



Global Threat Intelligence Report

Featuring AI Driven Threats and Cyber Resilience

Volume 17 - September 2026

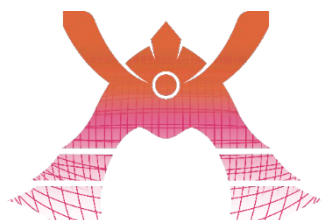
KDDI
KDDI Europe

KDDI
KDDI America

Table Of Contents

INTRODUCTION	3
This Month at a Glance	3
NEWS	4
The Latest Cybersecurity news	4
ReliaQuest Social Engineering Attack ^[1]	4
OZ Hair and Beauty Data Breach ^[2]	4
THREAT INSIGHTS	5
The Internet Is Full of Forgotten Doors. AI Just Learned to Find Them All.	5
REGULATORY INSIGHTS	8
Buying Digital Products After the Cyber Resilience Act: What IT leaders, security teams and procurement owners should now expect from technology suppliers	8
BLACK HAT USA 2026 REPORT	12
Observed Threat Trends at Black Hat USA 2026	12
SUGGESTIONS	16
Protection, Prevention and Takeaways	16
COMMON VULNERABILITIES AND EXPOSURES (CVES)	17
REFERENCES	18

Introduction



Welcome to the Global Threat Intelligence Report. This report provides a concise overview of recent cybersecurity threats, industry developments, and regulatory changes that may impact organisations worldwide.

At KDDI Europe, we remain committed to helping customers strengthen their cyber resilience through security expertise, continuous monitoring, and proactive threat intelligence. We hope the insights in this report support informed decision-making and stronger security outcomes.

With the addition of KDDI America's insights, the report now draws on expertise from across the KDDI Group, providing a broader perspective on emerging cyber threats and trends.

This Month at a Glance

This month's report examines how familiar weaknesses are being amplified across identity, cloud infrastructure and emerging technology. We cover the ReliaQuest social engineering attack and the Oz Hair & Beauty data breach, before exploring how AI can scale the discovery of dangling DNS records. Our Regulatory Insights section considers the Cyber Resilience Act from the buyer's perspective, outlining what organisations should expect from suppliers as the 11 September 2026 reporting obligations take effect. We also feature insights from KDDI America's observations at Black Hat USA 2026, highlighting AI-driven attacks, identity security, and cyber resilience.

Disclaimer

This content is provided for general informational purposes only and does not constitute legal advice. Readers should seek guidance from qualified legal professionals regarding the application of any law or regulation to their specific circumstances.

News

The Latest Cybersecurity news



Henry Finnah
Security Service Engineer



ReliaQuest Social Engineering Attack ^[1]

On 22 August 2026, ReliaQuest was targeted in a social engineering attack in which a threat actor created a fake ReliaQuest single sign-on (SSO) page and impersonated a security employee by phone to trick staff into entering credentials. One employee entered their password and approved an MFA prompt, briefly granting the attacker view-only access to an emerging technology dashboard session.

ReliaQuest stated that no applications, systems, or customer data were accessed. Existing security controls, including device trust policies and rapid containment actions, prevented further compromise and terminated the attacker's session.

Following an investigation, ReliaQuest confirmed no persistence was established and denied reports of ransomware or a broader breach.



OZ Hair and Beauty Data Breach ^[2]

In August 2026, Oz Hair & Beauty, the Australian online beauty and cosmetics retailer, disclosed that an unauthorised third party briefly accessed its online purchase and order platform. The company launched a forensic investigation, implemented containment measures, and reported the incident to the Australian Cyber Security Centre, the Office of the Australian Information Commissioner, and the New Zealand Privacy Commissioner.

Affected data for customers who made purchases before August 2026 may include names, email addresses, phone numbers, and purchase information. Oz Hair & Beauty stated that passwords, payment details, and credit card information were not accessed.

The incident is also listed on Have I Been Pwned (HIBP), which recorded approximately 2 million affected email addresses and added the breach to its database on 19 August 2026 .

Threat Insights



Hamza Bashir
Security Pre-Sales Consultant

The Internet Is Full of Forgotten Doors. AI Just Learned to Find Them All.

Billions of abandoned DNS records point to nothing. Researchers used AI to turn hundreds of them into working break-ins, against a federal agency, a bank, a carmaker and a drug company, in a single afternoon.

Every organisation leaves a trail of digital exhaust. A marketing team spins up a cloud server for a campaign, points a subdomain at it, `promo.yourcompany.com`, and moves on. Months later someone deletes the server to save money. Nobody deletes the subdomain. It now points at an address where nothing lives.

