NTT DATA Technology Foresight 2025

Trend 5: Accelerated security fusion

Visualize a future where security becomes an invisible, adaptive force, always one step ahead.

Contents

Introduction

Accelerated security fusion is a pivotal approach to defending against increasingly complex and sophisticated threats.

By integrating advanced technologies such as threat intelligence, machine learning (ML) and advanced real-time analytics across multiple security domains, organizations can create a unified defense system that empowers them to identify vulnerabilities proactively, streamline response processes and strengthen their security posture across diverse operational environments.

Using capabilities like automated incident response and AI-driven threat detection, accelerated security fusion allows businesses to adapt dynamically to emerging threats, ensuring resilience in an ever-changing risk landscape.

Significance and impact on business

Accelerated security fusion redefines cybersecurity by transitioning it from a traditionally reactive function into a proactive and anticipatory strategy. This paradigm shift allows organizations to safeguard critical assets, ensure operational continuity and bolster resilience in the face of mounting cyber risks. With cybercrime projected to inflict over $10.5 trillion in annual damages on the global economy this year, implementing adaptive and integrated security measures has become a critical business imperative.

Organizations that embrace accelerated security fusion are better positioned to reduce financial loss, protect their reputation and cultivate stakeholder trust in an increasingly interconnected world.

Key drivers

The adoption of accelerated security fusion is driven by several critical factors. The proliferation of connected devices, the rapid expansion of hybrid and multicloud environments, and the growing complexity of regulatory compliance necessitate innovative security solutions capable of addressing modern challenges. Integrated and adaptive security approaches enable organizations to protect sensitive data, meet regulatory requirements and maintain customer trust by delivering consistent and robust defenses across all touchpoints.

In the face of significant challenges, including the escalating prevalence of data breaches, regulatory complexities, and vulnerabilities within global supply chains, accelerated security fusion offers a comprehensive framework for mitigating risks. By leveraging advanced technologies and a unified strategy, businesses can protect critical infrastructure effectively, enhance operational efficiency and establish a strong foundation for long-term growth in an unpredictable digital environment.

Technical explanation

The trend of accelerated security fusion embodies an integrated approach to cybersecurity, merging advanced technologies and methodologies to strengthen an organization's defense against evolving threats, leveraging four key concepts:

1. Proactive cyberdefense

A proactive cyberdefense approach involves anticipating and mitigating cyberthreats before they lead to significant incidents. It uses threat intelligence, ML, cryptographic agility and advanced real-time analytics to predict and prevent potential attacks, minimizing damage and downtime by neutralizing threats early.

2. Digital-identity fortification

Secures user, device and application credentials using methods like multifactor authentication (MFA) and biometric verification. It ensures that only authorized users can access critical systems and data, reducing the risk of credential-based attacks. Protecting digital identities is crucial for maintaining system integrity and security.

3. Information safegarding

Information safeguarding involves protecting sensitive data through encryption, data-loss prevention and access control policies. These measures ensure data integrity, confidentiality and regulatory compliance, and protect information against data breaches.

4. Cyber-risk governance

Cyber-risk governance includes establishing policies, roles and processes for identifying, assessing and mitigating cyber risks. It ensures that security practices align with business objectives and compliance requirements. Effective governance fosters accountability and resilience against cyberthreats.

> “ With these concepts, organizations can build a resilient security posture that proactively mitigates threats, ensures regulatory compliance and maintains trust, ultimately safeguarding their assets and supporting sustained business growth in an increasingly interconnected digital landscape.

Technology

Zero trust architecture implements a security model that requires strict verification for every user and device attempting to access resources, regardless of their location. It enforces the principle of least privilege and continuously validates identities to minimize unauthorized access. By assuming threats could exist both inside and outside the network, zero trust architecture effectively mitigates risks.

Behavioral analytics uses AI to establish a baseline of "normal" user behavior, enabling the detection of anomalies that may reveal insider threats or compromised accounts. It enhances security by identifying unusual activities that traditional methods might overlook. The behavioral baselines can be used to detect zero-day attacks in software supply chains and cloud-native environments, thereby providing enhanced protection for modern applications.

Cyberfusion centers are centralized hubs that integrate threat intelligence, incident response and risk management to provide a unified and proactive cybersecurity strategy. Using technologies such as advanced threat protection, automation and real-time analytics, these centers enable the rapid detection, analysis and mitigation of security incidents. By fostering collaboration among various cybersecurity functions and adopting a holistic approach, cyberfusion centers improve an organization's ability to anticipate, respond to and counteract sophisticated cyberthreats.

Encryption technologies are at the core of cybersecurity and an active research field. See the research highlight for more details.

Business explanation

Accelerated security fusion is reshaping cybersecurity by uniting advanced technologies and methodologies into an adaptable, proactive defense. By dissolving silos within organizations and fostering collaboration across security functions, this approach leverages innovations like AI-driven security to counter increasingly complex cyberthreats with precision and resilience.

Key advantages of this transformative trend include:

Holistic security ecosystem

The unified integration of detection, response, identity and data-protection technologies ensures adaptability to evolving threats, with AI augmenting real-time decision-making and automation.

Enhanced operational efficiency

AI-powered threat detection and automated workflows minimize manual efforts, boost response times and optimize resource allocation.

Business resilience and trust

Proactive risk management, bolstered by AI's ability to predict and neutralize threats, fosters stakeholder confidence and maintains organizational integrity.

Future-ready adaptability

Advanced encryption, zero trust, and risk frameworks, enhanced by AI empower organizations to confront next-generation challenges like quantum computing and hyperconnected systems.

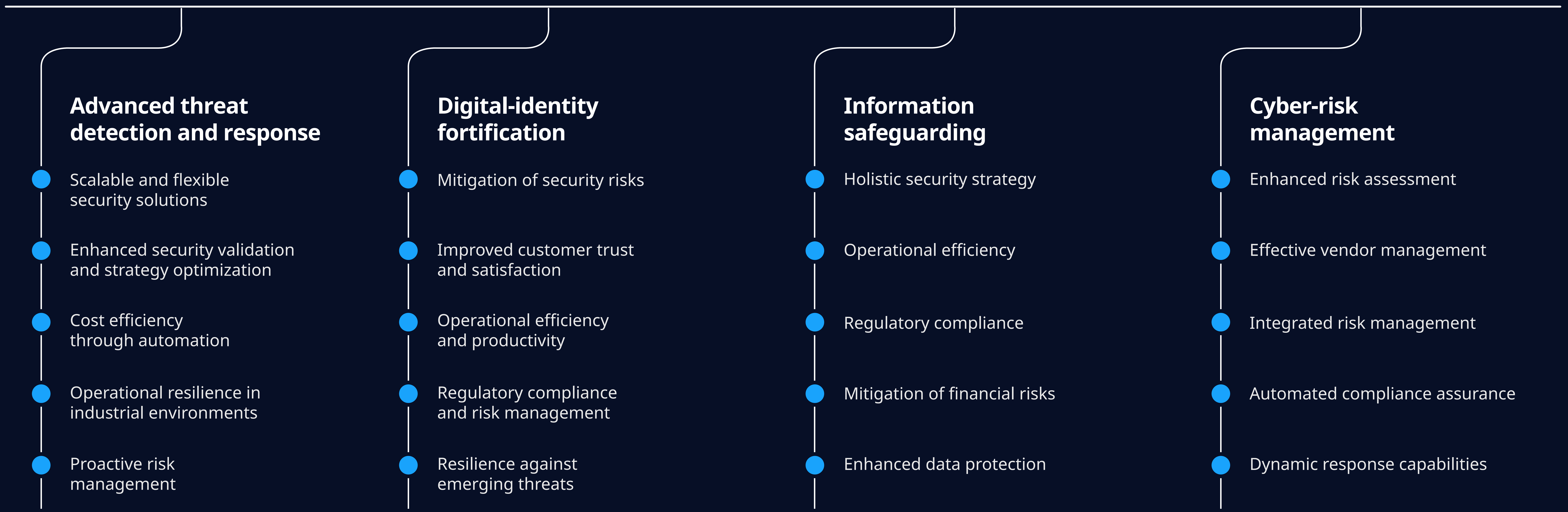
Underlying concepts

Underlying concepts

Organizations that neglect cybersecurity pillars face increased vulnerability to cyberattacks, data breaches, compliance violations and operational disruptions. This negligence can result in significant financial losses, reputational damage and competitive disadvantages in increasingly security-conscious business environments and societies.

Several interconnected elements form the backbone of a robust security strategy, enabling organizations to tackle complex cyberthreats. The accelerated security fusion megatrend represents a holistic approach to cybersecurity that integrates four pillars, explained below.

Accelerated security fusion



Advanced threat detection and response

- Scalable and flexible security solutions
- Enhanced security validation and strategy optimization
- Cost efficiency through automation
- Operational resilience in industrial environments
- Proactive risk management

Digital-identity fortification

- Mitigation of security risks
- Improved customer trust and satisfaction
- Operational efficiency and productivity
- Regulatory compliance and risk management
- Resilience against emerging threats

Information safeguarding

- Holistic security strategy
- Operational efficiency
- Regulatory compliance
- Mitigation of financial risks
- Enhanced data protection

Cyber-risk management

- Enhanced risk assessment
- Effective vendor management
- Integrated risk management
- Automated compliance assurance
- Dynamic response capabilities

Figure 1: Accelerated security fusion — underlying concepts and supporting trends

Underlying concepts

Advanced threat detection and response

Advanced threat detection and response integrates organizational strategies, new technologies and user engagement to address cyber risks proactively. By fostering a culture of preparedness and continuous monitoring, organizations enhance their ability to swiftly detect, respond to and mitigate threats.

> “ AI-powered tools elevate these defenses, enabling businesses to tackle both known and emerging challenges in a rapidly evolving digital landscape.

Scalable and flexible security solutions

- Organizations require adaptable defenses to address the complexities of modern cybersecurity.
- Scalable solutions like MDR services and real-time analytics help businesses remain secure while aligning with growth strategies. Flexible approaches ensure continued protection in the face of ever-changing threats.
- Cloud security services like AWS Shield provide scalable solutions that protect against distributed denial-of-service (DDoS) attacks and adapt to business growth. These services include automated monitoring and real-time threat detection, ensuring robust security as businesses expand.

Enhanced security validation and strategy optimization

- Regularly testing and refining cybersecurity measures keeps defenses strong against evolving threats. AI-powered analytics provide actionable insights, enabling organizations to continuously optimize their security strategies and meet compliance requirements.
- Solutions like Darktrace use ML algorithms to detect anomalous behavior and provide insights that allow organizations to strengthen their security strategies.

Cost efficiency through automation

- Automation reduces manual intervention, enabling faster incident responses and lower operational costs. AI-driven tools, such as breach and attack simulations, detect threats and optimize resource allocation, ensuring the effective management of cybersecurity budgets.
- Cortex XSOAR (formerly Demisto) helps organizations automate incident response workflows, significantly reducing the time needed to contain and remediate security incidents. This automation enhances efficiency and allows security teams to focus on more strategic tasks.

Operational resilience in industrial environments

- In sectors reliant on operational technology (OT), safeguarding infrastructure is critical. Advanced detection systems identify vulnerabilities across IT and OT environments, preventing disruptions and enabling seamless integration while ensuring compliance with industry regulations.
- Companies like Honeywell offer integrated security solutions that protect these systems from cyberthreats, helping to prevent unauthorized access and ensure operational continuity in critical environments.

Proactive risk management (PRM)

- Integrating cybersecurity into organizational strategies builds resilience against potential threats. Proactive measures, such as managed detection and response (MDR) and threat intelligence, enable businesses to identify risks early, minimize disruptions and protect assets. This commitment to data security fosters customer trust.
- To further strengthen these measures, adversarial ML defense techniques are employed, enhancing AI-powered tools to counter manipulative attacks designed to exploit weaknesses in AI models.
- This proactive integration not only maintains system integrity but also fosters customer trust by ensuring that emerging and advanced threats are effectively managed.

Underlying concepts

Digital-identity fortification

Digital-identity fortification is critical to safeguarding sensitive information and ensuring secure access to digital platforms. By enhancing identity and access management (IAM), organizations not only protect against breaches but also create seamless user experiences that drive customer loyalty.

> “ AI tools play a central role in this transformation, enabling the real-time detection of anomalies and delivering frictionless authentication.

1 Mitigation of security risks

Passwordless authentication and MFA reduce risks associated with traditional passwords, lowering the chances of credential theft and phishing.

These security measures enhance customer trust, essential for maintaining a competitive edge, and help prevent financial losses due to data breaches.

Integrating AI tools allows for real-time threat detection and swift responses, further improving security resilience.

By focusing on these strategies, organizations not only mitigate security risks but also strengthen their market position and foster customer loyalty.

2 Improved customer trust and satisfaction

Customers increasingly demand security and privacy for their personal information due to rising concerns about data breaches and identity theft. To meet these expectations, businesses must create secure systems that prioritize user trust. Implementing user-friendly identity verification methods boosts customer confidence. When customers feel their data is protected, they're more likely to engage with and remain loyal to a brand. A seamless authentication process enhances satisfaction, leading to increased loyalty and revenue growth.

AI technologies can further enhance customer trust by offering personalized verification processes. By analyzing user behavior for anomalies, AI ensures security measures are effective yet frictionless, helping organizations proactively address potential concerns.

3 Operational efficiency and productivity

Enhancing operational efficiency is crucial for organizations to remain competitive in today's fast-paced business environment. Employees need quick, secure access to resources, supported by robust security measures that protect against evolving cyberthreats.

