT*

Enabling always-on capabilities for detecting, preventing, and responding to persistent cyber threats

ConvergeSECURITY

INTRODUCTION

Cybersecurity remains a top business imperative. Across industries, organizations are sharpening their strategic focus on cyber, with 86% of surveyed executives taking moderate to significant action to increase cybersecurity.[1] And many are prioritizing these efforts while navigating existing budget limitations, striving to make the most of available resources.

The growing focus on security is clear. Cyber threats are rampant and growing, with 40% of surveyed organizations saying they have publicly reported six to ten cybersecurity breaches in the past year.[2] And no business is immune.

DELOITTE GLOBAL FUTURE OF CYBER

6–10

Cybersecurity breaches in the past year

Reported by 40% of surveyed organizations.

Increasing business complexity—from interconnected supply chains and business ecosystems to third-party apps and cyber talent shortages—compounds the challenge. At the same time, new technologies such as machine learning (ML) and Generative Artificial Intelligence (GenAI) continue to emerge and evolve, bringing new considerations for how to protect data and systems against new types of threats.

FROM COMPLEXITY TO STRATEGY

Amid this complex web of challenges and needs, organizations face a pivotal moment. To decisively and effectively address tomorrow's cybersecurity landscape, enterprise leaders need a broad strategy and intelligent, end-to-end capabilities that are always on—and that can evolve to meet new threats and new needs.

Bring together all the pieces of that strategy, and you can not only be better positioned to stand ready to respond rapidly to cyber threats; you can also unlock the potential to build greater trust in your business, drive efficiencies, and realize additional benefits.

1. Deloitte Global Future of Cyber Survey (4th Edition).
2. Ibid.

CHARTING A NEW PATH FOR SECURITY

Creating a broad security plan will require an enabling set of processes, technologies, and professionals that work in harmony to help the organization identify, respond to, and recover from incidents—while making the business more resilient and ready to face future threats. Internal alignment will be essential to ensure that everyone in your organization is informed, effectively equipped, and working toward common goals. By embedding cyber strategy into the DNA of your organization, you can enable your team to work together more effectively as they respond to cyber incidents.

The path forward should begin with a deep understanding of the critical assets—such as systems and data—that are most valuable to your business. Securing those assets should top the list of needs, along with creating greater visibility into your data, business-critical systems, and security tools—so you can better identify vulnerabilities and the steps to address them.

Developing strong threat hunting and identification capabilities, supported by intelligent technologies such as AI, should also be a priority. While such automated capabilities can alleviate burdens on your IT and cyber workforce, your people are paramount to strengthening cybersecurity. They are the ones who must build, test, and maintain a comprehensive readiness, recovery, and response plan.

Not only will they select and help implement the technologies that will be part of that plan; they will work to ensure that the overall plan provides the resilience your business requires. The work they do and the outcomes they target should be aligned with key business objectives such as enabling operational agility, adhering to service levels for customers, delivering efficiencies and cost savings, and avoiding specific risks including regulatory fines.

Developing strong threat hunting and identification capabilities, supported by intelligent technologies such as AI, should also be a priority.

Creating a culture to support new cyber capabilities is key to driving the cyber planning strategies and cyber activities that determine the readiness of your organization.

CYBER PLANNING STRATEGIES

Some examples include:[3]

- Analyzing and updating cyber plans annually
- Establishing a governing body composed of senior business and IT leaders, to oversee the cyber program
- Employing risk quantification tools to measure and enable return on cyber investments
- Conducting incident-response scenario planning at the organizational and/or board level
- Enlisting external help/ outsourcing to manage cyber initiatives

CYBER ACTIVITIES

Some examples include:[4]

- Annual cyber awareness training among employees
- A cyber incident response plan that gets updated and tested annually
- A detailed plan to assess how to protect data at each step, as to where data is stored, processed, and transmitted
- A cyber risk program to monitor and track the security posture of partners and suppliers
- An ongoing "voice of the customer" input for cyber and data privacy preferences

3. Future of Cyber Survey (4th Edition).

4. Ibid.

FOUR FACTORS THAT SHOULD INFLUENCE YOUR JOURNEY

How you shape your cybersecurity strategy—as well as your supporting ecosystem of solutions and culture—depends on several factors that should be central to operating with confidence in the future.