That is a dangling DNS record, and on a conservative estimate there are billions of them across the internet. Most sit harmlessly forever. None of them look dangerous. That assumption has just been proven catastrophically wrong. ^[3]

The forgotten door

The attack itself is not new, and it is embarrassingly simple. When a subdomain points to a deleted cloud resource, the link is left dangling, aimed at an address that is now up for grabs. An attacker who finds that record can go to the cloud provider, claim that exact address, and stand up their own server in its place. The subdomain now resolves to their infrastructure, wearing your company's name.

That is the dangerous part. `login.yourbank.com` still says `yourbank.com`. It carries your brand, your reputation, and the trust that every browser, email filter and employee extends to your domain. A phishing page hosted there does not look like a phishing page. It looks like you.

For years this stayed a niche technique, used mostly by criminals for modest financial gain. Checking whether a subdomain is genuinely exploitable, not just misconfigured but claimable, meant painstaking effort for every target. The

laboriousness was the defence. Nobody was going to comb millions of subdomains by hand.

Then somebody handed the job to an AI

Threat intelligence firm Silent Push asked a sharper question than the criminals ever had. Not how do I make money from this, but what would a nation-state do: someone who wants disruption rather than a payout, and who now has AI. They called the project DangleGeddon. ^{[4][5]}

The results should be read slowly. Starting from 12,500 domains, the team used an AI model to expand the hunt for subdomains far beyond what a human could enumerate, then filtered that flood down to the records that were genuinely exploitable, discarding everything without a claimable resource behind it. A dataset that would have taken days or weeks to work through by hand collapsed into a precise list of several hundred live targets. Then they automated the build-out of the infrastructure needed to seize them, leaving themselves, in their own words, one button push from Dangle Day. ^[5]

The targets were not obscure. A US federal government domain pointing at an unassigned Azure storage container, exploitable to serve phishing pages that inherit the trust of a .gov address. Société Générale, one of France's largest banks, with an Azure resource left dangling. Ford, with a development application gateway pointing at nothing, ripe for credential harvesting. Eli Lilly, with a narrower but usable exposure. Silent Push ran everything responsibly, replacing exploitation with a harmless security notice page and disclosing to the owners. A real attacker would have left something else. ^[4]

AI did not invent a new attack. It removed the friction that was quietly protecting everyone.

Most organisations cannot produce a current, accurate list of every subdomain they have ever created and where each one points today, and you cannot clean up leftovers you cannot see. Continuous discovery of your own external DNS footprint, correlated against which cloud resources still genuinely exist, is what turns a dangling record from an invisible liability into a ticket someone closes.

That is a monitoring discipline, not a one-off audit. The organisations that stay ahead of this are the ones watching their own attack surface the way an attacker does, all the time, looking for the door that was quietly left pointing at nothing.

The Bottom Line

There is no exploit here, no malware, no clever payload. Just a forgotten link, a trusted name, and, for the first time, an attacker patient enough to find every one of them, because that attacker is no longer human.

The question is not whether your organisation has dangling records. At any real size, it does. The question is whether you will find them before something that never gets tired does.

Regulatory Insights



Shintaro Takeda
Regional Chief Information Security Officer

Buying Digital Products After the Cyber Resilience Act: What IT leaders, security teams and procurement owners should now expect from technology suppliers

As Monica wrote in the previous report, the European Commission's July 2026 guidance clarified key questions on the Cyber Resilience Act (CRA), including remote data processing, open-source software, support periods and reporting obligations. ^{[6][7][8]} That article focused on organisations placing products with digital elements on the EU market.

This article looks at the other side: the organisations that buy, approve, introduce and operate those products. Product users are not the primary addressees of Article 14 reporting duties, but they depend on manufacturers to detect exploited vulnerabilities, communicate severe product-security incidents and provide corrective or mitigating measures. The 11 September 2026 reporting obligations therefore give buyers a timely reason to reassess supplier expectations. ^[9]

For CISOs, IT Managers and procurement owners, the CRA should not be treated only as a manufacturer compliance project. It is also a framework for asking better questions before approval, defining clearer contract responsibilities and ensuring supplier information reaches internal response teams quickly.

What Changes on 11 September 2026?

From 11 September 2026, manufacturers must report actively exploited vulnerabilities and severe security incidents affecting products with digital elements. The Commission sets out an early warning within 24 hours, full notification within 72 hours and a final report through the CRA Single Reporting Platform. ^[9]

These are manufacturer duties but they should change the buyer's conversation. Procurement review should test how suppliers identify affected products, communicate risk, distribute updates and support customers during a live event.

