NTT DATA

Secure your business success at the speed of AI

Turn cybersecurity into a strategic enabler for your business

Contents

Executive summary

To securely enable business in the age of AI, organizations must undergo a fundamental mind shift around cybersecurity.

Too often, security is treated as a technology stack, a cost and an afterthought — a collection of reactive tools and compliance requirements rather than a proactive enabler of business outcomes. But to confidently navigate a fast-changing, multifaceted environment, cybersecurity needs to be viewed through a business lens, as a strategic enabler tied directly to business performance and growth.

This requires outcome-focused security key performance indicators (KPIs) aligned with business objectives, not technical metrics owned solely by the CISO or CIO.

The new approach to cybersecurity

In this new approach, which is **business-aligned, outcomes-driven, simplified and integrated**, responsibility for risk and security management is shared between security and business leaders in your organization — spanning security controls, technology, processes and people.

This allows you to view cybersecurity not as a constraint but as an enabler of business performance:

- First, embed cybersecurity from the start into business strategy and operations, and measure its impact on business performance to keep it **business-aligned**.
- Next, your cybersecurity operations need to be **outcomes-driven** to help you achieve the security KPIs that align with your business outcomes, such as mean time to detect and respond, time to recover from security incidents, and reduced costs.
- You need to rationalize, standardize and transform your cybersecurity into a **simplified** and future-proof technology stack.
- At the same time, your cybersecurity technology and processes must be seamlessly **integrated** to enable swift, coordinated action — from proactive risk and security management to incident response and recovery.

Additionally, CISOs need single-pane-of-glass visibility into their cybersecurity controls and posture to consistently enforce policies that align with evolving business requirements and help to build stakeholder trust.

In this paper, we share practical guidance to help you turn cybersecurity into a strategic enabler for your business.

Why you need a fundamental shift in your cybersecurity strategy

AI is fast becoming central to business strategy, operations and customer engagement. Organizations are increasingly relying on the seamless adoption of AI to deliver best-in-class digital experiences to their customers, suppliers and employees. To support AI-powered workloads, they are rearchitecting their technology environments, deploying containerized applications, scaling compute-intensive operations across multicloud platforms and using edge devices to make real-time decisions.

However, while AI-enabled digital transformation is delivering clear advantages at an unprecedented speed and scale, it also presents a fundamental challenge: how to secure a constantly changing environment.

In AI-powered digital environments, the traditional concept of a static and reactive security posture no longer applies. Digital assets and infrastructure are interconnected, ephemeral and increasingly autonomous, creating conditions where even small misconfigurations or blind spots can escalate into critical vulnerabilities that cascade rapidly across systems.

A single misconfiguration can escalate into systemic compromise

A single misconfigured software update in a major IT management platform triggered one of the most far-reaching supply chain breaches in history. Threat actors inserted malicious code into a trusted software component, which was then automatically propagated to thousands of organizations worldwide. Thus, what began as a minor oversight in access control rapidly escalated into a systemic compromise.

New risks in a hyperconnected world

It's clear that automation and continuous deployment in a hyperconnected digital ecosystem can amplify not only efficiency but also security risks.

These risks are further compounded by the convergence of IT with OT, edge devices, and IoT and industrial IoT (IIoT) systems. This is especially true in the manufacturing, utilities and transportation industries. As these operational systems become more digitalized and connected, they are a prime target for threat actors looking to exploit nascent security controls. Every connected device and asset is a potential entry point for cyberattacks, and every integration can be a conduit to systemic failure.

Adding to the pressure, attackers have also rapidly evolved their methods. They are using GenAI to automate phishing at scale, generate convincing deepfakes, craft sophisticated prompt-injection attacks and exploit open-source code dependencies. Supply chains, for example, have become attractive targets, with attackers exploiting weak links to bypass hardened perimeters, while disinformation campaigns are creating a new layer of complexity where truth is manipulated at scale.

Compounding the issue is the patchwork of solutions that many organizations have accumulated over time, each addressing a specific threat or control requirement but unable to integrate with other solutions. This lack of integration creates problems such as visibility gaps, operational inefficiencies and inconsistent enforcement of security policies. It also places a growing burden on security teams, who must manage multiple systems, interfaces and alerts.

Rising investment in cybersecurity isn't delivering the expected results

The logical response for most organizations is to increase their cybersecurity investment to counteract this surge in attacks. Global cybersecurity spending is rising, with security services and cloud security among the fastest-growing segments.