1

Security as a strategic imperative

2

The persistent need for operational resilience

3

The AI factor

4

Your industry-specific lens

FOUR FACTORS THAT SHOULD INFLUENCE YOUR JOURNEY

1

DELOITTE GLOBAL FUTURE OF CYBER

57%

Cybersecurity budgets

Percentage of surveyed executives who anticipate increasing their budgets for cybersecurity over the next 12–14 months.

Security as a strategic imperative

In every industry, cybersecurity is an increasingly larger piece of the puzzle for business strategy. Cyber has risen to become a regular boardroom topic, and enterprise leaders with cyber responsibilities are claiming their seat at the table where critical decisions are being made about the future of the business.

As more organizations undertake digital transformation initiatives involving cloud, data analytics, 5G, Internet of Things (IoT), AI, and other technologies, securing those programs becomes vital. For example, 85% of surveyed executives said cybersecurity plays a large or moderate role in securing their organizations' investments in cloud initiatives; 80% said it plays a large or moderate role for their AI and cognitive computing endeavors.[5]

These leaders are approaching cyber with an end-to-end view of their business, recognizing its strategic importance to the benefits they are looking to achieve. For example, 57% of executives surveyed in the Deloitte Global Future of Cyber Survey (4th Edition) anticipate increasing their budgets for cybersecurity over the next 12 to 24 months. And 58% of those surveyed said they expect to begin integrating their cybersecurity spend with budgets for other programs, such as digital transformation initiatives, IT programs, and cloud investments.

As business impact remains a cyber priority—and as the enterprise technology landscape evolves to drive new strategic initiatives—leaders need to ensure that the organization is fully aligned and capable of evolving as new threats emerge. To drive business outcomes that matter, you should do more than embed security capabilities into your digital transformation initiatives; you should embed a "security first" mindset across your organization. Doing so can enable you to stand ready for and be able to respond to and recover from future threats—while keeping the business on track toward its strategic goals.

5. Future of Cyber Survey (4th Edition).

FOUR FACTORS THAT SHOULD INFLUENCE YOUR JOURNEY

The persistent need for operational resilience

To survive in today's environment, your business needs to be resilient—capable of withstanding and bouncing back from any chaotic event that comes your way. From phishing attempts and ransomware attacks to more complex cyber assaults, almost any attack can compromise data or paralyze critical operations. The potential for disruption is real and persistent—making it crucial to adopt capabilities that support business resilience. One disabled system or app can send an organization into manual mode, employing tedious workarounds to access information, serve customers, and keep key business functions running.

Operational disruption, in fact, is a top negative consequence resulting from cyber events and breaches, cited by 66% of surveyed organizations in Deloitte Global's survey.[6] And becoming operationally resilient is a growing priority as organizations look to safeguard not only the continuity of operations, but customer trust, business reputation, and revenue—all of which can take a hit when operations are disrupted by a cyber incident. Having always-on cyber capabilities is critical for maintaining an always-on business, improving readiness, resilience, and your ability to bounce back after an incident.

DELOITTE GLOBAL FUTURE OF CYBER

66%

Concerned with operational disruptions

Percentage of surveyed executives cited operational disruption as a top consequence of cybersecurity breaches.

6. Future of Cyber Survey (4th Edition).

FOUR FACTORS THAT SHOULD INFLUENCE YOUR JOURNEY

The AI factor

AI holds tremendous potential to enhance cybersecurity. AI solutions can recognize patterns and trends that other technologies or humans might overlook—identifying difficult-to-detect cyber events early on. They can also perform the "hands on" work of responding to cyber incidents—hunting down malicious code and taking action to remediate it, for example.

And as AI solutions perform their work, they can become more intelligent, learning from their own experience and incorporating those lessons into future actions. They also reduce the manual burdens of humans—letting the workforce focus more on value-added activities such as strategic cyber planning. Given all those possible benefits, understanding the potential of specific AI tools—and where they fit in your process and technology landscape—is essential.