Implementing zero trust management ensures continuous verification of users and devices while reducing repetitive security checks that slow operations.

Streamlining access controls and eliminating traditional password management allows employees to focus on their tasks, boosting productivity and satisfaction.

Additionally, integrating AI technologies automates identity verification and access management, analyzing user behavior to provide seamless access and reduce friction in the authentication process.

4 Regulatory compliance and risk management

As data protection and privacy regulations tighten, organizations must prioritize compliance to protect customer information and avoid penalties. Customers expect transparency, making adherence to regulatory standards essential for building trust.

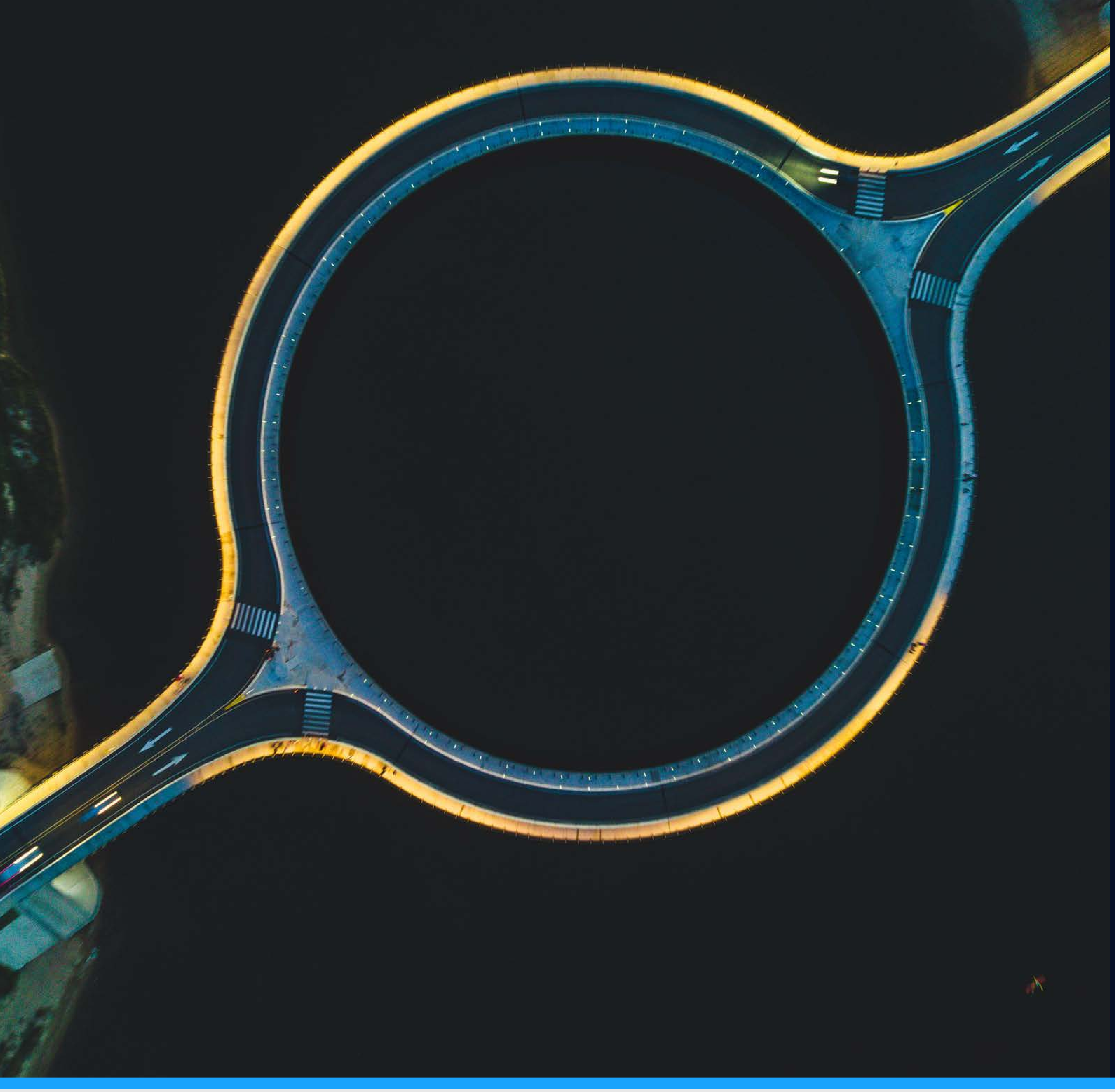
Implementing advanced identity verification technologies allows organizations to meet regulatory requirements efficiently, ensuring accurate record-keeping and streamlined reporting for easier audits. A proactive compliance approach reduces costly fines and enhances reputation.

Integrating AI further strengthens compliance by automating monitoring and reporting. AI can quickly identify compliance risks and detect anomalies in user behavior, ensuring real-time adherence to regulations and improving operational efficiency.

5 Resilience against emerging threats

Cyberthreats are becoming increasingly sophisticated, requiring organizations to enhance defenses to protect sensitive data and ensure continuity. Robust security measures are essential to foster resilience and maintain customer trust.

Adopting identity management strategies like passwordless systems and MFA enables businesses to effectively counter emerging threats. A zero trust model enhances security by promoting the continuous monitoring of user behavior for early detection of suspicious activities.



Underlying concepts

Information safeguarding

Information safeguarding involves measures designed to protect sensitive data from unauthorized access and breaches, ensuring the security of personal and organizational information.

Companies that prioritize data security can attract customers by demonstrating their commitment to privacy, fostering trust and loyalty in a data-conscious marketplace.

> “Additionally, employing advanced security practices enhances the framework by enabling continuous monitoring and management, which provides a robust defense against evolving cyberthreats.

Enhanced data protection

- As organizations increasingly depend on digital data, protecting sensitive information has become essential for building customer trust and loyalty.
- Advanced encryption techniques safeguard data at rest and in transit, effectively preventing unauthorized access and significantly reducing the risk of data breaches.
- Integrating AI into data-protection strategies strengthens security by identifying patterns and detecting anomalies, allowing for swift responses to potential breaches.
- The threat of "harvest now, decrypt later" attacks, where encrypted data is stolen with the hope of future decryption by more advanced technologies like quantum computers, necessitates the use of safeguards such as tokenization and post-quantum cryptography to secure data against future threats.

Mitigation of financial risks

- In light of increasing data breaches, organizations encounter significant financial risks that threaten their stability and reputation.
- Using network tokenization reduces those risks by replacing sensitive data with nonsensitive tokens, making stolen data less valuable.
- Adopting AI enhances risk mitigation by analyzing patterns for early detection of vulnerabilities, enabling quick responses to threats.
- Ultimately, the mitigation of financial risks is vital for safeguarding organizational stability and customer trust through solutions like tokenization and AI.

Regulatory compliance

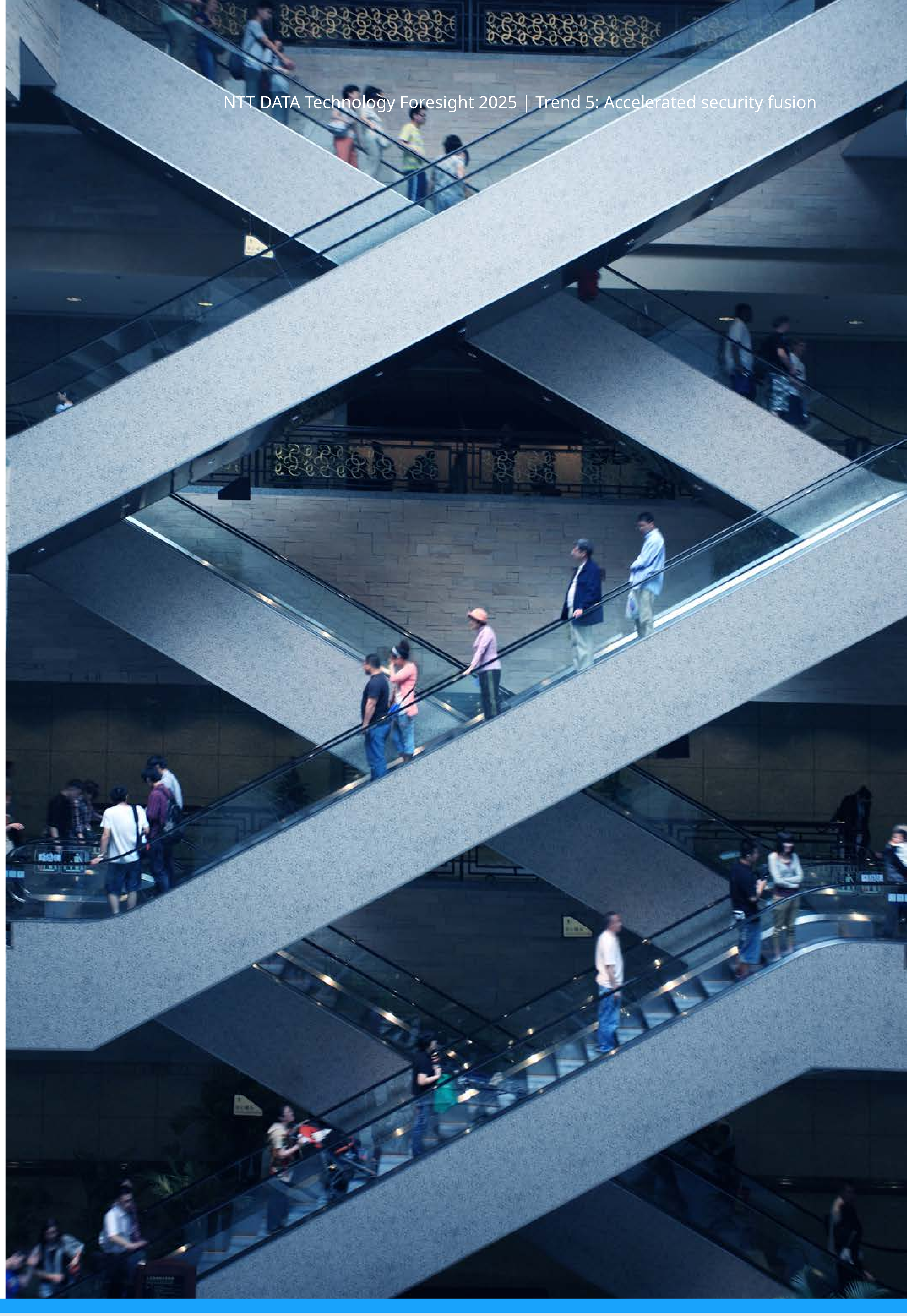
- As data privacy regulations like GDPR, HIPAA and CCPA evolve, organizations must prioritize compliance to protect consumer information.
- Implementing data security platforms and cloud security posture management (CSPM) enables the effective monitoring and management of data security configurations, ensuring adherence to legal requirements.
- Automation monitoring through AI analyzes data to identify compliance risks and ensures that security configurations align with legal standards.
- Achieving regulatory compliance is essential for protecting consumer data and maintaining public trust, while advanced security solutions and AI enhance organizational effectiveness.

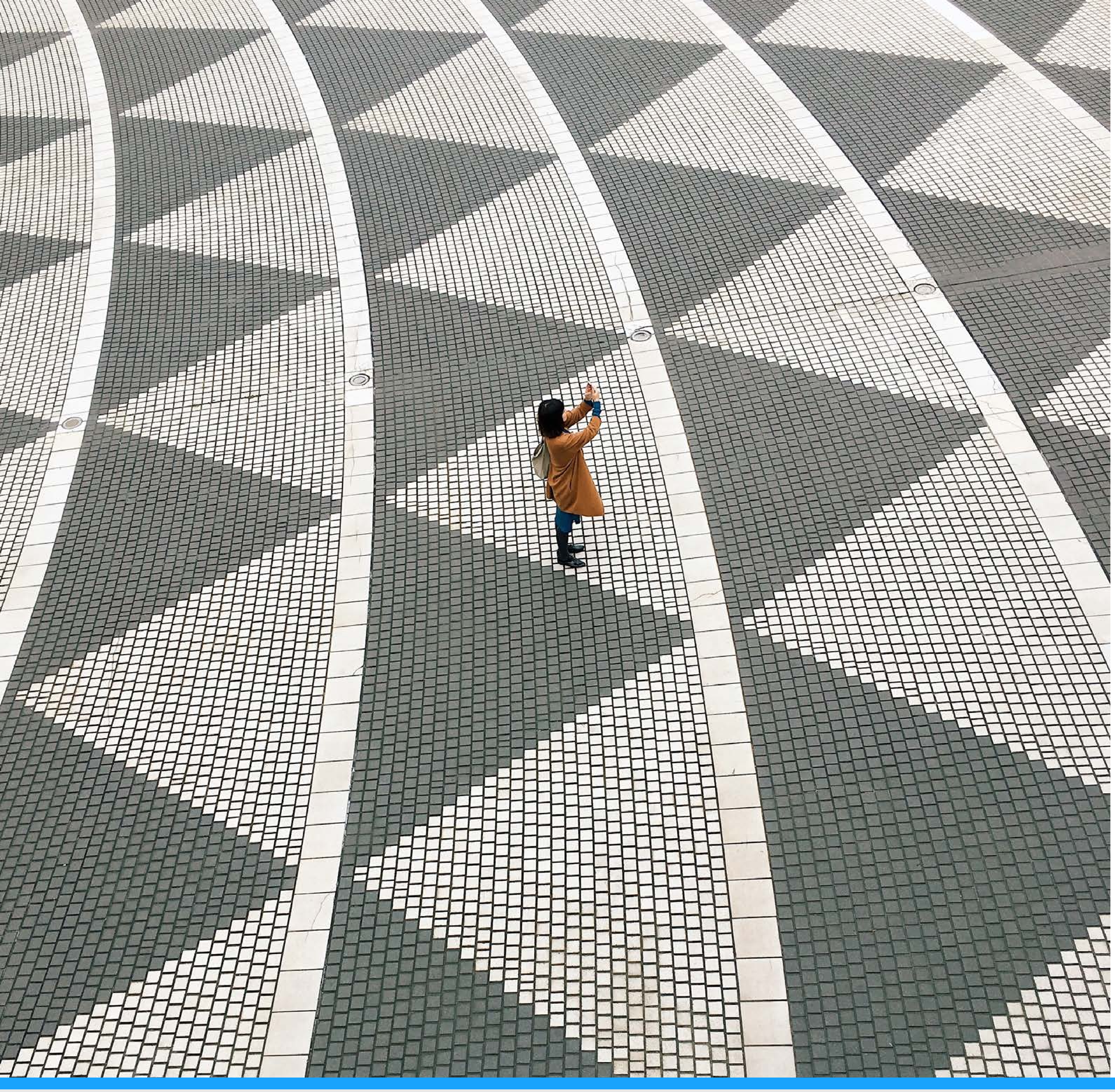
Operational efficiency

- Organizations face increasing security threats while striving to maintain operational efficiency in a rapidly changing digital landscape.
- Cloud-native application protection platforms (CNAPPs) and CSPM provide centralized security management that streamlines operations and automates monitoring, enhancing incident response times.
- Incorporating AI into security strategies improves operational efficiency by automating repetitive tasks and providing real-time analytics for faster threat detection.

