Modern business resilience

A practical guide to an agile and adaptive resilience strategy

Contents

Introduction

Introduction

Defining business resilience

For organizations, the term “resilience” has been largely related to business continuity. While this remains an important part of being resilient, in today’s world of rapid and unprecedented change, business resilience has evolved beyond this simple understanding.

According to ISO 22316 organizational resilience is “the ability of an organization to absorb and adapt in a changing environment”.[1] The BS 65000 definition is even more explicit:

> “Organizational resilience is the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruption in order to survive and prosper.”[2]

The key focus here is the ability to adapt to a fast-changing environment. Today, becoming resilient is core to your organization’s success, its sustained relevance in your industry, and ability to instil confidence and trust in your stakeholders, shareholders and customers.

In this guide by Omdia, with expert insights from NTT DATA, you will learn how an integrated approach to cybersecurity, from preparation to response and recovery, has become the cornerstone of business resilience. We explore the contrasting roles of AI in cyber resilience and provide practical recommendations to help you build an agile and adaptable enterprise.

1 ISO 22316:2017 Organizational resilience – Principles and attributes (published in 2017)
2 BCI, BS 65000:2014

The evolution of business resilience

Beyond disaster recovery to modern business resilience

Traditionally, resilience was a **static function** that focused on ensuring business continuity by creating a backup plan to continue business operations during a disaster or IT failure. While this seemed sufficient in the 1990s and early 2000s, the rapid pace of change and increasing complexity of the past decade led to a noticeable shift.

Leadership and crisis management teams have become proactively involved, giving rise to an **agile and adaptive** resilience function.

Resilience can no longer be ringfenced into a siloed practice. It must be established as a holistic, continuous and collaborative discipline that cuts across the entire organization and its value chain — and cybersecurity plays a central role in this shift.

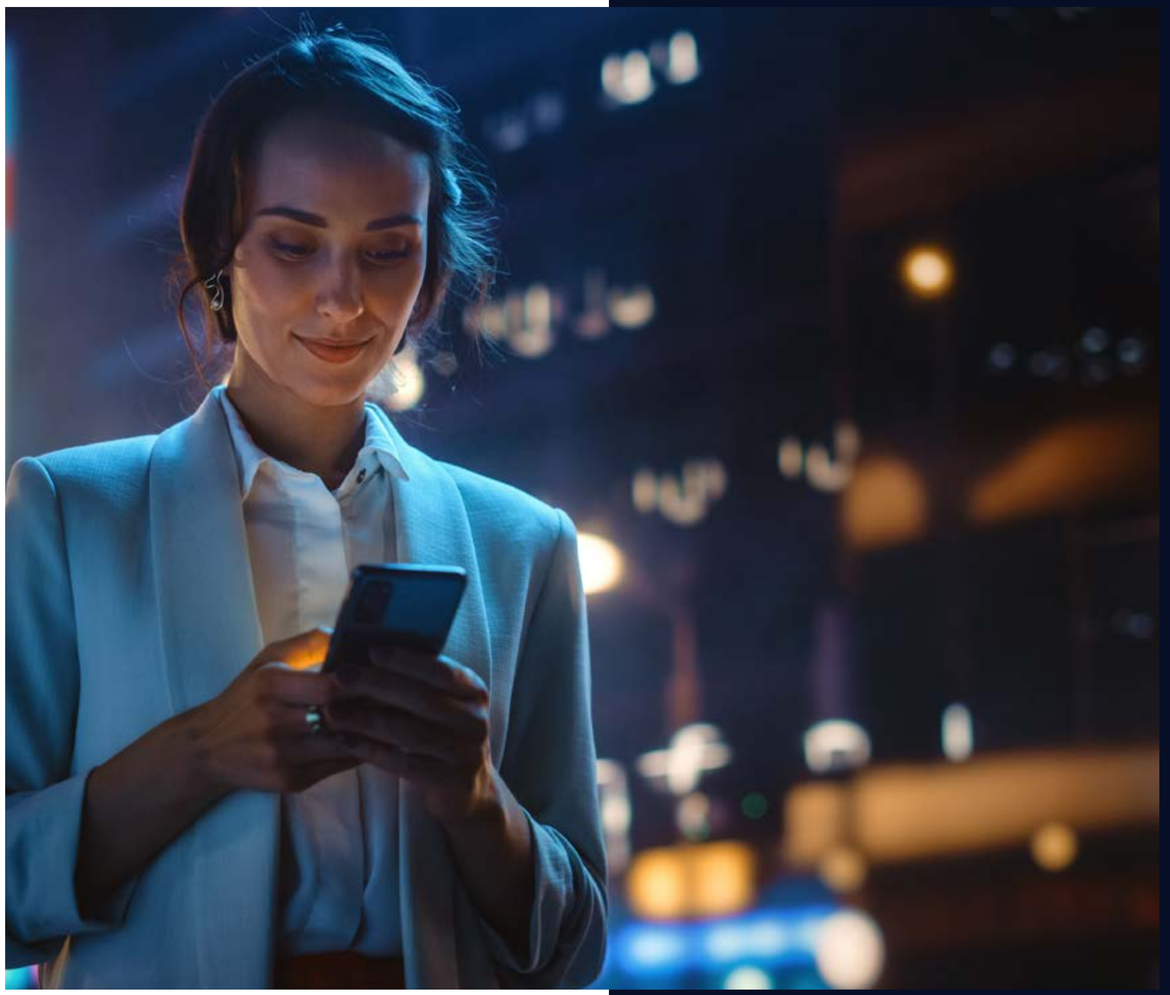
What's driving the shift from a static to an agile and adaptive resilience function?