AI, and GenAI in particular, presents a bold new territory for businesses to navigate in the digital era. Emerging AI technologies create risks as well as opportunities. Not only can attackers use them to create highly realistic malicious content and seemingly human interactions—from sinister chatbots to false likenesses and deepfake videos—they can also employ them to seek and identify weaknesses in enterprise security, requiring an additional layer of security and resilience considerations. For example, how will you respond if malware exploits one of your AI-enabled apps to gain access to sensitive data or create chaos in the user experience?

AI, and GenAI in particular, presents a bold new territory for businesses to navigate in the digital era.

FOUR FACTORS THAT SHOULD INFLUENCE YOUR JOURNEY

Your industry-specific lens

Incident readiness, response, and recovery is not a one-size-fits-all proposition. Each industry has specific needs and different definitions for what constitutes "critical assets." Attackers, meanwhile, may pursue different methods and different assets depending on the industry. It's not always about stealing money. Malicious motives, political or social objectives, and other factors are in play for many cyber attackers.

How will they come after your industry and, specifically, your business? And how will you tailor your incident response strategies and capabilities to address those threats and protect what is most vital to your business? Consider the ways two different industries face two distinct sets of challenges and needs, requiring them to balance and prioritize differently.

Malicious motives, political or social objectives, and other factors are in play for many cyber attackers.

INDUSTRY SPOTLIGHT
AN INTELLIGENT GAME-CHANGER FOR FINANCIAL SERVICES

Layers of regulations and standards—both existing and newly emerging ones—are forcing financial organizations to become more diligent about how they protect, manage, track, and report on customer data and other enterprise data.

At the same time, the amount of data across the industry is exploding, driven by growth in customer transactions and an expanding universe of supporting apps, both internal and external. With those new apps and the industry's ongoing adoption of cloud, the traditional enterprise perimeter is changing, making it more challenging to protect and defend sensitive customer information and, ultimately, financial assets.

For financial institutions, strong, proactive cybersecurity capabilities intersect with needs such as mitigating data breaches, tracking financial crime and enabling forensic analysis, protecting against payment fraud, and preventing compromised identities and account take-overs. Such cyber capabilities also become critical to the resilience of systems and the overall business when major disruptions occur—whether those disruptions involve failures in third-party software, supply chain issues, or some other event.

The amount of data across the industry is exploding, driven by growth in customer transactions and an expanding universe of supporting apps, both internal and external.

INDUSTRY SPOTLIGHT
AN INTELLIGENT GAME-CHANGER FOR FINANCIAL SERVICES

Always-on, AI-enabled capabilities can be a game-changer for the industry. Here's how...

REAL-TIME DEFENSE

AI solutions can provide 24×7 monitoring, detection, and response capabilities, with ML helping proactively identify unusual API patterns and other anomalies. Such capabilities become critical for getting ahead of cyber events that may seem isolated but are actually part of a more sophisticated, globally coordinated attack.

INVESTIGATIVE INSIGHTS

To support auditing of app logs and other log data, always-on capabilities should incorporate solutions such as a security data lake. Such a security lake can centralize siloed data from different parts of the organization and external sources. GenAI technology then can act on that data to intelligently automate incident detection, as well as post-event investigation, which can help reduce mean-time-to-detect (MTTD) to few seconds and mean-time-to-resolve (MTTR) to a few minutes for high-priority incidents. Ultimately, the technology can help organizations become more operationally vigilant and compliant.

EMBEDDING INDUSTRY KNOWLEDGE

While AI can go a long way toward helping to address the complexity in today's financial services landscape, organizations should understand that technology solutions alone cannot solve the industry's specific needs. Enabling truly intelligent, always-on cybersecurity will require an ability to tailor the technologies to the specific needs of financial services. Domain-level knowledge—human knowledge—will be essential for ensuring that AI solutions align with business realities and objectives.