Holistic security strategy

- In today's environment, organizations must adopt a comprehensive approach to security to protect critical assets from complex cyberthreats.
- By integrating advanced encryption techniques, network tokenization and robust data security platforms, organizations create a multilayered defense against cyberthreats.
- Incorporating AI into this strategy significantly improves threat detection and response times, offering real-time insights into potential vulnerabilities.





Underlying concepts

Cyber-risk management

Cyber-risk management provides organizations with a structured approach to identifying, assessing and mitigating risks in an increasingly complex threat environment.

> “AI integration enhances these processes, enabling businesses to stay ahead of emerging vulnerabilities and maintain stakeholder confidence.

Enhanced risk assessment

- Comprehensive risk assessments inform decision-making by quantifying potential threats and prioritizing resources. AI tools analyze large datasets in real time, uncovering patterns and vulnerabilities that might otherwise go unnoticed. This enables the precise allocation of resources and strengthens overall security.
- Mastercard's Decision Intelligence uses AI and ML to analyze transactions in real time, detecting potential fraud by evaluating various data points and cardholder behaviors. This system helps identify and prevent fraudulent activities before they escalate.

Effective vendor management

- Third-party vendors often introduce significant risks to an organization’s ecosystem. A strong vendor risk management strategy ensures continuous monitoring of their security measures, aligning with regulatory requirements. AI-driven tools automate this process, enhancing oversight and trust.
- RiskRecon, a Mastercard company, uses AI to continuously monitor and assess third-party vendors' cybersecurity. Its platform automatically scans public-facing systems, analyzes security practices, and delivers real-time risk assessments.

Integrated risk management

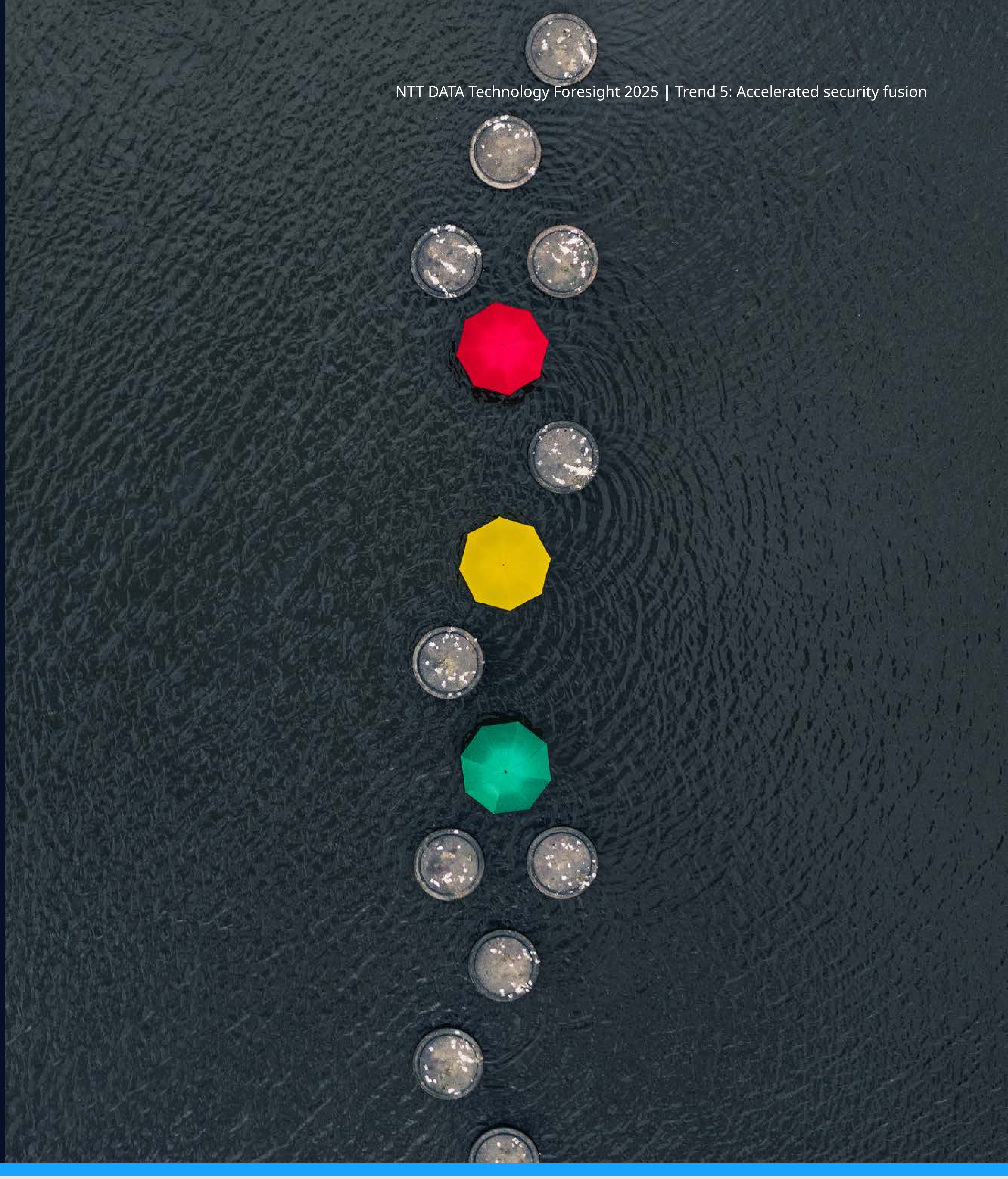
- Siloed risk management approaches can miss interconnected vulnerabilities. Integrated risk management (IRM) consolidates these efforts across functions, providing a unified view of risk exposure. AI improves IRM by automating assessments and generating actionable insights.
- ServiceNow's IRM platform uses AI and ML to consolidate risk data, prioritize risks, generate real-time insights, automate assessments and provide a unified dashboard for enhanced visibility across the organization.

Automated compliance assurance

- With regulatory landscapes constantly evolving, organizations must adopt proactive compliance strategies. AI technologies automate monitoring and reporting, reducing manual effort and ensuring real-time adherence to legal standards. This protects organizations from penalties and reinforces stakeholder confidence.
- OneTrust, a privacy management platform, uses AI and ML to help organizations comply with GDPR and HIPAA by scanning and classifying data, identifying compliance risks in real time, automating access requests and consent management and generating automated audit reports.

Dynamic response capabilities

- In today's fast-paced environment, organizations must adapt quickly to new threats. AI enables dynamic risk management by automating threat detection and accelerating incident response. This agility ensures operational continuity and enhances trust in the organization's ability to protect sensitive information.
- Microsoft's Copilot for Security leverages AI to analyze incidents, provide contextual insights, prioritize threats and recommend containment strategies, enabling faster and more effective decision-making in cybersecurity operations.



Tech radar

Tech radar

In the constantly changing tech landscape, keeping up with the latest developments is essential, not just advantageous.

Continually analyzing technology trends and tracking their evolution will help you anticipate changes and prepare yourself for upcoming shifts.

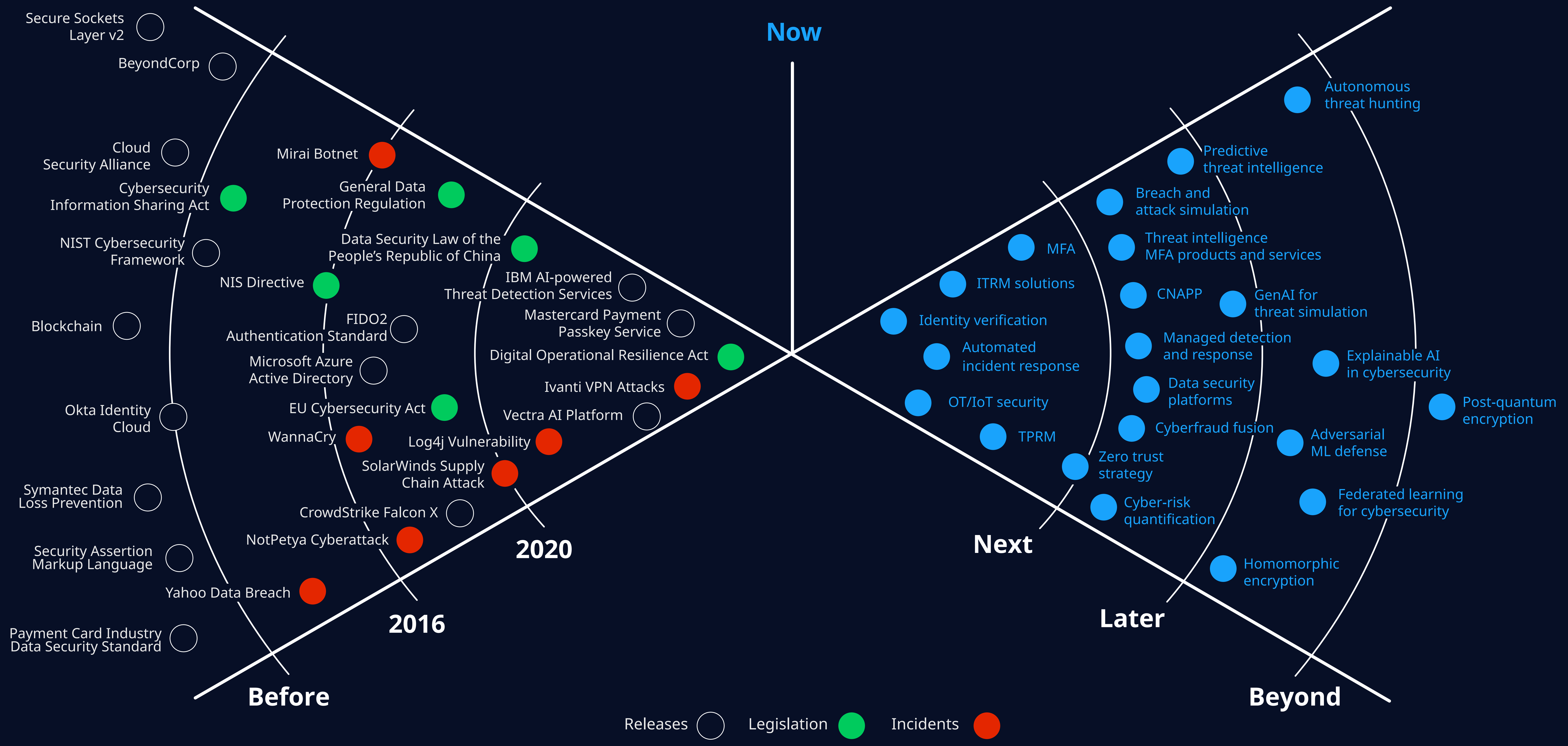

Now
Before
2016
2020
Next
Later
Beyond
Secure Sockets Layer v2
BeyondCorp
Cloud Security Alliance
Cybersecurity Information Sharing Act
NIST Cybersecurity Framework
Blockchain
Okta Identity Cloud
Symantec Data Loss Prevention
Security Assertion Markup Language
Payment Card Industry Data Security Standard
Mirai Botnet
General Data Protection Regulation
NIS Directive
FIDO2 Authentication Standard
Microsoft Azure Active Directory
EU Cybersecurity Act
WannaCry
CrowdStrike Falcon X
NotPetya Cyberattack
Yahoo Data Breach
Data Security Law of the People's Republic of China
IBM AI-powered Threat Detection Services
Mastercard Payment Passkey Service
Digital Operational Resilience Act
Ivanti VPN Attacks
Vectra AI Platform
Log4j Vulnerability
SolarWinds Supply Chain Attack
MFA
ITRM solutions
Identity verification
Automated incident response
OT/IoT security
TPRM
Predictive threat intelligence
Breach and attack simulation
Threat intelligence MFA products and services
CNAPP
Managed detection and response
Data security platforms
Cyberfraud fusion
Zero trust strategy
Cyber-risk quantification
Autonomous threat hunting
GenAI for threat simulation
Explainable AI in cybersecurity
Post-quantum encryption
Adversarial ML defense
Federated learning for cybersecurity
Homomorphic encryption
Releases ○
Legislation ●
Incidents ●

Figure 2: Tech radar — past and future technology

Future tech: now

A **Identity verification**
The process of confirming a person’s identity by analyzing official documents, verifying live presence, and matching the individual to the document.