- Increased frequency of disruptive events
- Growing competitive landscape (organizations no longer have the luxury of downtime to recover from events)
- Growing complexity in business ecosystems, coupled with a rapidly evolving threat landscape
- Increasing and evolving stakeholder expectations: less tolerance for downtime, higher expectations for reliable delivery, decreasing customer loyalty and evolving customer preferences
- Impact of social media and real-time news on brand protection during crisis

Rise of agile and adaptive resilience strategy

Omdia firmly believes that modern business resilience must be agile, adaptable and underpinned by a robust cybersecurity ethos. There are simply too many threat actors in operation, too many attacks happening and too few defenders in place to address them all. Add to that the fact that contemporary trends such as cloud computing, working from anywhere, and the growing adoption of AI and ML significantly expand the attack surface of most organizations, and it becomes clear that **proactive preparedness now goes beyond a choice to becoming a necessity for business resilience.**

Cybersecurity’s role in driving an agile and adaptive resilience strategy



"Modern business resilience demands more than just recovering from cyberattacks — it requires proactive preparation to protect critical assets, and continuous detection and response to navigate an evolving threat landscape. To be effective, this entire process must be simplified and seamlessly integrated, enabling swift, coordinated action from preparation through to response and recovery. For CISOs, this means aligning systems, people and processes around risk and resilience, leveraging AI and ML for faster, smarter responses, while ensuring the full engagement of the C-suite in this mission."

Sheetal Mehta
SVP and Global Head of Cybersecurity
NTT DATA, Inc.

Cybersecurity’s role in driving an agile and adaptive resilience strategy

Cybersecurity is pivotal to modern business resilience

Today, every business is a digital business, and technology is everywhere, from strategy to operations. However, this widespread technology use has expanded the attack surface and will continue to do so. The growing adoption of emerging technologies like AI and GenAI makes businesses more vulnerable to cyberthreats — and makes cybersecurity pivotal to an organization’s business resilience strategy.

Building a resilience strategy begins with **preparation**: identifying critical assets and protecting them through continuous risk management by reducing the attack surface and removing vulnerabilities before they can be exploited. Next, you need to establish a strong **response**, enabling continuous detection and rapid response to cyberthreats and attacks as they emerge.

Finally, create a robust **recovery** plan that ensures operational continuity and maintains stakeholder confidence — and your reputation.

This means embedding not only security by design but **resilience by design** into the core of your strategy, operations and digital experience management. A simple, secure and tightly integrated flow across preparation, response and recovery empowers resilient enterprises to navigate change confidently, **balance the risk and rewards of transformative technologies like AI**, quantum computing and private 5G, and ensure **stakeholder trust and business performance.**

Navigating an evolving threat landscape

Navigating an evolving threat landscape

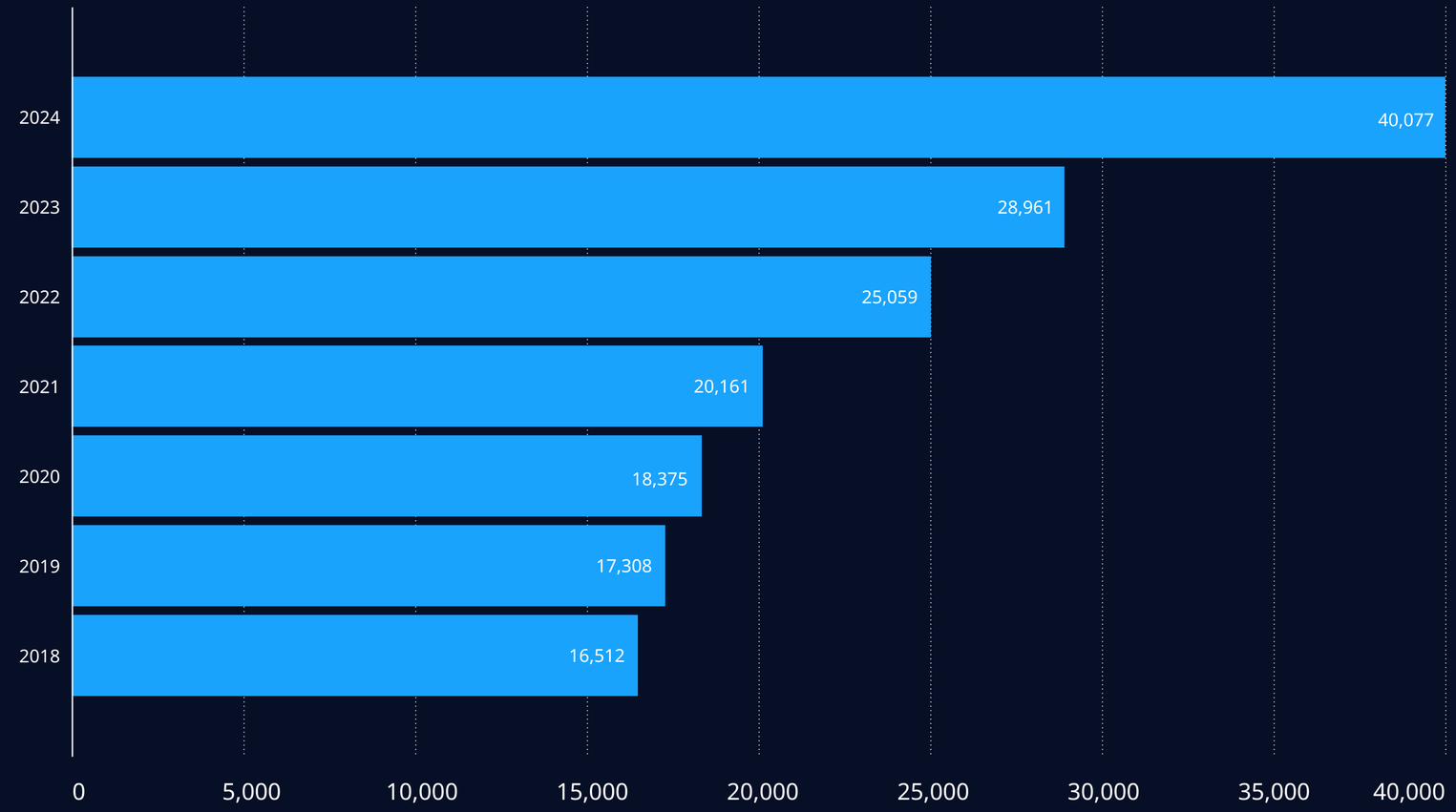
Common vulnerabilities and exposures are increasing