However, this rise in spending isn't translating into proportional gains in security postures. In fact, far from it. The reasons are clear: a lack of alignment with business objectives, technology complexity and tool sprawl, integration issues, inefficient operations and talent shortages. Most security environments are an accumulation of tools added incrementally over time, including firewalls and solutions for endpoint protection, cloud security, secure access management and compliance monitoring.

Each serves a purpose, but the lack of cohesion among them creates multiple systemic issues:

- **Lack of business alignment:** When cybersecurity is seen as nothing more than a technology stack, a compliance exercise and an afterthought to business strategy, the result is a reactive security approach that adds friction to business processes and digital experiences.
- **Siloed visibility:** Different tools produce different alerts across different consoles. This creates blind spots and duplicated effort.
- **Inconsistent enforcement:** Security policies applied unevenly across cloud, on-premises, edge and operational environments introduce risk.
- **Operational overload:** Security teams face alert fatigue and a drain on resources as they try to manage multiple disconnected tools.
- **Higher cost and complexity:** Redundant capabilities inflate cost, while integration challenges slow down incident response and remediation.
- **Lack of trust:** Stakeholders often view cybersecurity as a constraint on business performance.

Instead of spending more, we need smarter investments and strategic realignment with business on looking at cybersecurity from a business lens. This demands a fundamental shift in your cybersecurity strategy — from reactive, fragmented and static to continuous, connected and capable of adapting in real time. It means moving toward a cohesive cybersecurity strategy that provides holistic visibility, coordinated responses and future-ready resilience.

In the following pages, we explore how to enable your organization to securely enable businesses to adopt AI, innovation and growth at speed and scale.

How to transform your cybersecurity for the AI era

Organizations must move fast while staying secure. In the rush to deliver AI-powered innovation that enables superior digital experiences, cybersecurity often lags.

Traditional cybersecurity models with fragmented architectures, disconnected toolsets and reactive incident response weren't designed for this kind of velocity or complexity. For example, customer-facing GenAI tools interact with many different public and private application programming interfaces, third-party data sources and cloud services, but legacy security tools cannot keep pace with these changing environments that put sensitive customer information at risk.

The result is a growing tension: The more you scale and diversify your technology stack, the more you struggle to secure it effectively without a modern cybersecurity strategy. You need a business-aligned, outcomes-driven, simplified and integrated approach to defend against known threats while anticipating and adapting to emerging ones. Let's explore the four pillars of this strategy.

1. Implement business-aligned cybersecurity

In the age of AI, where digital transformation underpins every business outcome, cybersecurity must be business-aligned — tightly integrated with strategy, operations and performance objectives. This makes it a driver of innovation, resilience and trust.

When cybersecurity is business-aligned, success is measured not only by the number of incidents prevented but also by how effectively it helps you achieve your organization's goals. This shift redefines the role of cybersecurity from a control function to a strategic capability that protects value creation, customer experience and regulatory confidence. Security leaders collaborate with line-of-business executives to co-own cyber risk and embed protection into every initiative — from AI deployments and product launches to supply chain modernization and customer engagement.

Once security is embedded in decision-making and measured by business outcomes, it becomes a catalyst for growth and, enabling you to innovate confidently and securely.

Business-aligned cybersecurity enables your organization to:

- Embed cybersecurity into business strategy, governance and planning
- Establish shared accountability for cyber risk across lines of business
- Align KPIs with business outcomes such as trust, resilience and efficiency
- Strengthen collaboration between CISOs and business leaders
- Turn cybersecurity into a strategic enabler of sustainable growth

2. Shift to an outcomes-driven approach

In this new approach, cybersecurity performance is measured by outcomes that matter to your business — not just by technical or compliance activity. Instead of tracking the number of alerts or compliance checks, you should align KPIs to business-impact metrics such as:

- Reduced time to detect and respond to incidents
- Reduced incident dwell time and time to recover from security incidents
- Improved critical asset availability and operational resilience
- Reduced supply chain risks and fully secured digital transactions
- Increased customer trust and regulatory confidence

CISOs need to reduce operational costs and make better use of scarce cybersecurity resources to keep improving their security KPIs aligned with these business-impact metrics. In an AI-enabled threat landscape, this calls for the adoption of AI and machine learning to prioritize risks, reduce false alerts, detect threats faster and launch automated responses.

Increasingly, we're also seeing a shift from passive analytics to agentic AI — autonomous, goal-driven systems that can carry out complex security tasks without manual intervention. In practice, this means you can push beyond basic automation and take decisive steps to reduce dwell time (how long an attacker stays undetected within a system after gaining access and before being removed), limit lateral movement and maintain compliance — all without waiting for human input. Whether you're dealing with a supply chain breach or trying to contain a compromised AI workload that is critical to your digital customer experience, agentic AI brings a new layer of precision, speed and scale to your security operations.