B **OT/IoT security**
Protects interconnected operational systems and IoT devices from cyberthreats and operational risks, securing hardware, software and networks.

C **Automated incident response**
Centralized systems that use automation to streamline and accelerate incident routing, resolution and collaboration.

D **IT risk management (ITRM) solutions**
Tools for managing IT risks, supporting compliance, regulatory requirements and cyber-risk assessment through governance workflows.

E **Multifactor authentication (MFA)**
Security method requiring multiple forms of verification, such as biometrics, tokens or passwords, for access control.

F **Third-party risk management (TPRM)**
Tools for identifying, assessing and managing risks associated with external vendors, suppliers and partners.

G **Zero trust strategy**
A security framework that enforces strict, adaptive access controls based on user identity, context and asset sensitivity, eliminating implicit trust.

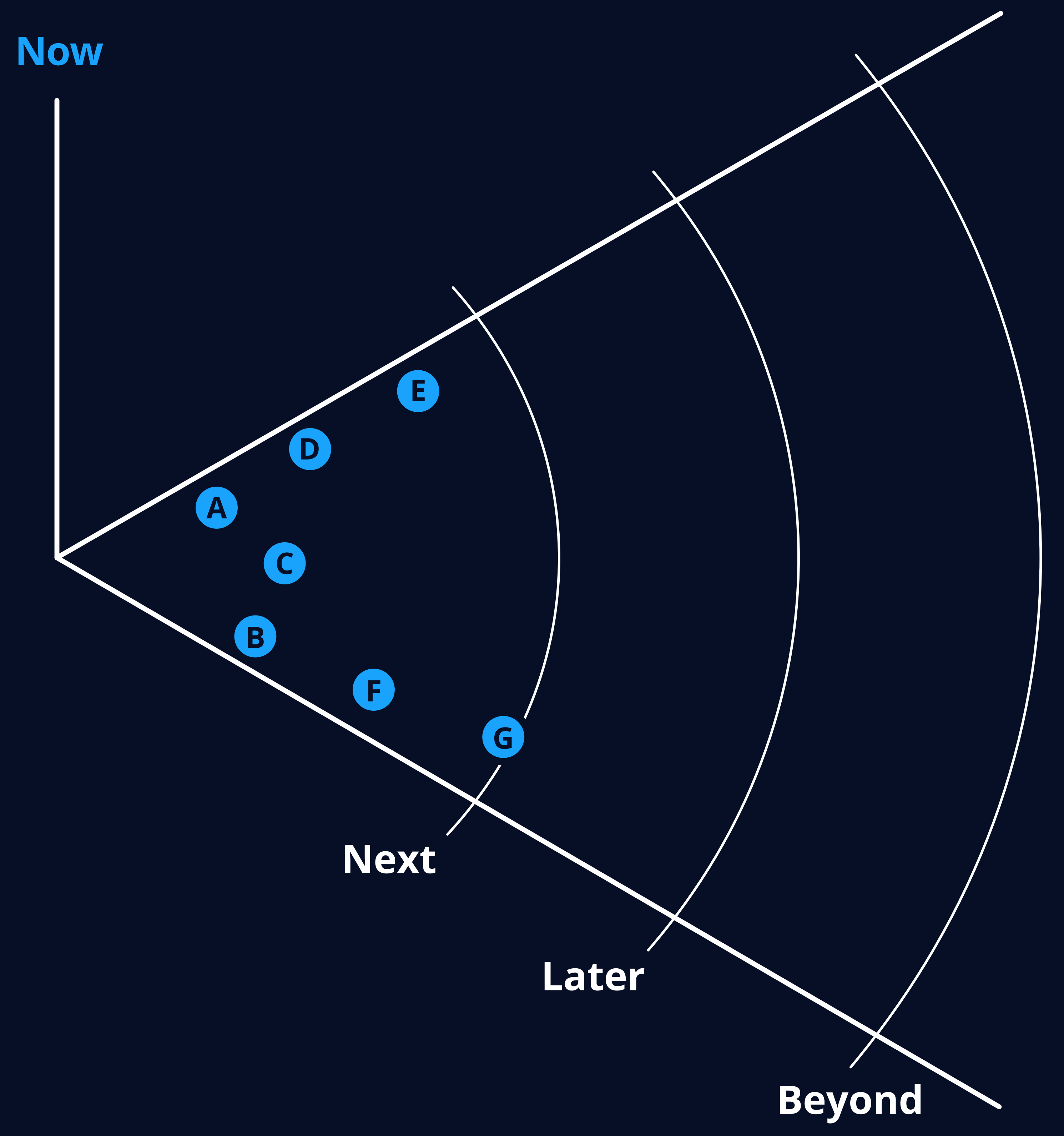


Figure 3a: Tech radar — future technology

Future tech: next and later

H **Breach and attack simulation (BAS)**
Tools that simulate cyberattacks to test organizational defenses, identify vulnerabilities and improve security posture.

I **Threat intelligence products and services**
Systems providing insights into the cyberthreat landscape by analyzing tactics, techniques and adversaries to enhance preparedness.

J **CNAPPs**
Integrated tools that secure cloud-native applications by combining workload protection, security posture management and application security.

K **MDR**
Services that proactively detect and respond to cyberthreats through advanced analytics, threat hunting and predefined workflows.

L **Data security platforms (DSPs)**
Solutions aggregating data protection requirements, including data discovery, masking, encryption and access controls across ecosystems.

M **Cyberfraud fusion**
Integrated approach combining cybersecurity and fraud prevention strategies to address evolving fraud tactics and improve response.

N **Cyber risk quantification (CRQ)**
Method of assessing risk exposure in business terms, such as financial impact or operational disruption, using mathematical models and historical data.

O **Homomorphic encryption**
Encryption method allowing computations on encrypted data without decryption, ensuring privacy during processing.

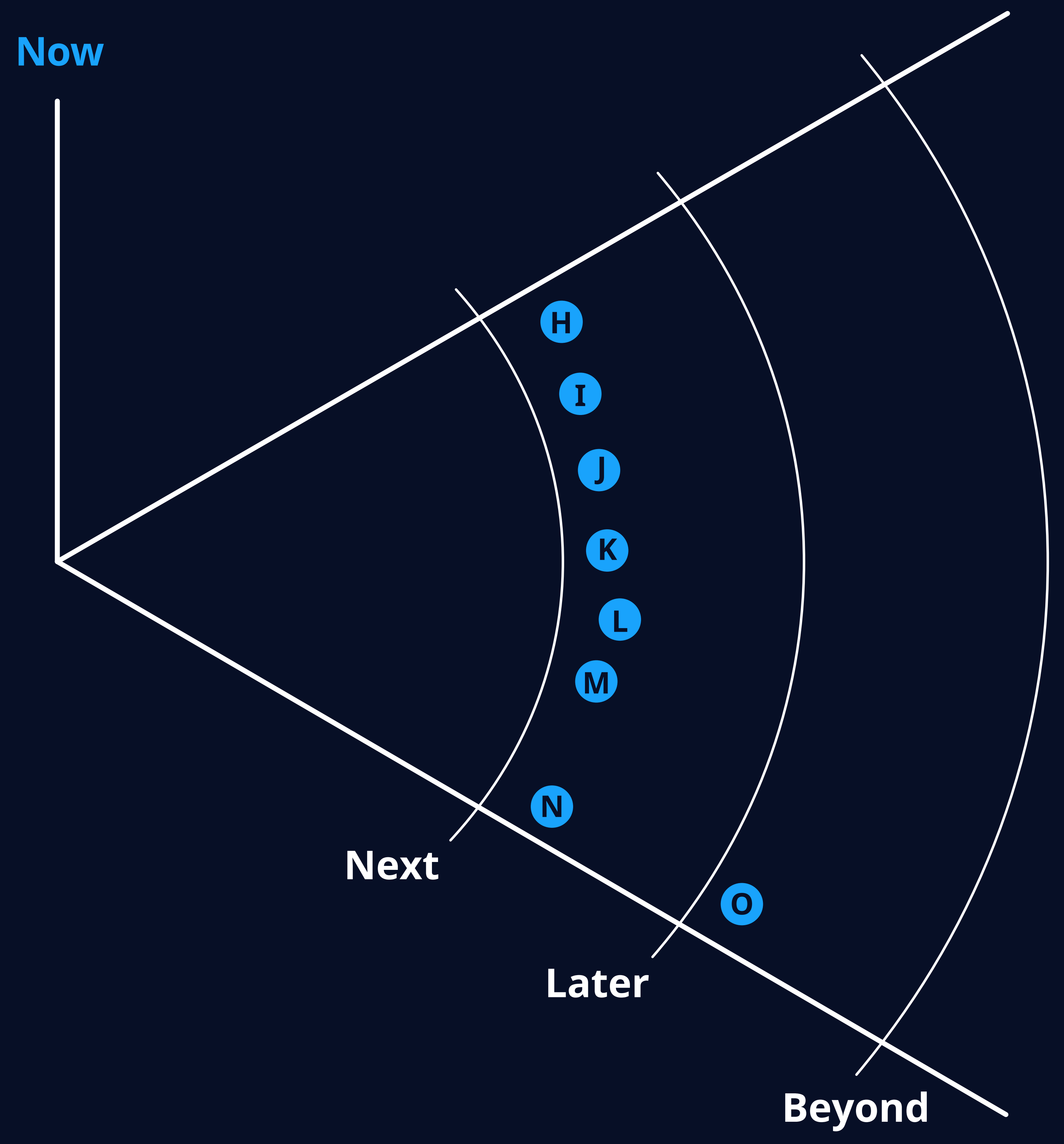


Figure 3b: Tech radar — future technology

Future tech: later and beyond

P **Post-quantum encryption (PQE)**
Cryptographic techniques designed to withstand attacks from quantum computers, ensuring long-term data security.

Q **Predictive threat intelligence**
AI-powered tools that analyze historical data and real-time feeds to forecast and prepare for future cyberthreats.

R **Generative AI for threat simulation**
AI-driven systems that create realistic attack scenarios to test and improve an organization's defenses

S **Autonomous threat hunting**
Fully AI-driven solutions that proactively search for vulnerabilities and threats without human intervention.

T **Adversarial ML defense**
Techniques to identify and mitigate manipulative attacks on AI models designed to exploit their weaknesses.

U **Federated learning for cybersecurity**
A collaborative AI training approach that protects sensitive data by sharing model updates instead of raw data.

V **Explainable AI in cybersecurity**
Tools and frameworks that make AI-driven cybersecurity decisions interpretable and transparent to users and regulators.