According to the Common Vulnerabilities and Exposures (CVE) program, which identifies, defines and catalogs publicly disclosed vulnerabilities, the number of new vulnerabilities discovered accelerated in 2024.

In one sense this is bad news, as software vendors struggle to deliver comprehensive security. On the other hand, it shows the scale of the problem confronting CISOs and IT security teams, and supports the case for a proactive approach to security.

Improved resilience stems from being proactive: finding issues and addressing them to become less of a target for cyberattacks.

Number of published CVEs, year on year



Source: CVE Program, Apr 2025

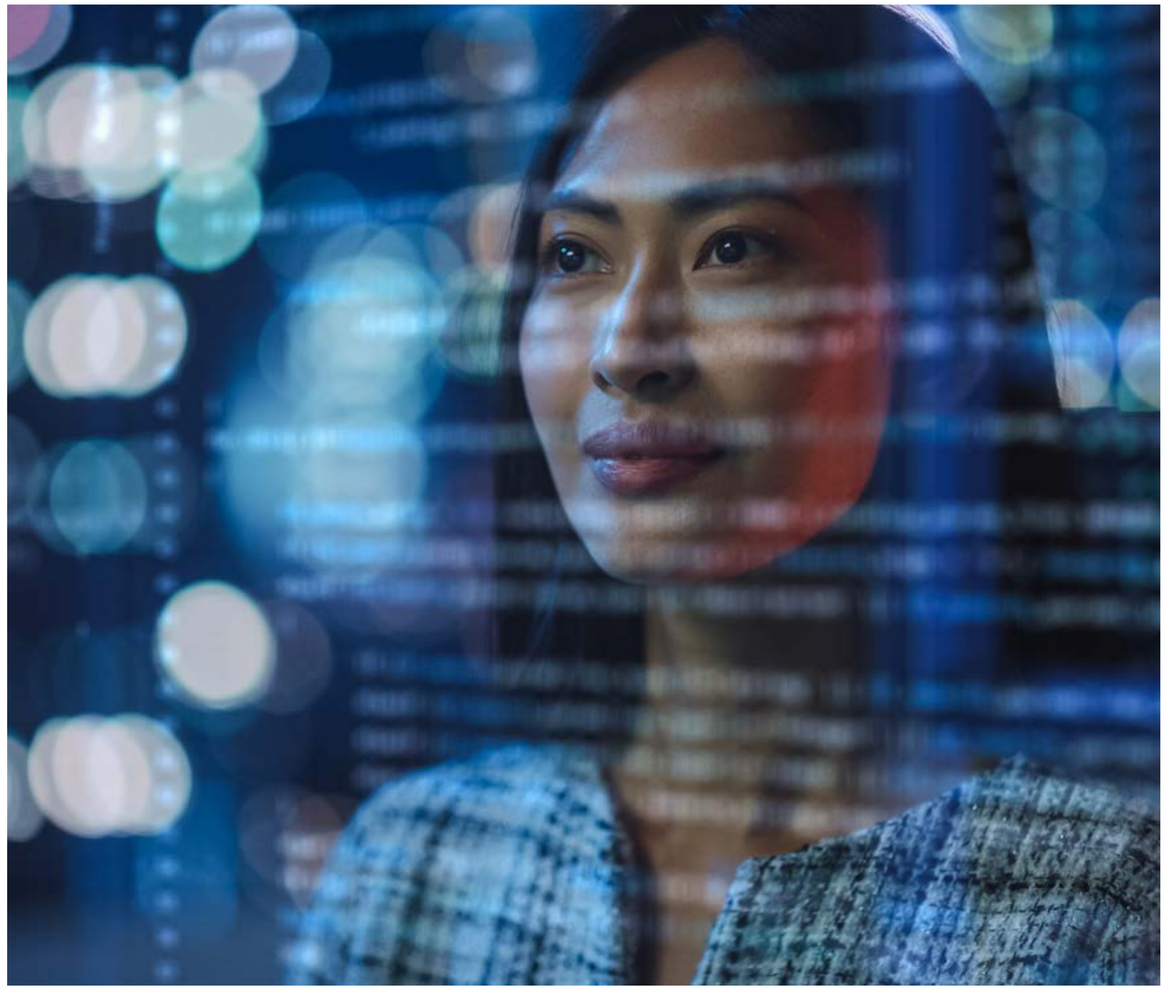
Navigating an evolving threat landscape

Data exposure has been the leading consequence of security breaches since 2019

Since H1 2023, data exposures have grown by 8% and remain the most significant security breach outcome.