The Product Decision Is Also a Lifecycle Decision

Technology selection often focuses on functionality, integration, price and implementation effort. The CRA also requires buyers to assess post-purchase factors: support duration, vulnerability handling and customer communication when security conditions change.

A product that is secure at introduction may not remain secure. New issues can emerge in software, firmware or remote services, so buyers need confidence that suppliers can maintain security over time.

Four Decisions Product Owners Should Revisit

Decision	Old question	CRA-informed buyer question
Selection	Does the product meet our functional and security requirements today?	Can the supplier maintain the product securely throughout our intended period of use?
Contract	What service levels and support are included?	How quickly will we receive vulnerability, incident and mitigation information?
Introduction	Can the product be integrated into our environment?	Can it be inventoried, monitored, patched and isolated if the supplier reports a serious issue?
Renewal / Continued Use	Should we continue using or renew the product?	Can we continue using it securely, or do we need to replace, isolate or compensate?

Support Periods Become a Procurement Issue

The Commission guidance addresses CRA support periods. ^[8] Buyers should ensure security support aligns with intended use, refresh cycles and product dependency. If use continues beyond supplier support, lifecycle risk increases.

Before approval, the product owner should confirm:

- The security-support period and start date.
- Which versions and components receive updates.
- Whether updates require extra licences or support.
- How end-of-support and major security changes are communicated.
- Whether the organisation can replace, isolate or manage the product when support ends.

CE Marking Is Not Ongoing Assurance

CRA conformity assessment, the EU Declaration of Conformity and CE marking apply from December 2027. ^[7] They are useful compliance signals, but buyers still need to assess product risk against their own architecture, data, privileges and operational dependencies.

From Supplier Notification to Customer Action

The CRA reporting timetable is based on manufacturer awareness and notification duties. ^[9] Product users still need an internal process so supplier advisories reach the right owner and can be matched to deployed versions.

Organisations should turn supplier notifications into rapid action: locate deployments, confirm affected versions, assess mitigation and track remediation. These are buyer practices, not separate Article 14 duties.

- Supplier: provide advisories, affected versions, mitigations and updates.
- Procurement/vendor management: route notices to technical owners.
- Product owners: identify deployments, dependencies and constraints.
- Security operations: assess exposure and prioritise action.
- Change/risk owners: approve remediation, exceptions or controls.

Supplier Evidence Checklist Before Approval

Area	Checklist item	Supplier evidence
Ownership	Confirm who owns product security and customer notification.	Named security contact and escalation route.
Vulnerabilities	Confirm how vulnerabilities are reported, validated and tracked.	Disclosure policy and vulnerability-handling process.
Components	Confirm how affected dependencies and versions are identified.	Component information (SBOM).
Updates	Confirm how security fixes are distributed and prioritised.	Update policy, supported versions and advisory examples.
Incidents	Confirm how customers are notified of exploited vulnerabilities or severe incidents.	Notification process and contractual commitments.
Lifecycle	Confirm what happens when security support ends.	Support period and end-of-support policy.

Contracts Should Support What Buyers Expect

The CRA does not write the customer's contract. Buyers should ensure terms cover notification routes, information content, updates, investigation cooperation, subcontractor dependencies and end-of-support notice.

Terms should reflect product risk and business criticality. Low-impact applications may need a lighter review, while privileged, sensitive, OT-connected or critical products require stronger evidence and escalation arrangements.

Internal Actions Product Buyers Should Take Now

The September milestone is an opportunity to improve internal technology governance before the full CRA regime applies in December 2027. These actions help product users turn supplier information into ownership, workflow and response changes.

Focus	Immediate action	Outcome
Classify products	Apply deeper review to products with high privilege, sensitive data or critical service dependencies.	Assurance effort matches business risk
Strengthen approval	Embed supplier evidence checks into product approval workflows.	Approval requires security evidence
Map ownership	Record internal business owner, technical owner and deployed versions.	Internal ownership is clear
Review contracts	Check notification, update, investigation and end-of-support provisions.	Supplier expectations are explicit
Connect advisories	Route supplier notices into vulnerability, incident and change workflows.	Supplier information drives response
Test a scenario	Exercise an actively exploited supplier vulnerability affecting a critical product.	Gaps are found before a real event

Conclusion

As Monica wrote in the previous report, the July 2026 Commission guidance gave manufacturers and other economic operators greater clarity on the CRA.^{[8][10]} For product users, the September reporting milestone sends a practical message: supplier security should remain visible through introduction, operation, renewal and continued use.

The CRA places the primary reporting obligation on manufacturers, but product users depend on the quality and speed of the manufacturer's response. Organisations that know what they operate, who owns it, how long it is supported and how notifications reach response teams will be better positioned to act when serious vulnerabilities emerge.