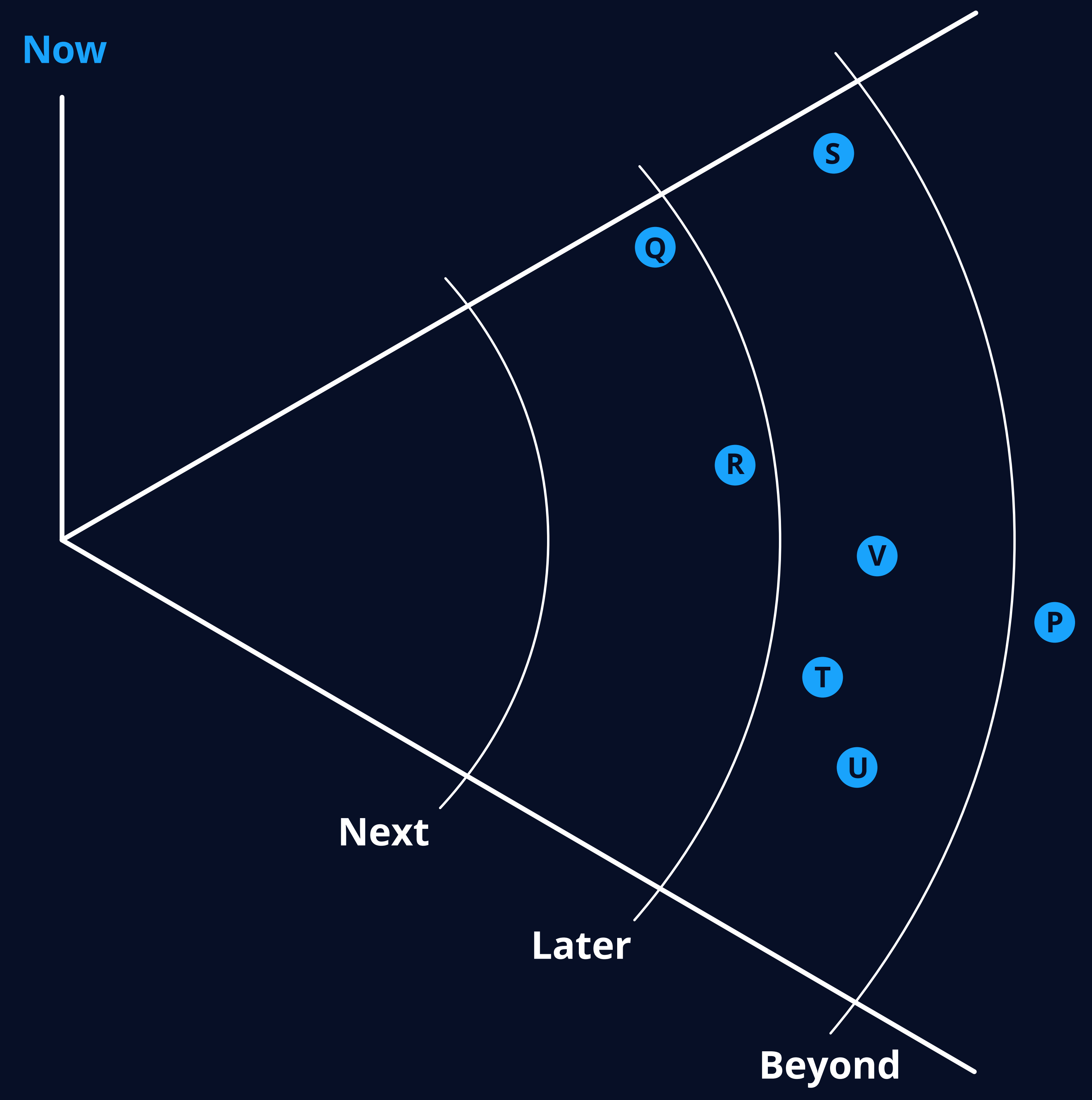
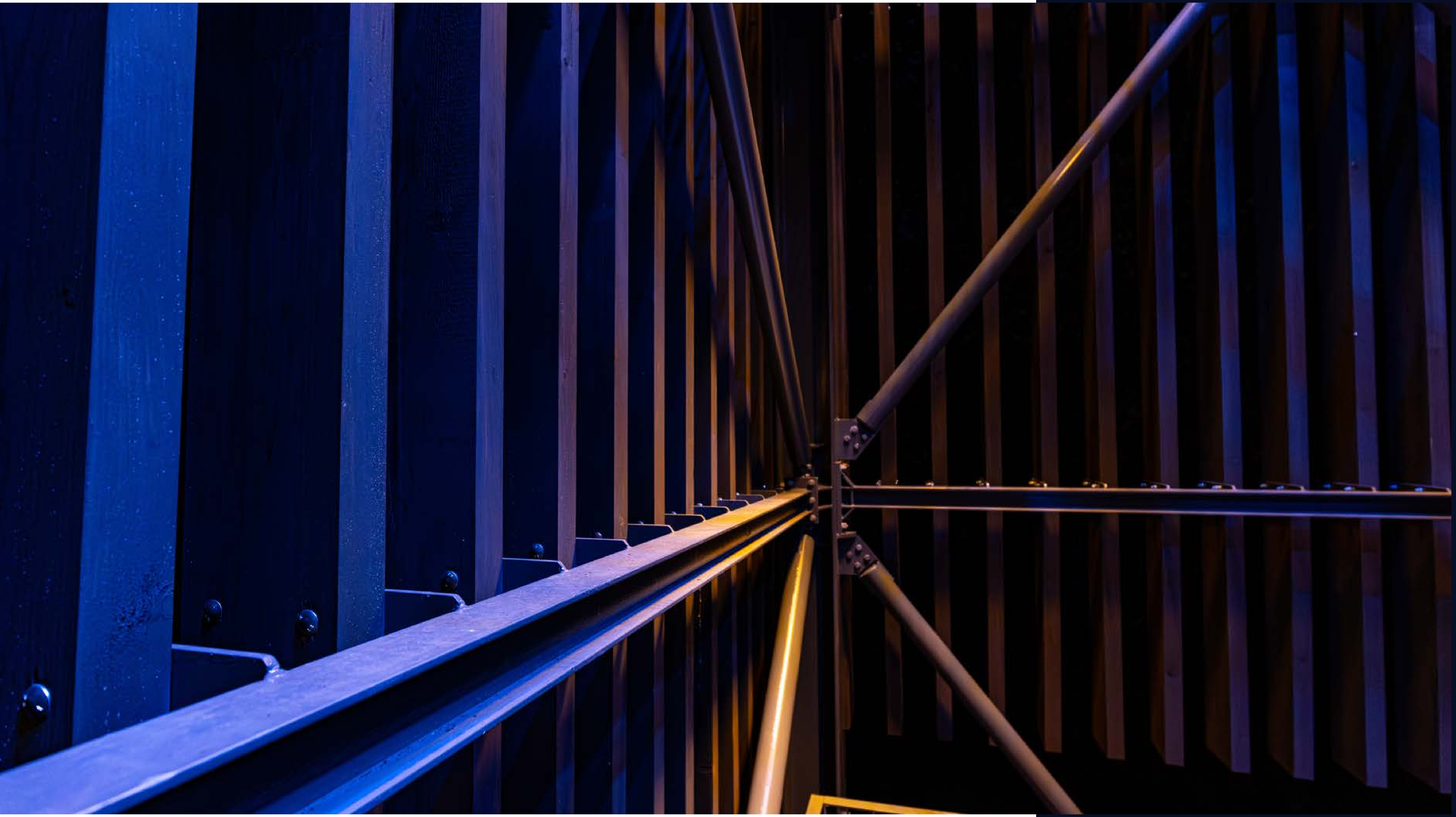


Figure 3c: Tech radar — future technology

R&D highlight



R&D highlight

Innovative encryption technologies

The ever-evolving digital landscape necessitates robust encryption technologies to safeguard against sophisticated cyberthreats.

NTT's research focuses on next-generation encryption methods designed to meet the demands of various applications.

Attribute-based encryption

This revolutionary paradigm combines encryption with attribute-based access control, allowing access to encrypted data based not just on a private key but also on a set of attributes.

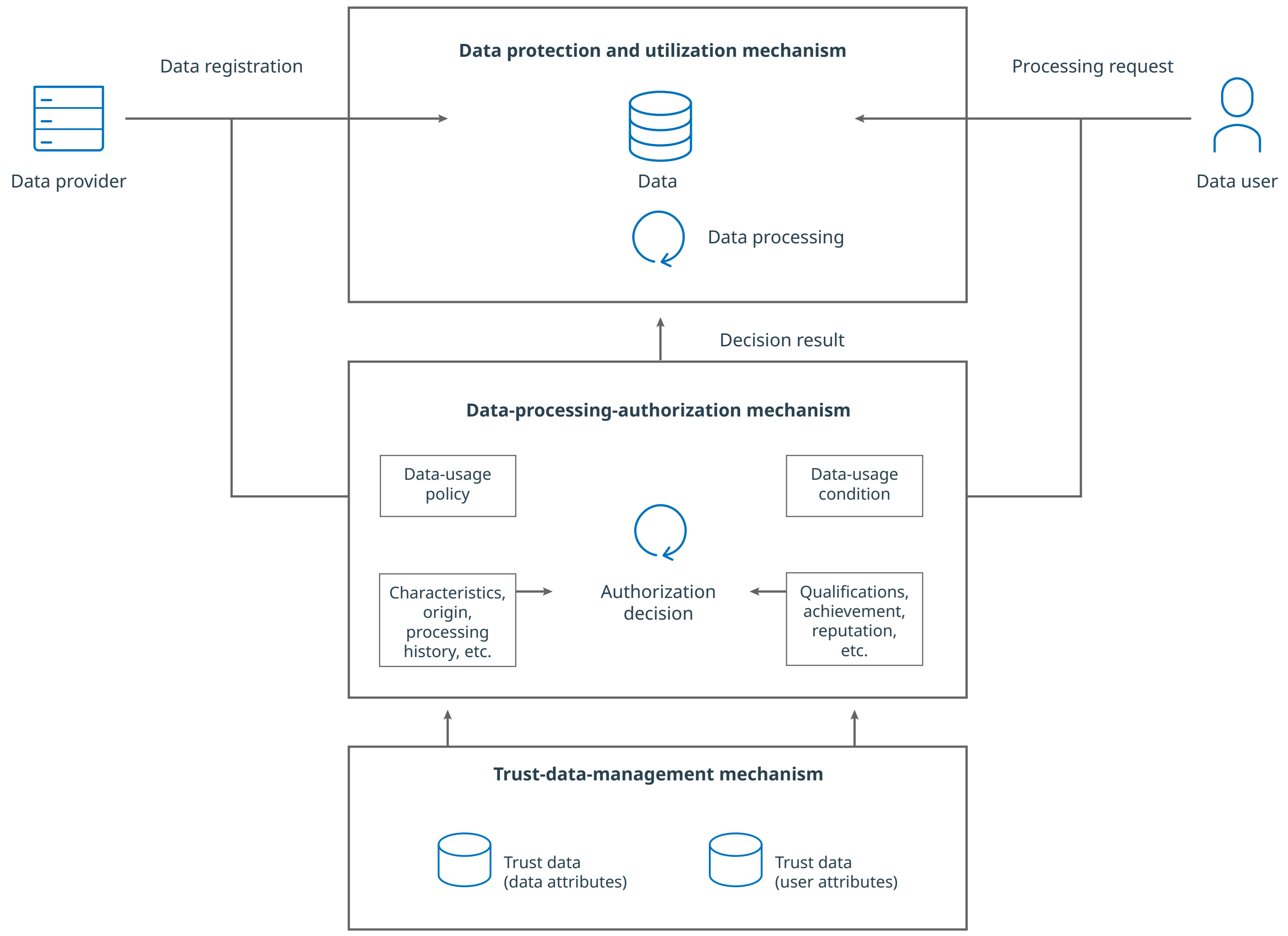
This enables the definition of flexible access policies based on a variety of attributes, such as user role, geographic location or access time, thus offering a more granular control over sensitive data in different scenarios like content distribution, secure data-sharing and privacy-preserving transactions.

Homomorphic encryption

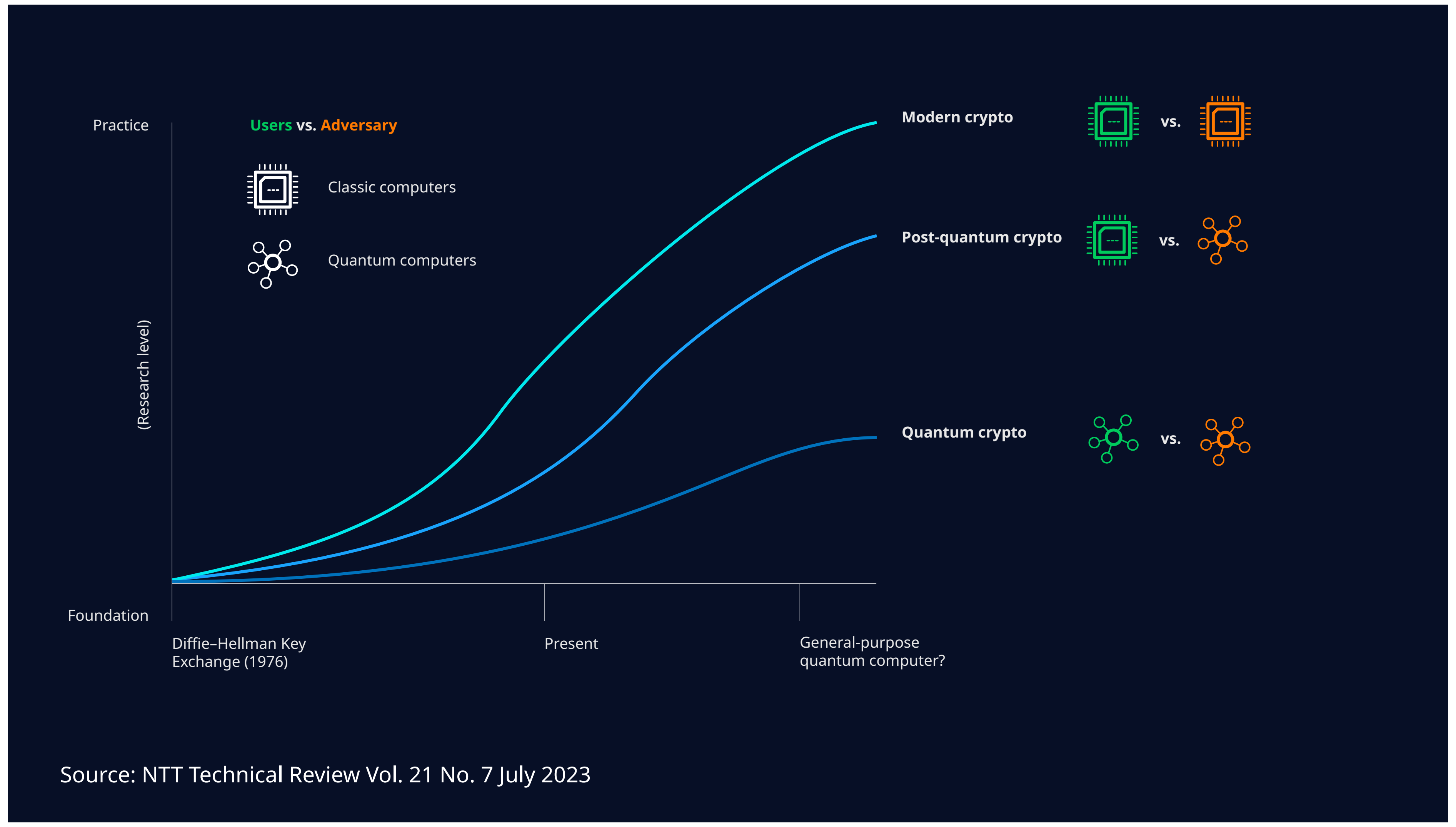
NTT is pioneering research into fully homomorphic encryption, focusing on enabling computations on encrypted data without requiring decryption. Arithmetic operations, such as addition and multiplication, can be performed directly on ciphertexts (the result of encrypting plaintext), providing a powerful mechanism for processing sensitive information securely. This is particularly beneficial for applications in cloud computing, as data can be processed by external servers without exposing the underlying information, thereby ensuring privacy and compliance with data protection regulations.