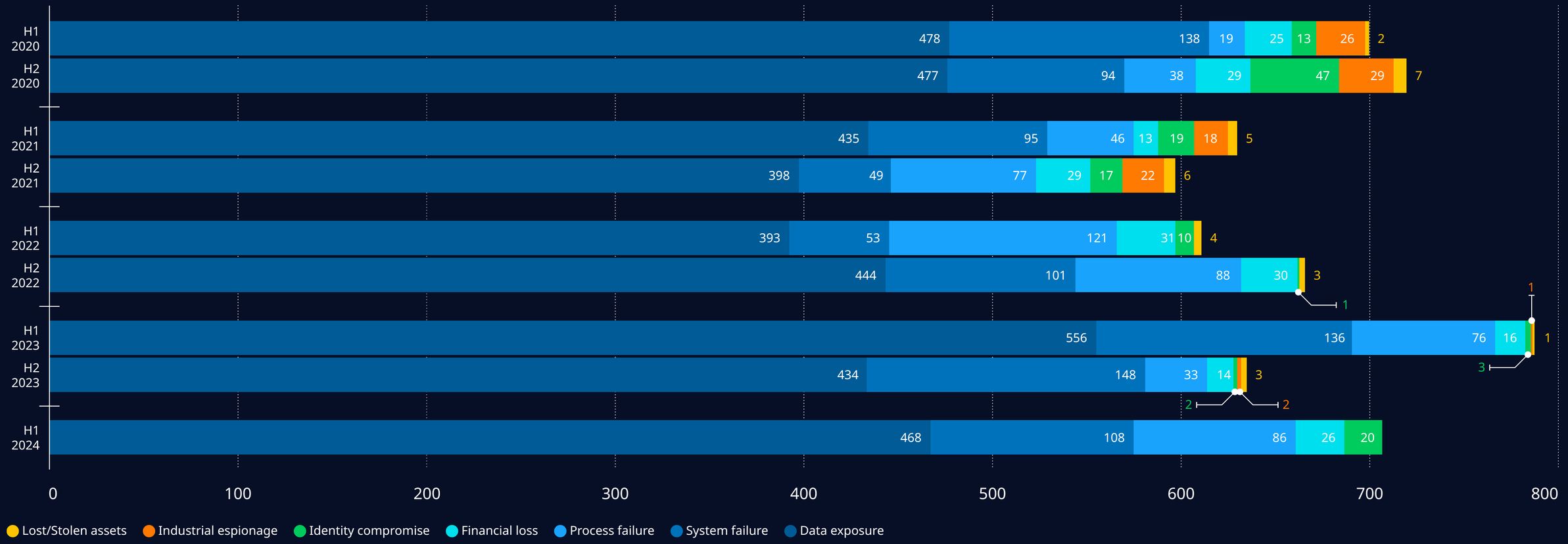
Top breach outcomes	
Data exposures	66%
System failures	15%
Process failures	12%
Financial losses	4%

Top breach tactics	
1	**Malicious hacking attempts**
2	**Supply chain compromises**
3	**Ransomware**



Source: Security Breaches Tracker – 2Q24 Database, Omdia, 2024 |

Security breach outcomes in the tracked announcements, 2020–H1 2024



Source: Security Breaches Tracker – 2Q24 Database, Omdia, 2024 | **Note**: Breaches displayed in this chart are inclusive of multiple breach outcomes |

Navigating an evolving threat landscape

The impact of data exposure on modern business resilience

The quarterly Omdia Security Breaches Tracker, which summarizes and categorizes announcements related to security breaches across the globe, noted 6.9 billion records affected during H1 2024, a 6% increase from 6.5 billion records in H2 2023.

About 3.7 billion (54%) of affected records were attributed to the US. Some of the largest data exposure was attributed to Discord, the instant messaging and VoIP social platform, when Spy.pet, a data mining site, harvested messages from 620 million Discord users from 14,000 chat servers and attempted to sell access to the data. After investigating the incident, Discord banned accounts affiliated with Spy.pet.

In France, the personal data of 43 million individuals registered with France Travail, a government agency responsible for unemployment and jobseekers, was leaked when a threat actor gained unauthorized access to the agency's database.