3. Simplify and modernize your cybersecurity technology stack

Rather than layering more tools onto an already bloated legacy environment — which might seem logical when faced with growing AI-related risk — you should start by evaluating your current cybersecurity maturity.

Once you understand where you are, you can create a roadmap to rationalize, consolidate and standardize your cybersecurity technology stack and move toward a unified cybersecurity architecture that eliminates redundancy across tools and controls.

This puts the foundation in place for a simplified, modernized cybersecurity technology stack that can secure your AI-powered digital ecosystem today and easily adapt to your future needs.

By streamlining vendors and consolidating overlapping capabilities, you can reduce your total cost of ownership, close visibility gaps and enforce policies consistently across complex environments. This rationalization is especially critical if you're navigating complex multicloud or hybrid landscapes, where visibility and control can easily erode. Streamlining also gives stakeholders assurance that their digital experiences are secure, no matter where data or workloads reside.

4. Integrate your cybersecurity environment

Many cybersecurity environments suffer from operational silos, with different teams running different tools for cloud security, endpoint protection, identity governance and more. This fragmented model hinders collaboration, slows incident response and increases risk exposure.

To be effective, you need to move toward an integrated approach to avoid operating your cybersecurity program as a series of disconnected point solutions. This ensures:

- Consistent policy enforcement and orchestration from cloud to edge
- Unified governance across identity, data, applications, workloads, devices and networks
- A streamlined operational model where technologies and processes are integrated
- Unified reporting with a single-pane-of-glass view into the operational agility and adaptiveness of your cybersecurity program

Integrated cybersecurity will enable your organization to confidently and securely navigate change, innovate, gain a competitive edge and turn cybersecurity into a true strategic advantage.

Transform your cybersecurity with NTT DATA

We use our deep vertical integration, edge-to-cloud capabilities and a comprehensive cybersecurity portfolio to help your organization build a business-aligned, outcomes-driven, simplified and integrated approach to cybersecurity. It's a holistic model that few can replicate, and one designed to enable your business priorities without compromising security.

Cybersecurity must be viewed as an evolving capability that is a strategic business enabler rather than a reactive, one-off solution to a problem. Your security strategy needs to be underpinned by a full suite of lifecycle services that continuously adapt your security posture to your business strategy, operational and technology landscape, and broader threat environment.

To deliver these services, we rely on our global expertise and centers of excellence that combine local accountability with domain expertise tailored to your industry.

Whether you're securing a branch network in Southeast Asia, protecting AI workloads in a German data centre or enabling secure identity access for millions of citizens in California, our platform-first approach can be tailored to secure your specific business use cases so you can focus on innovation and growth without compromising security.

Full-stack capabilities, from edge to cloud

We couple our cybersecurity approach with our full-stack, edge-to-cloud digital infrastructure capabilities, which include:

- Always secure by design, we help you modernize your infrastructure and applications for high-performance AI workloads with embedded controls that protect data in transit, at rest or in use. Our deep experience in multicloud and hybrid architectures helps you achieve flexibility and resilience without sacrificing visibility or compliance.
- From zero trust network architectures to software-defined wide area networking (SD-WAN) and secure edge deployments, we design intelligent, adaptive networks that provide the scale and responsiveness that AI systems demand — and we do this without introducing new threat vectors.
- We deploy dedicated 5G environments to secure remote access at the edge. Private 5G offers ultralow latency, high throughput and reliable connectivity, augmented with end-to-end encryption and integrated threat detection tailored to your environment.

Our end-to-end cybersecurity portfolio helps you simplify and integrate your cybersecurity technology stack and operations to securely enable your business to succeed in the age of AI. We protect your complete digital ecosystem — from applications, data and digital identities to cloud and hybrid data centers, large language models and AI environments, as well as distributed endpoints and networks.

Secured endpoint and network

Protecting a connected enterprise requires endpoint security that spans IT environments as well as OT, IoT and IIoT ecosystems.

Endpoint protection goes far beyond antivirus tools. Using integrated detection and response, encrypted data policies and embedded threat intelligence, you can detect early signals of compromise, isolate affected assets and contain threats before they spread.

In OT, IoT and IIoT environments, passive network monitoring and microsegmentation are crucial. Our industrial security capabilities help you map your asset landscape, continuously monitor for anomalies and implement policies that minimize the impact of an attack, all without disrupting production uptime.

At the network level, you benefit from modern architectures such as zero trust network access and secure access service edge (SASE) that unify networking and security. You gain granular control over who and what has access to your corporate systems and data, with secure connectivity for branch offices, cloud services, remote workers and third-party vendors.