Post-quantum cryptography

In response to the growing threat posed by quantum computers, which have the potential to break current public-key encryption schemes, NTT is investing in post-quantum cryptography research. By combining advanced security techniques with quantum key distribution, NTT provides robust end-to-end security solutions. These innovative approaches are designed to protect today's encrypted data from future quantum attacks, thereby ensuring long-term security and maintaining trust in digital communications.


Data registration
Data protection and utilization mechanism
Processing request
Data provider
Data
Data user
Data processing
Decision result
Data-processing-authorization mechanism
Data-usage policy
Data-usage condition
Characteristics, origin, processing history, etc.
Authorization decision
Qualifications, achievement, reputation, etc.
Trust-data-management mechanism
Trust data (data attributes)
Trust data (user attributes)

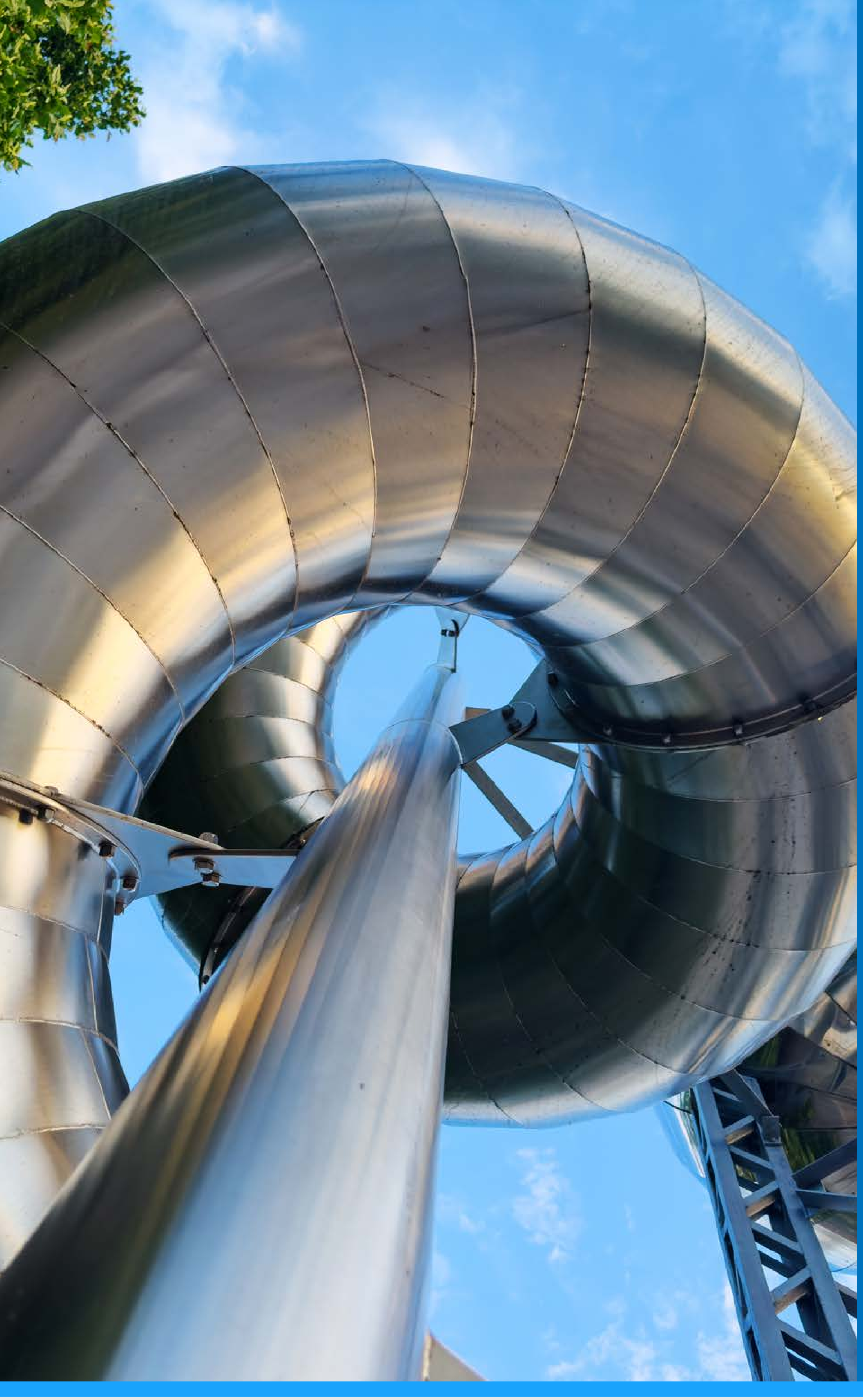
Source: NTT Technical Review Vol. 19 No. 6 July 2021



Source: NTT Technical Review Vol. 21 No. 7 July 2023

Figure 4: Innovative encryption technologies

Quantification



Relevant financials

Accelerated security fusion

Market size, 2024:

$26.9 billion

Market size growth, 2023–2024 (YoY):

+10.6%

Forecast CAGR, 2024–2030:

11.3%

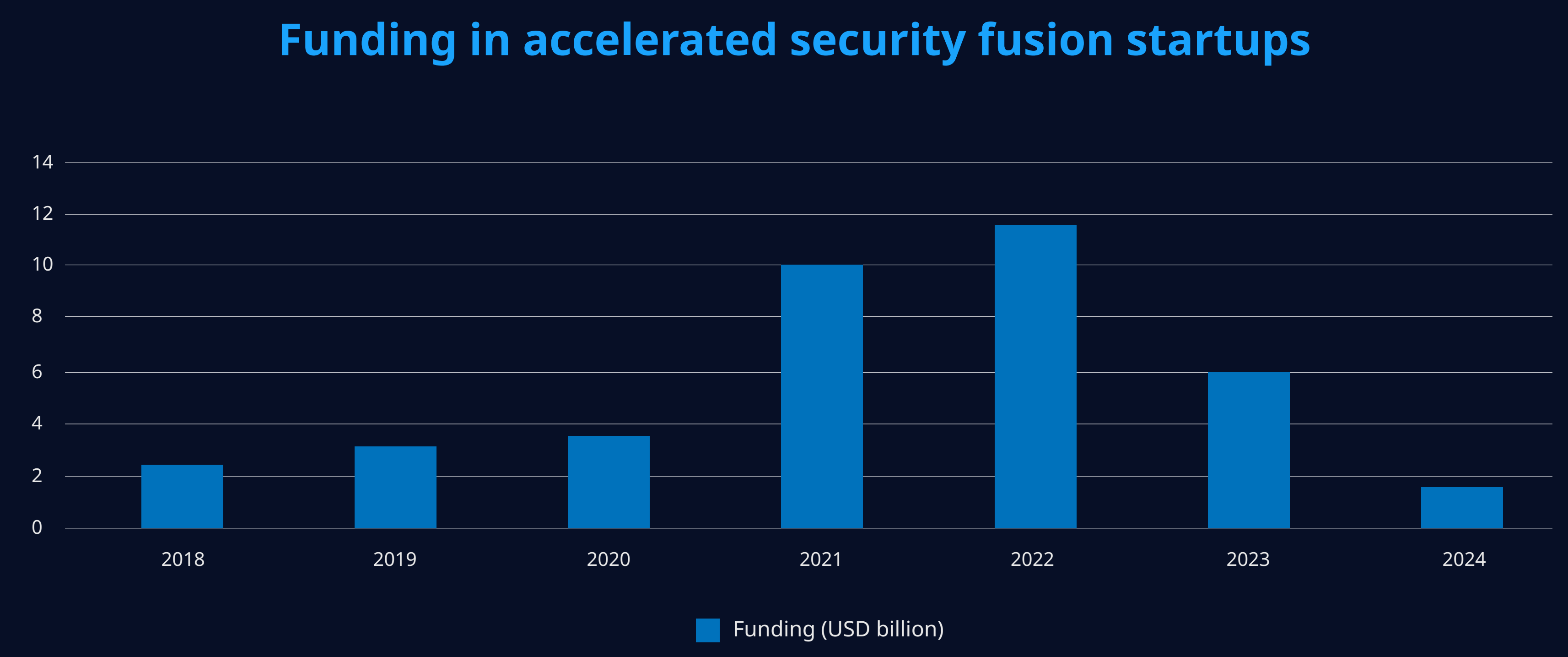


Figure 5: Funding in accelerated security fusion startups

> “69% of enterprise executives believe AI will be necessary to respond to cyberattacks.

Impact of AI on security

Organizations using AI and automation for their security efforts experienced an average data breach cost of $3.05 million, compared to $4.43 million for those without.

90%

of organizations are actively implementing or planning to explore LLM use cases, **while only 5% feel highly confident in their AI security preparedness.**

77%

of companies experienced breaches in their AI systems over the past year.

37%

of data leaders say they have a comprehensive strategy in place to remain compliant with recent and forthcoming AI regulations and meed data-security needs.

71%

of security stakeholders are confident that AI-powered security solutions are better able to block AI-powered threats than traditional tools.

62%

of organizations have deployed an AI package with at least one common vulnerability and exposure (CVE).

Research and development

16,300*

Patents registered 2023

*Approximate figures

Use cases

Automated automotive cybersecurity solution

Industry: **Automotive**

An advanced cybersecurity platform is transforming automotive security with an automated solution for OEMs and Tier 1 suppliers. It ensures compliance with global standards and enables proactive security management through risk-driven approaches and digital-twin capabilities.

Business value

1 Automates critical cybersecurity processes, reducing compliance costs

2 Ensures rapid adherence to evolving regulatory standards, enhancing product security

> “ AI automates cybersecurity for vehicles, ensuring compliance and proactive protection while reducing costs.

Integrated cybersecurity platform for supply chain

Industry: **Logistics**

This solution enhances the protection of a global logistics and supply chain network by integrating data from diverse sources, including cybersecurity systems, IoT sensors and physical security systems. It enables real-time threat detection, analysis and response to minimize risks like cyberattacks and operational disruptions.

Business value

1 Integrating data from multiple sources improves threat detection and response times, safeguarding the logistics and supply chain network.

2 Enhanced protection against cyberattacks boosts operational efficiency and reduces costly interruptions.

Enhanced smart-grid security

Industry: **Public sector; energy**

Quantum-resistant encryption strengthens the security and resilience of smart grid infrastructure against cyberthreats, including those from quantum computing. This implementation protects critical data and boosts consumer confidence in the utility's commitment to robust, future-proof cybersecurity.

Business value

1 Long-term data protection by safeguarding data from quantum threats

2 Increased consumer trust through proactive security

> “Quantum-resistant encryption fortifies smart grids, safeguarding critical data and building consumer confidence.

Real-time fraud detection

Industry: **Financial services**

A real-time fraud-detection system uses ML to identify and prevent suspicious transactions, safeguarding customer accounts. By significantly reducing fraud losses and improving customer retention, the bank demonstrates a strong commitment to protecting its clients' finances.

Business value

1 Reduce fraud loss by up to 40%, protecting the bank's assets

2 15% better customer retention through improved account security

Cloud permission management

Industry: **Cross-industry**

A cloud-security platform manages and analyzes permissions across multicloud environments. It examines configurations and behavior patterns across identities, networks, data and computing resources to prevent breaches caused by misconfigurations or excessive permissions.

Business value

1 Reduces data-breach risks by identifying and mitigating excessive or misconfigured permissions

2 Simplifies compliance management in complex multicloud environments

Secure digital content within entertainment

Industry: **Media**

A leading streaming service uses attribute-based encryption to control access to its content library based on user attributes such as age, subscription level and location. This ensures that only authorized users can access specific titles, protecting copyrighted material while offering tailored viewing experiences.

Business value

1 Enhanced content security by reducing the risk of unauthorized access and safeguarding intellectual property

2 Personalized user experience by transforming specific attributes into recommendations

> “Attribute-based encryption secures content and personalizes experiences, protecting intellectual property while tailoring viewing for users.

AI-powered penetration testing

Industry: **Cross-industry**

A startup provides an autonomous penetration testing solution that continuously evaluates an organization's security across external, identity, IoT and cloud attack surfaces. By simulating real-world attacks, it identifies vulnerabilities before they can be exploited.

Business value

1 Lowers costs and complexity of security testing through automation

2 Enables ongoing assessments to keep pace with evolving cyberthreats

> “Continuous automated penetration testing identifies vulnerabilities, staying ahead of evolving cyberthreats.

Use cases

Success case

Europe | Healthcare

SECANT: Security and privacy protection for IoT devices

Business need

A report by F5 Labs found a 280% growth in attacks on IoT devices. Similarly, Symantec reported a staggering 600% growth in IoT cyberattacks over a six-month period.

The healthcare sector relies heavily on interconnected IoT solutions. It's an industry where sensitive information is processed every moment, and the race for contact-tracing applications has promoted the need for privacy. Healthcare services relying on IoT devices need to be cyber resilient and equipped with advanced cybersecurity capabilities for ensuring quick recovery in the face of crippling modern cyberthreats.