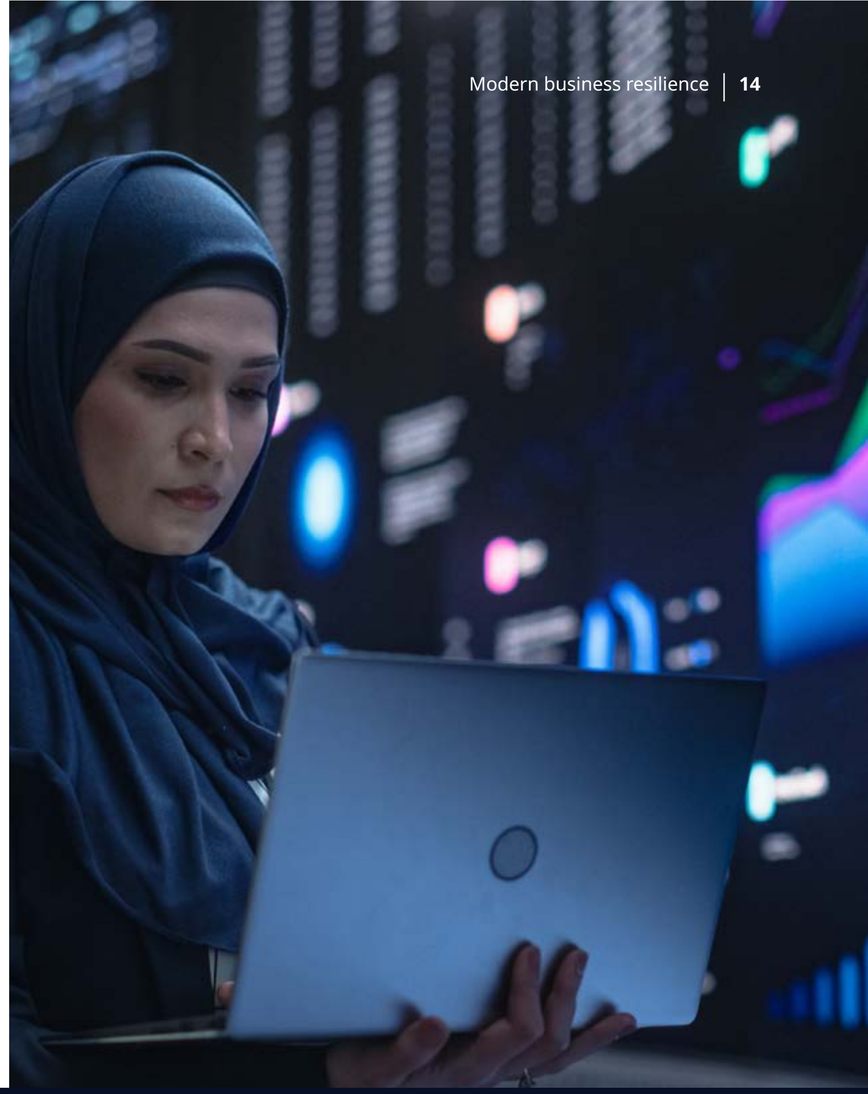
Resilience by design reduces data exposure

Since data is at the core of every business, a data-centric approach to security is critical. Resilience by design works to protect data through a holistic security strategy.

Integrated systems deliver resilience by working together to reduce vulnerabilities using direct communications and secure, predetermined routes for data transfer.

By integrating systems across lines of business, leaders have confidence in data integrity and are able to plan more quickly and effectively.

CISOs and CIOs can ensure systems are optimized to underpin business development, enablement and growth.



Recent global outages demonstrate that IT is as important to economies and society as energy, water and raw materials. An integrated approach to cybersecurity protects organizations against exposure and, by doing so, becomes a catalyst for business resilience and growth.

2024 Omdia Security Breaches Tracker

6.92 billion

Records affected in H1 2024

North America

Subregion with the largest volume of records affected (54% of total affected records)

6% increase

In records affected since H2 2023 (6.5 billion)

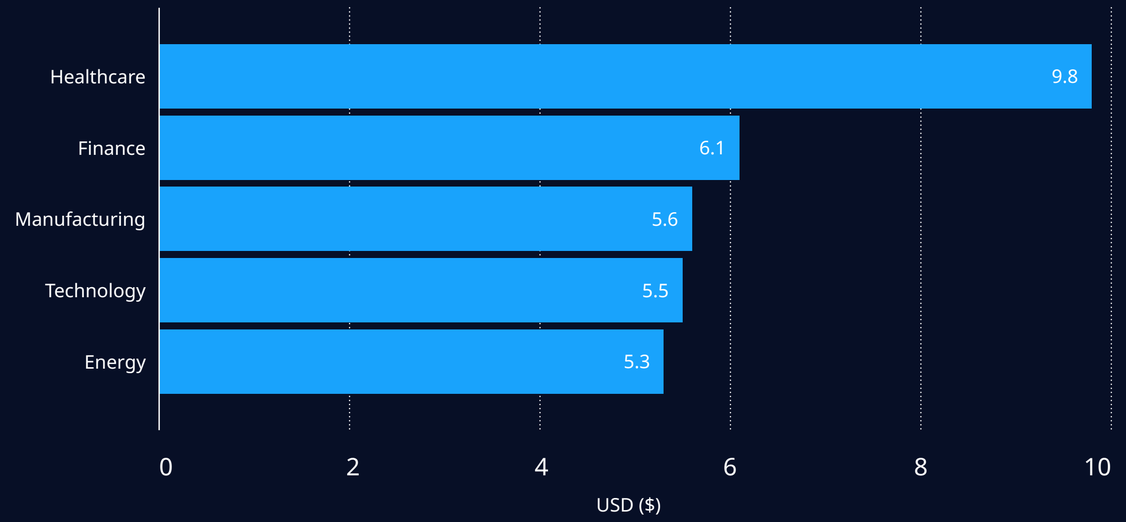
Navigating an evolving threat landscape

The high cost of data breaches

The average cost of a data breach is just under $5 million, a 10% increase from 2023. In the US, the number almost doubles to $9.4 million. The chart to the right shows how these costs vary by industry.