INDUSTRY SPOTLIGHT

"MORE THAN HUMAN" CAPABILITIES FOR LIFE SCIENCES AND HEALTH CARE

Protecting patient information and other sensitive data remains a top priority for life sciences and health care (LSHC) organizations around the world. From DNA data to patient care instructions to payment information, there is no shortage of targets for ransomware attacks or other forms of cyberattacks. There is also no shortage of regulatory scrutiny for the management of that data.

But it is not just data security that is at stake. It is the lives of humans that rely on LSHC systems, devices, and services to operate reliably. Protecting that data and ultimately human lives requires intelligent, always-on capabilities that are more than human.

From DNA data to patient care instructions to payment information, there is no shortage of targets for ransomware attacks or other forms of cyberattacks.

INDUSTRY SPOTLIGHT
"MORE THAN HUMAN" CAPABILITIES FOR LIFE SCIENCES AND HEALTH CARE

Here are some potential applications:

DATA ACCESS MANAGEMENT

Managing and protecting data is a complex and constantly evolving challenge. And the organizational policies that govern access to data only add to that complexity. Who has access to which data, and when? And how may they use it? Using GenAI solutions, organizations can leverage the latest intelligent solutions on a massive scale to monitor data access policies and spot anomalies that indicate potential abuse or unauthorized access of the data.

IN-TRANSIT DATA PROTECTION

Data protection is not limited to ensuring the security of information at rest; it extends to safeguarding data in transit as well. For instance, as a patient transitions from a primary care physician to a specialist or participates in a clinical trial, their medical records move across multiple systems, creating potential points of vulnerability. Leveraging a broad cloud infrastructure and advanced AI capabilities, organizations can continuously monitor data in transit, detect cyber risks in real-time, and promptly respond to potential threats in an effort to contain the risk before any compromise occurs.

RESEARCH GUARD RAILS

Clinical trials and other scientific research projects are data-intensive, often combining data from multiple patients and other sources, as well as engaging support from third parties. The potential for personal or sensitive data to end up where it should not be is a persistent reality that increases the cyber risk. With AI capabilities and a data security lake for centralizing sensitive data, organizations can put guardrails around information, to protect data from external and internal threat actors or inadvertent misuse, and identify vulnerabilities in real time.

ConvergeSECURITY

SUPPORTING END-TO-END ENTERPRISE SECURITY

Looking at cybersecurity through a new lens—one that is more strategic and enabled by intelligent technologies—can help you to keep pace with a rapidly changing and persistent threat landscape. You can begin to unlock a host of business benefits, from increasing visibility into security threats to deploying talent more effectively to enabling innovation through digital transformation initiatives.

To help you fast-track your ability to deploy strategic, intelligent cybersecurity capabilities, Deloitte and Amazon Web Services (AWS) have collaborated to create ConvergeSECURITY.

BROAD AND AI-ENABLED

ConvergeSECURITY makes autonomous security a reality by helping you create an intelligent security environment for sharing threat intelligence powered by GenAI with ML models. It offers a broad cybersecurity solution that brings together:

- AI-enabled cloud security and compliance solutions
- Deep industry-based consulting experience
- Tailored resources
- End-to-end threat management, detection, response, and recovery at the enterprise level

With ConvergeSECURITY, you can take advantage of the flexibility, scalability, and cost benefits of a cloud-enabled IT infrastructure while having an integrated and cohesive set of cybersecurity services.

ConvergeSECURITY
SUPPORTING END-TO-END ENTERPRISE SECURITY

CLOUD INNOVATION VALUE

ConvergeSECURITY provides end-to-end security, working natively on AWS and enabling your enterprise to realize value quickly while accelerating cloud initiatives and digital innovation—providing you confidence in your security posture and peace of mind for the ongoing digital transformation journey.

ConvergeSECURITY brings together the capabilities of Deloitte and AWS in a powerful combination that delivers a bigger impact—through Deloitte's deep industry knowledge and experience plus AWS's leadership in cloud innovation.

ConvergeSECURITY includes:

Managed Extended Detection and Response (MXDR)

Safeguard your enterprise with MXDR by Deloitte as your fully managed cybersecurity solution. Deloitte's experienced specialists operate your security with a powerful combination of market-leading Software-as-a-Service-based threat hunting, detection, response, and remediation capabilities. Deloitte specialists are trained to pursue and respond to threats before they become attacks, helping you reduce the impact to your business.