Solution

NTT DATA leads the SECANT Consortium, which has developed an automated threat detection platform for computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs), focused on threat identification and security awareness in complex ICT infrastructures, such as healthcare.

The platform enhances stakeholders' capabilities by implementing:

- Collaborative threat intelligence collection, analysis and sharing
- Advanced risk analysis for interconnected industrial ecosystems
- Trust and accountability mechanisms for data protection
- Employee security-awareness training for more informed security choices

The platform was validated in four pilot use cases in the healthcare sector. It aims to:

- Improve organizational readiness and resilience against modern cyberthreats
- Increase privacy, data protection and accountability across the interconnected ICT ecosystem
- Reduce training costs

Outcomes

The SECANT platform empowers supply chain stakeholders, including CERTs and CSIRTs, with advanced cyberthreat intelligence collection, analysis and sharing capabilities. It delivers innovative risk analysis tailored for interconnected industrial ecosystems, advanced trust and accountability mechanisms for data protection, and comprehensive security awareness training to support more informed cybersecurity decisions.

Startups

Startup radar

In this section, we review a selection of startups relevant to accelerated security fusion, based on our observations, partnerships and investments.

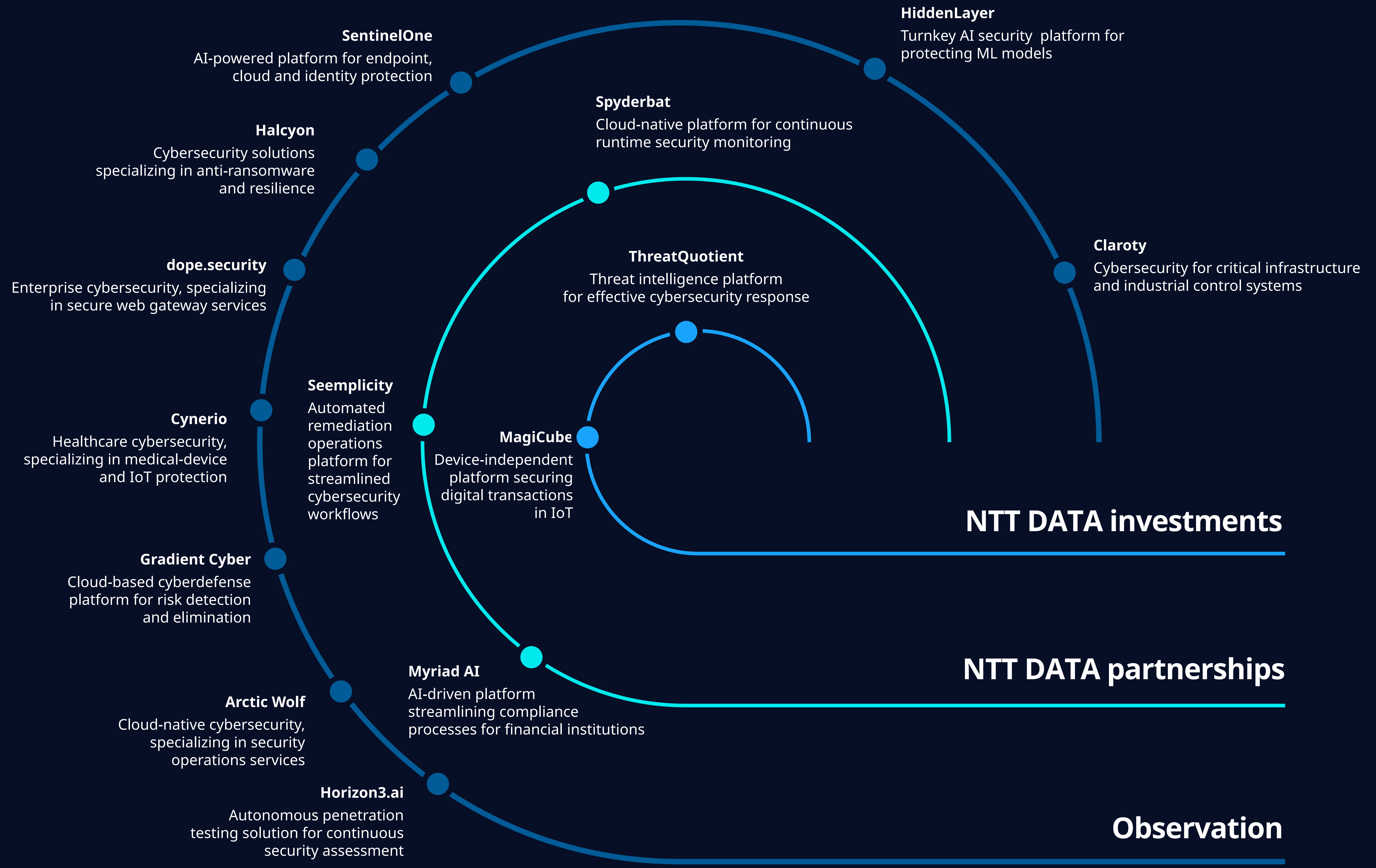

SentinelOne
AI-powered platform for endpoint, cloud and identity protection
HiddenLayer
Turnkey AI security platform for protecting ML models
Spyderbat
Cloud-native platform for continuous runtime security monitoring
Halcyon
Cybersecurity solutions specializing in anti-ransomware and resilience
dope.security
Enterprise cybersecurity, specializing in secure web gateway services
ThreatQuotient
Threat intelligence platform for effective cybersecurity response
Claroty
Cybersecurity for critical infrastructure and industrial control systems
Seemplicity
Automated remediation operations platform for streamlined cybersecurity workflows
Cynerio
Healthcare cybersecurity, specializing in medical-device and IoT protection
MagiCube
Device-independent platform securing digital transactions in IoT
NTT DATA investments
Gradient Cyber
Cloud-based cyberdefense platform for risk detection and elimination
NTT DATA partnerships
Myriad AI
AI-driven platform streamlining compliance processes for financial institutions
Arctic Wolf
Cloud-native cybersecurity, specializing in security operations services
Horizon3.ai
Autonomous penetration testing solution for continuous security assessment
Observation

Figure 6: Investment in accelerated security fusion startups

Startups

Observation

Arctic Wolf

Founded in 2012, Arctic Wolf specializes in security operations. Its cloud-native platform offers services such as MDR, managed risk, managed security awareness and incident response. These services are delivered through a concierge delivery model, providing organizations with 24x7 monitoring, detection and response capabilities.

Stage
Series F

Funding
$899.2 million

Valuation
$4.43 billion

Industry
Cross-industry

HiddenLayer

Founded in 2022, HiddenLayer specializes in AI security, providing a turnkey platform for ML models that protects enterprises against threats such as inference attacks and model theft. Its solution offers robust protection without adding complexity or requiring access to raw data. The company aims to establish itself as a leader in the rapidly evolving AI security landscape.

Stage
Series A

Funding
$56 million

Valuation
Not disclosed

Industry
Cross-industry

Cynerio

Founded in 2017, Cynerio is a healthcare-focused cybersecurity company specializing in protecting medical devices and IoT systems in healthcare environments. It integrates generative AI into its Cynerio 360 platform, enhancing capabilities in device classification, security, rule generation and anomaly detection. Cynerio also offers a unique attack detection and response (ADR) product tailored for healthcare.

Stage
Series B

Funding
$37 million

Valuation
Not disclosed

Industry
Healthcare

Halcyon

Founded in 2021, Halcyon specializes in anti-ransomware solutions and cyber resilience for enterprise customers. Its platform provides layered protection against ransomware, including pre-execution detection, behavioral modeling and recovery features, as well as key capture and automated decryption to prevent data extortion. Halcyon primarily serves the global enterprise sector, offering tools and assessments to enhance cyberdefense capabilities.

Stage
Series B

Funding
$90 million

Valuation
Not disclosed

Industry
Cross-industry

SentinelOne

Founded in 2013, SentinelOne provides an AI-powered platform for endpoint, cloud and identity protection. SentinelOne's autonomous endpoint protection technology uses a single AI-powered agent to unify prevention, detection, response and threat hunting across all attack vectors, automatically eliminating threats in real time for both on-premises and cloud environments.

Stage
Post-IPO

Funding
Not disclosed

Valuation
Not disclosed

Industry
Cross-industry

Claroty

Founded in 2015, Claroty protects cyber–physical systems (CPS) and the extended Internet of Things (XIoT), focusing on critical infrastructure and industrial control systems. The Claroty Edge platform is a zero-infrastructure industrial cybersecurity solution that provides complete visibility of industrial networks without requiring network changes, sensors or physical footprint.

Stage
Series D

Funding
$735 million

Valuation
Not disclosed

Industry
Manufacturing; public sector; energy; telecommunications

dope.security

Founded in 2021, dope.security focuses on secure web gateway services. Its main offerings include an on-device proxy for direct internet access, with local SSL traffic inspection and an AI-powered data-loss prevention tool for cloud applications. The company primarily serves sectors that require robust cybersecurity solutions for endpoint and cloud applications.

Stage
Series A

Funding
$20 million

Valuation
Not disclosed

Industry
Cross-industry

Startups

NTT DATA partnerships

Myriad AI

Founded in 2023, Myriad AI is developing an AI-driven platform designed to streamline compliance processes for banks and fintech companies. The platform leverages advanced AI to enhance access to regulatory information, aiming to simplify and automate compliance tasks. This approach seeks to reduce the complexity and time associated with traditional compliance methods, offering a more efficient solution for financial institutions.

Stage
Pre-seed

Funding
$2 million

Valuation
Not disclosed

Industry
Financial services

Seemplicity

Founded in 2020, Seemplicity offers a remediation operations (RemOps) platform designed to automate and streamline risk-reduction workflows. Its platform consolidates security findings from various tools, enabling security teams to prioritize and manage vulnerabilities efficiently. By automating remediation processes, Seemplicity aims to accelerate vulnerability reduction and enhance overall security posture.

Stage
Series A

Funding
$32 million

Valuation
Not disclosed

Industry
Cross-industry

Spyderbat

Founded in 2019, Spyderbat provides a cloud-native runtime security platform that delivers continuous security monitoring, improved observability and timely alerting. Their platform uses eBPF-based* agents to capture comprehensive runtime events, enabling organizations to detect, identify and block threats in real time across hybrid and multicloud environments.

Stage
Series A

Funding
$14.2 million

Valuation
Not disclosed

Industry
Cross-industry

* eBPF: extended Berkeley Packet Filter

Startups

NTT DATA investments

MagicCube

Founded in 2014, MagicCube provides security solutions for digital transactions in the IoT sector. The company offers a device-independent platform that secures digital transactions on any device, in transit and in the cloud, providing a level of security comparable to hardware solutions but without the associated complexity and cost.

Stage
Series C

Funding
$25.95 million

Valuation
$100–$500 million

Industry
Cross-industry; financial services

ThreatQuotient

Founded in 2013, ThreatQuotient offers a threat intelligence platform designed to help organizations understand and respond to cyberthreats effectively. Its solutions integrate threat data, prioritize security operations and facilitate collaboration among security teams to enhance overall defense strategies.

Stage
Series C

Funding
$87.6 million

Valuation
Not disclosed

Industry
Cross-industry

Future scenarios

As industries transform, new value chains emerge and technological advancements grow exponentially, companies must navigate complex, evolving landscapes.

Future scenarios and GenAI powered personas allow organizations to explore possible futures, simulating realistic business environments and minimizing risk through scenario-based planning.

Uncertainties represent what we cannot know but identifying them can reduce the risks of blind spots down the road.

Future scenarios

Uncertainty: effectiveness of GenAI for threat simulation

AI's dual edge

What if GenAI becomes a double-edged sword in cybersecurity?

As GenAI evolves into a powerful tool for simulating and preempting cyberthreats, it makes defenses more adaptive than ever. However, the same technology may empower malicious actors to design more sophisticated attacks, creating a constant race between innovation in defense and exploitation.

Guardians of tomorrow

What if AI-driven defenses redefine cybersecurity, transforming it into a predictive science?

GenAI is increasingly becoming a proactive agent, predicting and countering cyberthreats before they occur, significantly reducing attacks. Beyond protection, the efficiency gains from AI will allow organizations to redirect resources to innovation, boosting overall productivity and technological development.