Secured AI, hybrid data center, cloud and operations

Our comprehensive security solutions are tailored for hybrid and multicloud environments, which means you can securely adopt cloud and AI technologies while maintaining control over your data and applications.

A cloud security monitoring platform can help you protect your applications and data across virtual machines, containers and serverless environments. Your workloads are safe regardless of where they run.

Keeping a bank and a drinks manufacturer secure

A state-run bank in Southeast Asia needed to rapidly modernize their infrastructure across more than 1,200 branches and two core data centers. Following an aggressive timeline to support a national rollout, NTT DATA provided advanced secure networking, encrypted connectivity, integrated threat detection and seamless scalability.

Additionally, we helped a global drinks manufacturer transform from on-premises security to cloud-based zero trust security. Our managed SASE service is tailored to each client's needs and maturity level. For this client, we prioritized preemptive actions, proactive risk management and a shift from traditional, hardware-based security to a more flexible, software-defined approach so their infrastructure could adapt more easily to new threats and business needs. This intervention significantly reduced costs while strengthening the manufacturer's security posture and enabling operational efficiencies.

These platforms also continuously audit cloud environments for misconfigurations, drift and compliance violations to reduce the risk of breaches caused by human error or oversight.

As AI becomes increasingly central to your business strategy, NTT DATA facilitates safe and responsible AI adoption at speed and scale, spanning everything from your employees' GenAI use to model protection, application security, infrastructure safeguards and compliance. We ensure that innovation doesn't come at the cost of risk.

With our integrated offensive security services (such as red-teaming and penetration testing), vulnerabilities are proactively identified and remediated before they can be exploited. Hybrid and multicloud environments are governed through a unified lens so you can innovate with control and confidence.

Secure business enablement for an automaker and an insurer

A German car manufacturer was transforming its digital operations and needed to secure more than 40,000 cloud workloads across their engineering, manufacturing and customer service platforms. NTT DATA designed and implemented a tailored solution with workload visibility, posture management and incident-response capabilities. The result was a notable uplift in threat detection, shorter incident response times and better governance across the manufacturer's multicloud architecture.

In India, a leading insurance aggregator, operating under strict regulatory oversight, required deep visibility and control across multiple cloud providers. Through our cloud security posture management and cloud infrastructure entitlement management services, we enabled real-time monitoring, effective access governance, and automation that complied with the requirements of the Insurance Regulatory and Development Authority of India and the country's Digital Personal Data Protection Act. This helped the aggregator reduce their risk exposure, speed up audits and build a secure foundation for growth.

Secured identity, applications and data

We help you build a digital trust framework that balances strong security with a seamless user experience — establishing strong access controls and protecting sensitive information, always compliant with regulatory requirements.

With our identity and access management services — including multifactor authentication, privileged access management, and identity governance and administration — only the right people (and machines) have access to the right resources at the right time. These solutions also support secure federation and single sign-on across on-premises and cloud environments.

Application security becomes foundational. By integrating secure coding practices and automated scanning tools into your DevSecOps lifecycle, you can proactively reduce vulnerabilities and strengthen software resilience.

For data security and privacy, we apply policies around classification, tokenization, encryption and data loss prevention. This protects your data at all times in alignment with compliance mandates such as the European Union's General Data Protection Regulation (GDPR), the US Health Insurance Portability and Accountability Act (HIPAA) and regional privacy regulations.

Security at scale for a public health agency

A public health agency in California needed to provide secure, streamlined access to critical systems for more than 15 million users — including healthcare providers and citizens. We implemented an enterprise identity and access management solution with fine-grained access control, federation across multiple domains, and multifactor authentication for added protection. This helped the agency deliver security and efficiency at scale.

Get in touch to securely enable your business in the age of AI

As AI becomes central to business success, it's critical to secure the digital technologies and infrastructure that power it. From data centers and cloud to networks and edge environments, every layer must be architected with agile, adaptive security built in by design to support safe and scalable AI adoption.

We invite you to connect with our cybersecurity experts to identify opportunities to streamline and strengthen your security posture through a simplified, integrated and outcomes-focused cybersecurity program to support your AI-driven future.

Whether you're building next-generation AI models, deploying real-time intelligence at the edge or securing complex hybrid environments, we can help you protect it all — and turn cybersecurity into a strategic enabler for your business.

Visit our website to begin the conversation.

Learn more

Visit nttdata.com to learn more.

NTT DATA is a global innovator of digital business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have experts in more than 70 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.

NTT DATA


NTT DATA