- Nearly half **(46%)** of all breaches involve customer personal identifiable information.
- It takes organizations an average of **204 days to identify a data breach and 73 days to contain it.**
- Breach notification costs rose to **$370k in 2023**, a **19.4% increase from 2022**.
- Cyberattacks using stolen or compromised credentials increased **71% year-over-year**.
- **74%** of all breaches include the human element.
- **12%** of employees were able to take sensitive IP with them when they left an organization, such as customer and employee data, health records and sales contracts.
- **98%** of organizations have at least one third-party vendor that has suffered a data breach.
- **61%** of organizations use some level of security AI and automation.

Cost of data breach by industry

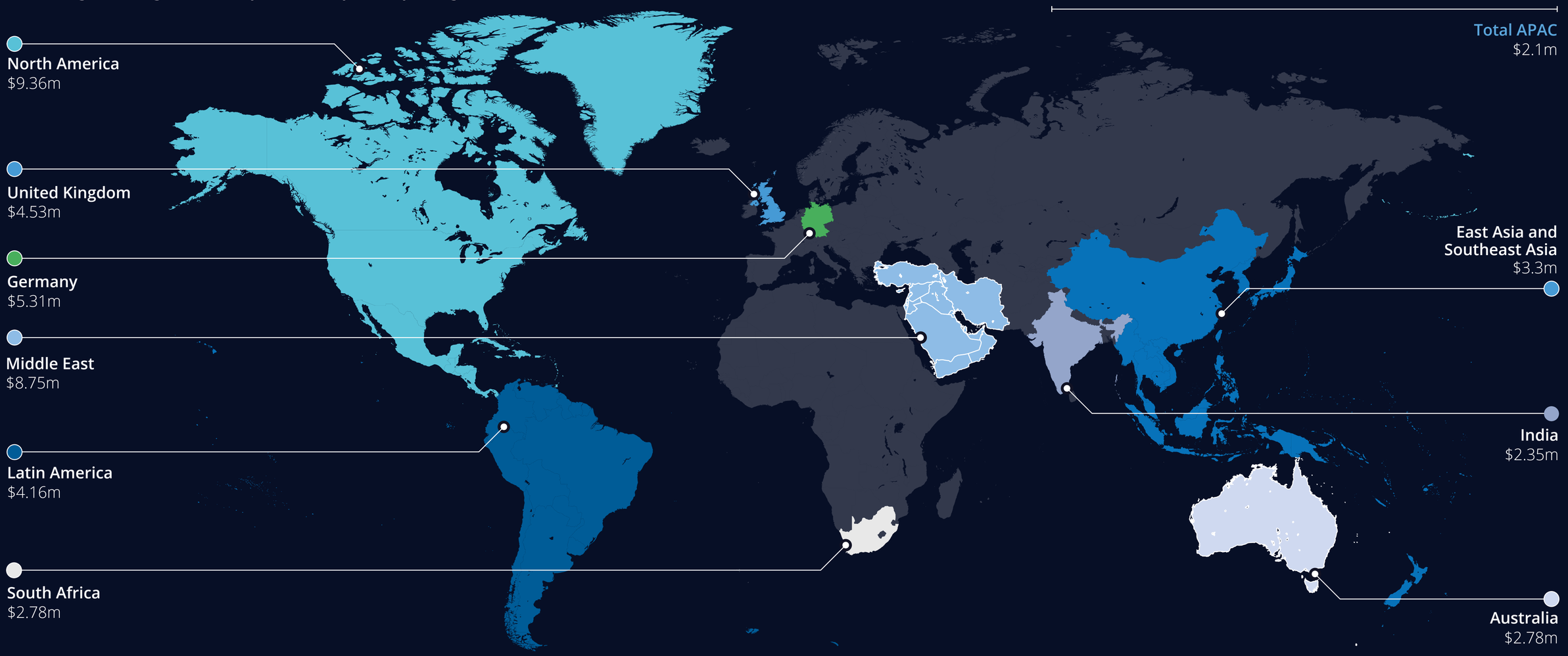


Factors affecting the cost of a data breach

1	**Complexity**	Legacy best-of-breed approach creates unmanageable infrastructure
2	**Skills shortages**	Overall lack and depth of skills
3	**Third-party integration**	Inherited risk from external systems

Source: IBM (with Ponemon Institute) – ‘Cost of a Data Breach Report 2024’

The average cost of global security breaches by country or region



“Business resilience has evolved, with cybersecurity now playing a critical role. Being agile and adaptive is fundamental, and there are pitfalls for those that get it wrong.”

Adam Strange
Principal Analyst, Data Security
Omdia

Balancing the risks and innovation potential of AI

Balancing the risks and innovation potential of AI

How does AI-assisted cybersecurity help business resilience?