Incident response and recovery

Embed trust across customers, businesses, and third parties with efficient and effective cyber incident management. Deloitte's incident response and recovery capabilities help you prepare for, respond to, and recover from cybersecurity incidents, safeguarding data, systems, and reputation. With deep industry knowledge and market-leading technology, we can help you achieve cloud transformation for lasting resilience.

ConvergeSECURITY
SUPPORTING END-TO-END ENTERPRISE SECURITY

ConvergeSECURITY includes:

Cyber Analytics and AI Engine (CAE)
Generate higher quality insights with Deloitte's Advanced CAE. The CAE module ingests MXDR-generated telemetry for hunting, incident response, and analytics using AI. Operated by experienced professionals, CAE builds asset visibility and alerting, helping you achieve your desired cyber outcomes.

Cyber Cloud Managed Services (CCMS)
Accelerate your journey on the AWS cloud with Deloitte CCMS, a cloud security service that provides 24/7 security monitoring and protection for essential resources. Gain peace of mind knowing that security is built in from day one, enabling faster cloud transformation.

ConvergeSECURITY unlocks potential benefits across the enterprise, including:

- Eliminate data silos
- Get actionable insights
- Anticipate and prevent attacks
- Enable rapid response and recovery

ConvergeSECURITY brings together the capabilities of AWS and Deloitte.

Leading AWS cloud technologies, including:

Amazon Security Lake (ASL)
The underlying technology that solves the siloed data challenge across the digital estate.

Amazon Bedrock
GenAI and ML are critical to delivering quality data and actionable insights that reduce risk and improve response and recovery.

ConvergeSECURITY
SUPPORTING END-TO-END ENTERPRISE SECURITY

ConvergeSECURITY is being used to help organizations address real threats in the real world now.

ISSUE

A multinational hospitality company wanted to embed security at the heart of its digital transformation efforts. To do that, the organization needed guidance on how to boost cybersecurity data management efficiencies and enable advanced analytics. Finding a cloud-native solution that could improve enterprise security monitoring was a primary goal.

SOLUTION

Deloitte helped the company establish a data lake platform, built on AWS, with a modular design. The solution went beyond on-premises applications, applying security automation across the company's cloud environments.

IMPACT

- Improved migration of data from current-state platforms
- Developed a solution to support net-new security analytic use cases
- Enabled efficient, cost-effective data collection, migration, analytics, and integration across the digital estate
- Adopted a cloud-native AWS solution to replace and augment the current log, storage, search, and analytics solution set

BRINGING ALL THE PIECES TOGETHER

How will you enable more intelligent, more strategic cybersecurity capabilities that position your organization for the future? How will you create a secure enterprise landscape that supports cloud innovation, embeds a competitive business advantage, and provides the confidence your business needs to address tomorrow's threats?

Contact us to get additional insights on cyber transformation, to schedule a demo of ConvergeSECURITY, or to discuss a specific security challenge your organization is facing.

Contacts

Emily Mossburg
Cyber leader, Consulting Services
Deloitte Global
emossburg@deloitte.com

Julie Bernard
Principal,
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
juliebernard@deloitte.com

Simon Philips
Principal
Global FSI Industry Leader
phsimo@amazon.com

Mauraan Schultz
Global HCLS Lead
Amazon Web Services (AWS)
mauraans@amazon.com

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Amazon

Amazon is guided by four principles: customer obsession rather than competitor focus, passion for invention, commitment to operational excellence, and longterm thinking. Amazon strives to be Earth's Most Customer-Centric Company, Earth's Best Employer, and Earth's Safest Place to Work. Customer reviews, 1-Click shopping, personalized recommendations, Prime, Fulfillment by Amazon, AWS, Kindle Direct Publishing, Kindle, Career Choice, Fire tablets, Fire TV, Amazon Echo, Alexa, Just Walk Out technology, Amazon Studios, and The Climate Pledge are some of the things pioneered by Amazon. For more information, visit amazon.com/about and follow @AmazonNews.