Future scenarios

Uncertainty: post-quantum cryptography readiness

Quantum race, digital chaos

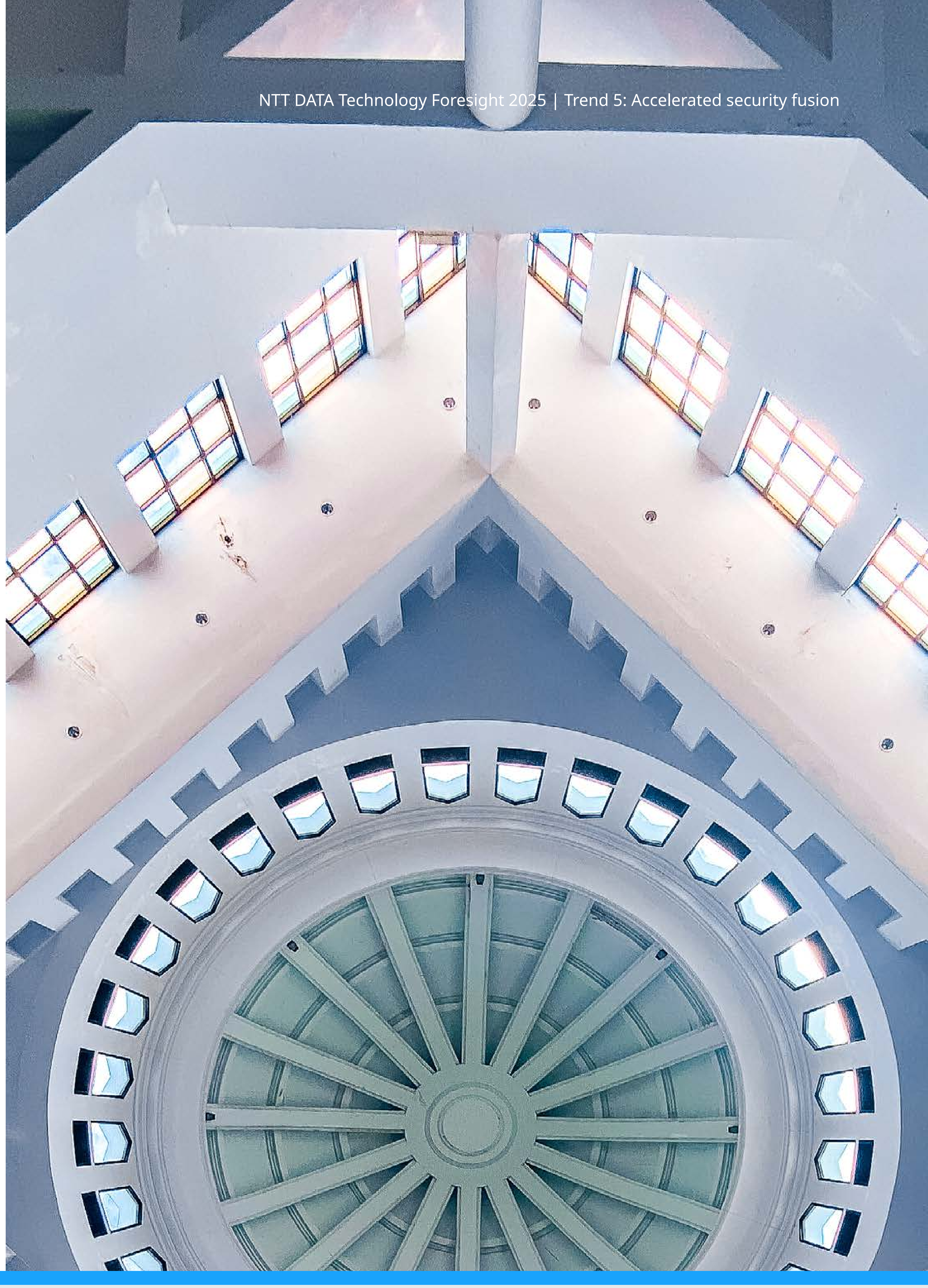
What if a fragmented digital ecosystem accelerates innovation while exposing vulnerabilities to quantum-powered attacks?

As early adopters of post-quantum cryptography secure critical systems, laggards face heightened risks, creating a global digital divide. This competition may drive rapid advancements in encryption and decentralization technologies, enabling niche industries and robust local solutions to thrive.

Quantum strongholds

What if quantum readiness becomes the new determinant of power and resilience in the digital age?

Nations and corporations investing in post-quantum cryptography will create secure, future-proof infrastructures that can withstand quantum-powered breaches. The race for quantum resilience may fuel a renaissance in science, engineering, technology and math (STEM) education and workforce development, creating a generation of quantum-savvy professionals.



Conclusion and next steps

Conclusion and next steps

Think about this

As businesses face increasing security complexity, identifying and prioritizing weaknesses across detection, response, identity management and data privacy becomes essential.

How robust is your organization's approach to systematically analyzing vulnerabilities, including cryptographic standards, to safeguard against emerging risks?

AI-driven threat intelligence programs unlock value by fostering cross-departmental alignment, streamlining information-sharing and enhancing decision-making capabilities.

How does your organization ensure integration between teams and technologies to establish a cohesive and proactive defense strategy?

With automation reshaping security paradigms, optimizing incident response workflows can significantly reduce operational bottlenecks and improve agility in addressing critical threats.

Are your security systems leveraging automation to enhance speed, accuracy and scalability in cyberincident management?

Conclusion and next steps

Do this next

5 minutes

Identify and address security weaknesses

Assess the current state of your organization's security infrastructure. Identify gaps in threat detection, response or identity management that could benefit from AI-driven solutions.

5 days

Select and prepare simulation tools

Evaluate and shortlist breach and attack simulation tools. Prepare an implementation plan and secure approvals to launch a proof-of-concept project.

5 months

Build a security deployment roadmap

Develop a roadmap for deploying key accelerated security fusion technologies, such as MDR services, CNAPPs and zero trust frameworks.

Contact information

Experts | Accelerated security fusion (Security)

Sheetal Mehta
Global Portfolio Lead
sheetal.mehta@global.ntt

Patrick Schraut
Distinguished expert
Patrick.Schraut@nttdata.com

About the research

Contributors

Name	Surname	Country
Valentina	Contini	Germany
Johannes	Reim	Germany
Diana	Hauser	Germany
Oliver	Koeth	Germany
Iris	Pfeifer	Germany
Thorsten	Harth	Germany
Leska	Reuster	Germany
Alberto	Acuto	Italy
Christian	Koch	Germany
Moshe	Karako	Israel
Thomas	Plass	Germany
Leticia	Lastra	UK
Nick	Mc Fetrich	UK
Markus Alexander	Hessler	Germany
César	Zayas	UK
Marta	Garayoa	Spain
Yumiko	Goshima	Japan
Ryoto	Ando	Japan
Yuya	Kawamata	Japan
Hiroshi	Furukawa	Japan
Tom	Winstanley	UK
Maria del Pilar	Quiros Gascon	Spain
Maria Mercedes	Medina Mora	Spain
Lucia	Ciordia Navarro	Spain
Sara	Alvarellos Navarro	Spain
Jose Carlos	Chavez Peinado	Spain
Martina	Palmucci	Italy
Filippo	Capocasale	Italy
Krasimir	Dzhigovechki	Germany
Nathan	Quadrio	Germany
Fabian	Warthenpfuhl	Germany
Volker	Ganz	Germany
Florian	Soelch	Germany
Dennis	Tischer	Germany
Markus	Lunz	Germany
Enno	Kätelhöhn	Germany
Daniel	Miner	Germany
Maria Vittoria	Trussoni	Italy
Bernhard	Stay	Germany
Takashi	Okada	Japan
David	Pereira	Spain
Global Content Hub		Global

References and sources

Trend 5: Accelerated security fusion

- Kimbrel, J. Vectra. Now playing: 2024 state of threat detection and response.
- Orca Security. 2024 State of AI Security Report.
- Sajid, H. Lakera. AI security trends 2025: market overview and statistics.

Glossary of key terms

Enhanced humans

People and machines are collaborating to shape a future where human potential isn't limited by time, task or knowledge.

Ambient intelligent experiences

Technologies like AI, spatial computing and automation are fundamentally changing how organizations connect with their audiences across different touchpoints.

Digital sustainability for economic resilience

A new business strategy is emerging where organizations integrate environmental stewardship with economic growth and assign individual and collective responsibility.

Cognitive cloud convergence

By integrating advanced cloud computing technologies with AI and human cognitive abilities, organizations can improve operations, enhance decision-making and understand their data in real time.

Accelerated security fusion

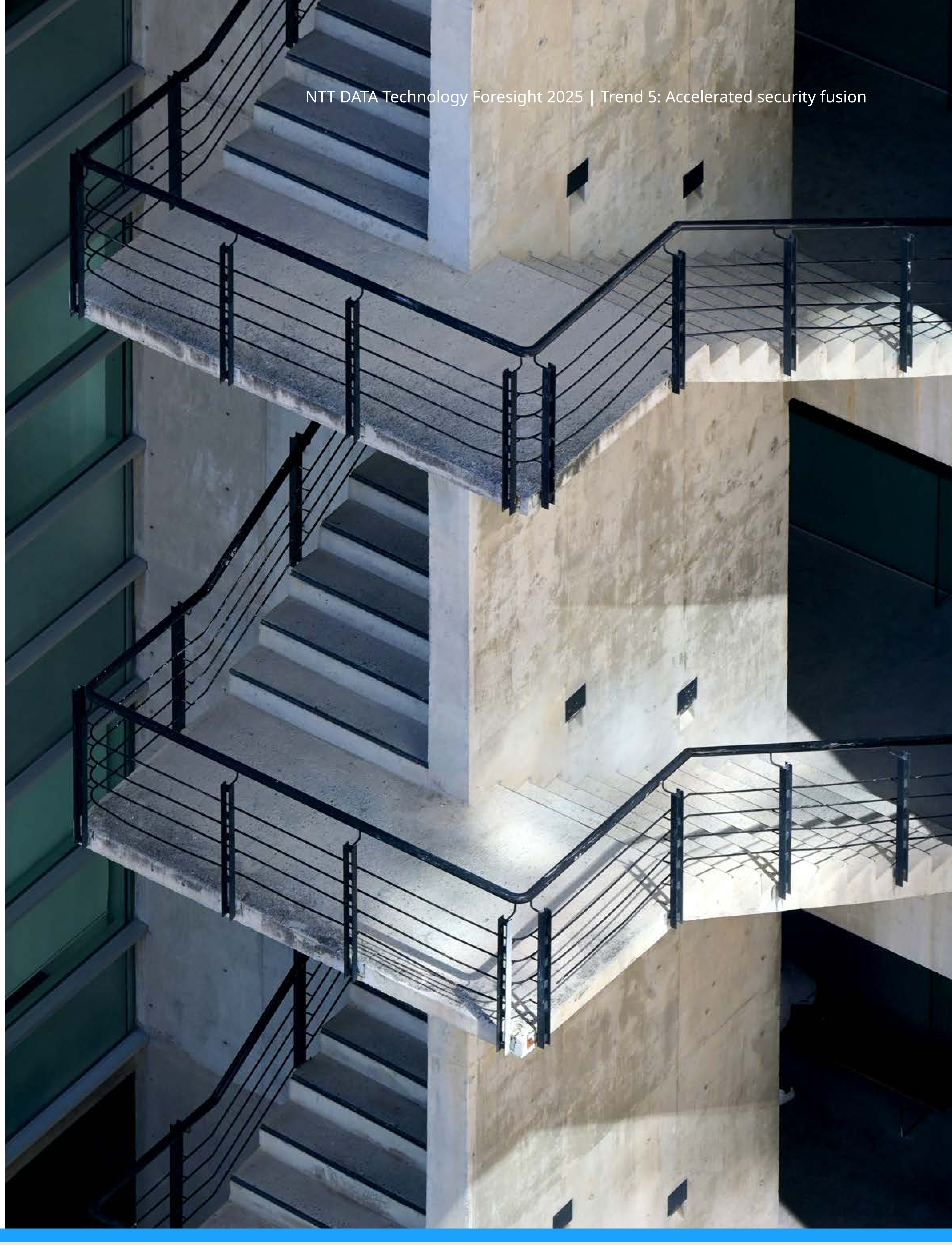
A new business strategy is emerging where organizations integrate automated incident response and AI-driven threat detection to adapt dynamically to emerging threats and build cyber resilience.

List of abbreviations

ADR	attack detection and response
AGV	automated guided vehicles
AI	artificial intelligence
AIASE	AI-augmented software engineering
AIOps	AI for IT operations
AMR	autonomous mobile robots
API	application programming interface
AR	augmented reality
ASIC	application-specific integrated circuit
AutoML	automated machine learning
AWS	Amazon Web Services
BAS	breach and attack simulation
CDN	content delivery network
CERT	computed emergency response team
CGI	computer-generated imagery
CGM	continuous glucose monitor
CI/CD	continuous integration and continuous delivery or deployment
CNAPP	cloud-native application protection platform
CPS	cyber-physical systems
CPU	central processing unit
CRQ	cyber risk quantification
CSIRT	computer security response team
CSPM	cloud security posture management
CX	customer experience
CVE	common vulnerabilities and exposure
DevSecOps	development, security and operations
DDoS	distributed-denial-of-service
DoT	deep learning of things
DSP	data security platform
EMS	energy management systems
ESG	environmental, social and governance
eVTOL	electric vertical takeoff and landing
FPGA	field programmable gate array
GenAI	generative AI
GPU	graphics processing units
GPT	generative pretrained transformer
IAM	identity and access management
IDE	integrated development environment
IOWN	Innovative Optical and Wireless Network
IPA	intelligent personal assistant
IRM	integrated risk management

List of abbreviations

ITRM	IT risk management
ITSM	IT service management
IoT	Internet of Things
LIME	Local Interpretable Model-Agnostic Explanations
LLM	large language model
MAG	multiagent generative system
MDR	managed detection and response
MFA	multifactor authentication
MLOps	machine learning operations
ML	machine learning
MR	mixed reality
NLP	natural language processing
OEM	original equipment manufacturer
OT	operational technology
PaaS	platform-as-a-service
PET	privacy-enhancing technology
PDE	provider data extractor
PQE	post-quantum encryption
PRM	proactive risk management
RAG	retrieval-augmented generation
RemOps	remediation operations
RPA	robotic process automation
RFID	radio frequency identification
SaaS	software-as-a-service
SHAP	Shapley Additive exPlanations
SSL	secure sockets layer
STEM	science, technology, engineering and math
TPU	tensor processing unit
UAV	unmanned aerial vehicle
VA	virtual assistant
MLOps	machine learning operations
VoC	voice of the customer
VR	virtual reality
XIoT	extended IoT
XOps	cross-functional operations



NTT DATA