Machine learning

- Faster data analysis
- Reducing analytical drudgery
- Timely alerting to issues for proactive and reactive security

Generative AI

- Suggests remedial actions for security operations center (SOC) teams
- Improves best practice by learning and propagating knowledge

Agentic AI

- Automates routine tasks based on training a large language model (LLM)
- Frees SOC teams to focus on more complex issues requiring human attention

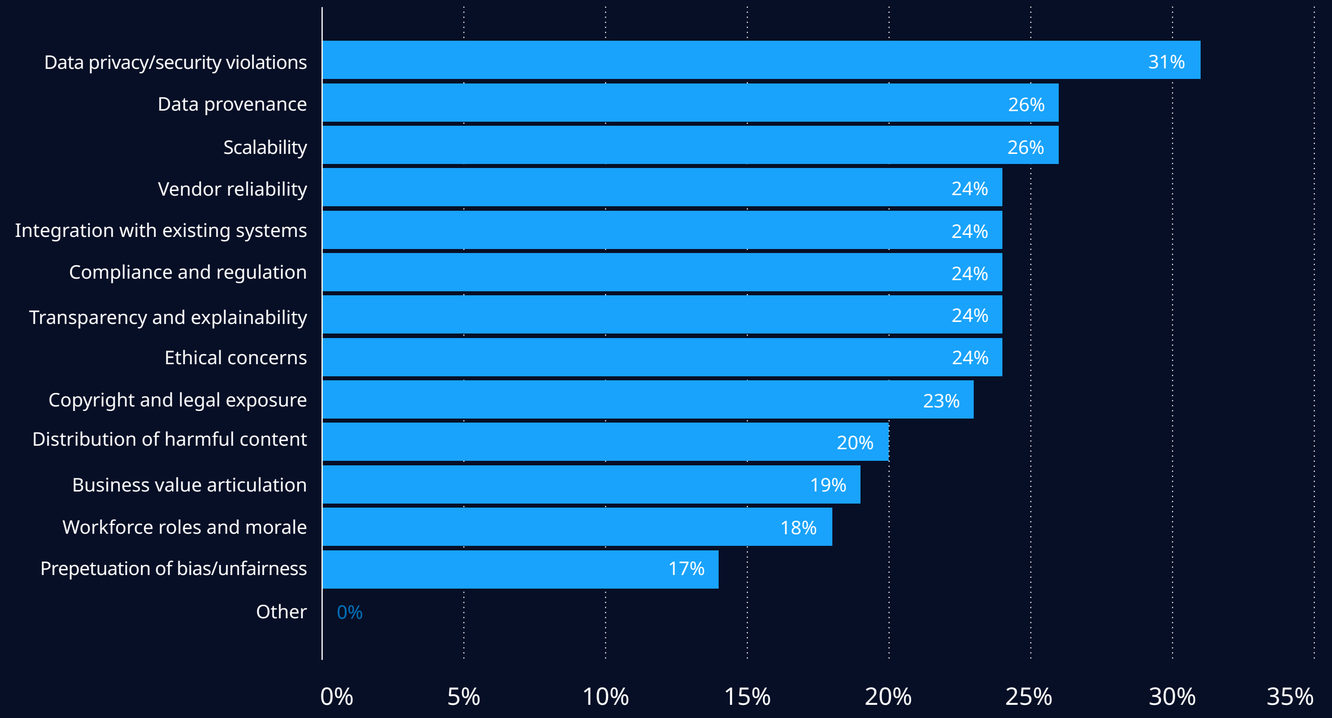
Balancing the risks and innovation potential of AI

The contrasting impact of AI on business resilience

AI is here to stay, and its impact will be profound. Omdia sees data volumes that exceed humans' ability to manage. The opportunity is for automation to provide control, but risk needs to be accurately quantified too.

Benefits of AI	
Data discovery	Find all data in all data repositories: on-premises, software as a service (SaaS) applications and cloud
Classification	Use AI to determine content and apply appropriate labeling
Encryption	Automatically encrypt data according to content
Data loss prevention (DLP)	Interrogate data to ensure distribution is compliant with policy
Event management	AI for automatic detection and reduction of false positives
Threat detection	Inspection and detection of data traffic against known threats

What are your organization's biggest concerns about utilizing AI, including generative AI?



Source: Omdia, N=964 | **Copyright**: ©2025 Omdia

From Omdia's research, AI is raising some concerns: The above data originates from Omdia's annual IT Decision Maker survey, which assimilates responses to key cybersecurity questions from just under 1,000 senior security professionals worldwide, and across the full range of industries and organizational sizes.

Resilient enterprises build stakeholder trust and drive sustainable growth

Resilient enterprises build stakeholder trust and drive sustainable growth

Preparation keeps resilient organizations one step ahead

An integrated approach to business resilience is crucial for staying ahead of evolving threats and ensuring long-term stability. This involves identifying critical assets and proactively monitoring and detecting potential threats, enabling organizations to take preemptive action that reduce the likelihood of breaches and associated costs.

The benefits of being prepared

Operational agility

The integrity and security of critical data and systems enable agile operations.

Data protection

Strong authentication and authorization ensure only the right users have controlled access to the right data sources, reducing risks.

Business focus

A strategy that enables resilience builds confidence and empowers enterprises to focus on innovation and business growth.

Collective responsibility

All employees across the enterprise are appropriately trained and involved and assume responsibility for cybersecurity and resilience.

Reputation and trust

Effective preparation helps to protect stakeholder trust and strengthens investor confidence.

Resilient enterprises build stakeholder trust and drive sustainable growth

Agile response and recovery enables continuity and trust

Cyberattacks are inevitable, making the ability to detect and respond to incidents in real time a key component of an agile and adaptive enterprise. By responding to cyberthreats and attacks with speed and efficiency, organizations can reduce downtime, prevent revenue loss and retain trust.

The benefits of an agile response and recovery

Respond decisively

A response plan is rapidly activated, with prescribed roles, communications and actions, avoiding panic and indecision during a breach.

Operational resilience

Ensure minimal disruption to the business by restoring critical assets and operations as part of the minimal viable company.

Data resilience

A robust 3-2-1 backup strategy (3 copies, 2 media types, 1 off-site/air-gapped) ensures data integrity and enables timely, reliable recovery in the event of data corruption or loss.

Financial resilience

Swift breach containment and recovery limits financial impact and protects the bottom line.

Emerge stronger and more secure

Effective post-incident recovery ensures malware is removed, vulnerabilities are remediated and systems are sanitized to restore full operational efficiency and strengthen the organization’s security posture.

“Robust cybersecurity must deliver the resilience needed for operational stability, financial viability, sustained innovation and growth.”

Rik Turner
Senior Principal Analyst, Cybersecurity
Omdia

Recommendations: How to be a resilient enterprise

Recommendations

Omdia sees a shift in what constitutes business resilience, moving beyond a **static** and reactive approach to operational continuity to one that enables organization-wide **agile and adaptive** resilience as an integral part of business strategy.

To address the risks presented by an expanding threat landscape and growing attack surface, including the risks of AI-driven threats, organizations must take an integrated approach to resilience that includes proactive preparation, a strong response strategy, robust recovery and a collaborative approach that spans all functions as well as the C-suite.

By embedding **resilience by design**, organizations can confidently navigate the fast-changing environment, maintain stakeholder trust, and achieve sustained performance and prosperity.

Recommendations

Enabling an agile and adaptive resilience strategy with an integrated approach to cybersecurity

Effective business resilience requires swift, coordinated action from preparation through to response and recovery. To achieve this, organizations must move beyond siloed efforts and embrace a tightly integrated, simplified approach to cybersecurity.

1 Prepare

Identify and protect critical assets and processes against a dynamic threat landscape.

- Identify critical assets and processes, and prioritize associated risks
- Proactively manage vulnerabilities with threat modeling and assessment
- Enable data discovery, visibility and protection with strong encryption and immutable backup
- Enable least privilege access control and multifactor authentication and authorization
- Apply zero trust principles across network infrastructure and cloud layers

2 Respond

Detect and respond to AI-driven cyberattacks with AI-enabled security operations and an incident response plan.

- Implement AI-enabled real-time threat monitoring and detection
- Execute an incident response playbook with clear roles and resonsibilities
- Embrace Agentic AI powered security operations to improve productivity and time to respond
- Integrated platform-first approach that enables unified security command and control center with a single-pane-of-glass view

3 Recover

Recover to a minimum viable company and emerge stronger and more secure.

- Restore minimum viable company with critical operations and relying on immutable data backup
- Conduct digital forensics to ensure infected systems and data have been isolated
- Execute a crisis management playbook and communications plan to ensure stakeholder trust and confidence
- Emerge stronger and more secure for the future

The role of the C-suite in business resilience

Business resilience is an organization-wide proposition that affects all roles and lines of business, even at board level. It is no longer only about preparation and response: today, the C-suite is accountable to the board for establishing operational continuity and clear recovery timelines in the event of a breach.

Facilitating and enabling the C-suite's role in business resilience

CEOs

CEOs need a strong operational environment to make informed decisions, stimulate innovation and growth, and instill stakeholder trust. When systems and data are not available to support this environment, a CEO needs to assume control and steer the organization back to the path of full operations.

CISO/CIOs

CISOs and CIOs need to combine cybersecurity platforms, services, people and policies to build a unified and layered cybersecurity capability that allows the organization to identify, respond to and recover from intrusions. A continuous process of testing and evaluation will ensure a robust security posture is maintained.

CROs and CFOs

Without adequate and robust systems for optimized operational delivery, reliable revenue streams are unlikely, raising concerns among employees and external stakeholders alike. CROs and CFOs need reliability and performance, both delivered through a resilient infrastructure. Assurance of revenue continuity will instil trust.

NTT DATA

Contact Us

Get in touch with NTT DATA's cyber resilience experts to discuss how you can enable an agile and adaptive resilience with an integrated approach to cybersecurity.

Contact us

About us

About us

NTT DATA

About NTT DATA

NTT DATA is a $30+ billion global innovator of business and technology services. We serve 75% of the Fortune Global 100 and are committed to helping clients innovate, optimize and transform for long-term success. As a Global Top Employer, we have experts in more than 50 countries and a robust partner ecosystem of established and startup companies. Our services include business and technology consulting, data and artificial intelligence, industry solutions, as well as the development, implementation and management of applications, infrastructure and connectivity. We are also one of the leading providers of digital and AI infrastructure in the world. NTT DATA is part of NTT Group, which invests over $3.6 billion each year in R&D to help organizations and society move confidently and sustainably into the digital future.

Visit us at: nttdataservices.com

Omdia

About Omdia

Omdia is a market-leading data, research and consulting business focused on helping digital service providers, technology companies and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development and go-to-market initiatives.

Our unique combination of authoritative data, market analysis and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Appendix

Authors

Authors

Rik Turner
Senior Principal Analyst,
Cybersecurity
askananalyst@omdia.com

Adam Strange
Principal Analyst,
Data Security
askananalyst@omdia.com

Sheetal Mehta
SVP and Global Head
of Cybersecurity

Copyright

Copyright notice and disclaimer

NTT DATA is a trusted global innovator of business and technology services, helping clients innovate, optimize and transform for success.
As a Global Top Employer, we have diverse experts in more than 50 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.