Black Hat USA 2026 Report



Yuka Homma
Security Service Engineer

Observed Threat Trends at Black Hat USA 2026

About The Conference

Black Hat USA 2026 was held in Las Vegas from August 1st to August 6th.

Black Hat, an international computer security event series founded in 1997, is one of the largest and respected cybersecurity conferences in the world. It is where security researchers, vendors, and government agencies share the latest attack techniques, defensive strategies, industry trends and market trends.

Autonomous “Agentic” Artificial Intelligence (AI) and Frontier AI models dominated the majority of the events’ topics, while topics such as identity security, ransomware, and supply-chain risk were also discussed.

This report summarizes the three major trends we, KDDI America, observed at Black Hat USA 2026.

The Three Trends and Our Responses

Trend 1: AI Is Scaling Up Existing Attack Methods

A big highlight of this year’s presentation was on how fast and cheap cyberattacks can be mass-produced.

In one presentation, AI successfully generated working exploits for 182 out of 200 vulnerabilities. On average, each exploit took approximately 21 minutes and cost \$3.61 to create¹. In another presentation, an AI-driven team reached full domain control of a realistic enterprise environment in roughly 20 minutes².

With the price of AI, criminals are now able to expand their existing criminal ecosystems similar to how a business would expand. As a result, Ransomware-as-a-Service (RaaS) has converted cyberattacks into a franchised business with specialized roles for developers, access brokers, affiliates, and launders.

¹ From Briefing session “Keynote: The End of Rare: Defending When Offense Is Cheap” by David Weston, Aentic Security Leader

² From Briefing session “Catch Me If You Can: AI Investigators Hunting Autonomous Attackers” by Jayson Grace, Principal Software Architect, Dreadnode, Martin Wendiggensen, AI Research Scientist, Dreadnode, and Shane Caldwell, Principal Research Engineer, Dreadnode

When a RaaS organization called LockBit³ got taken down, the wider threats persisted, as its affiliates immediately dispersed into smaller cells to reconstitute themselves. The concern now is what happens when AI-driven automation is layered on top of that mature ecosystem: the volume, speed, and accessibility of attacks rise sharply.

Trend 2: Identity as the Common Attack Surface

Not every threat this year was about autonomous AI. Identity remains a common attack surface.

Importantly, attackers no longer need to steal a password to abuse identity. On-site examples ranged from confusing a directory service into trusting an attacker as someone else, to socially engineering a helpdesk into removing Multi-factor Authentication (MFA). In a recent cloud breach, attackers exploited helpdesk processes to bypass identity verification, retrieved a GitHub token from a password manager, and used legitimate cloud features to execute a script, resulting in a \$107 million loss⁴. Each action appeared completely normal on its own; the attack was only visible when the entire sequence was correlated. Non-human identities were also an important topic this year. Service accounts, access tokens, and AI-agent identities are increasing, but many organizations do not manage them as carefully as employee accounts. As the case showed, one exposed token may be enough to reach highly sensitive systems and data.

Trend 3 - From Monitoring and Prevention to Detection, Response, and Resilience

Prevention remains essential, but organizations must assume that some attacks will succeed and design for continued operation and recovery. As stated during the Locknote⁵ session, organizations should aim to be “secure enough to continue operating,” rather than expecting perfect protection.

This shift was closely tied to how AI is being used in security operations.

³ LockBit is a major cybercriminal group and ransomware-as-a-service (RaaS) operation. They have hit a lot of global enterprise, hospitals and government agencies. LockBit's core ransomware infrastructure was dismantled by international law enforcement in February 2025 as part of a multi-county initiative known as Operation Cronos.

<https://www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant>

From Briefing session “Anatomy of a Takedown: Inside the Operation That Broke LockBit” by Brett Leatherman, Cyber Division Federal Bureau of Investigation and Paul Foster, interviewer

⁴ From Briefing session / “The Crypto Caper: Exposing a Sophisticated Multi-Cloud Bandit” by Yotam Meitar, Cloud Response, Wiz

⁵ Locknote is a closing panel discussion where analyzing key conference takeaways and provide valuable insights on how emerging trends will shape future security strategies.

From Briefing session “Locknote: Conclusions & Key Takeaways from Black Hat USA 2026” by Stephanie Domas, VP SecurityMozilla, Nathan Hamiel, Senior Director of ResearchKudelski Security, Jason Healey, Senior Research ScholarColumbia University SIPA, Jeff Moss, FounderBlack Hat & DEF CON, and Window Snyder, Founder & CEOThistle Technologies

The consistent message was that AI works best not as a fully autonomous “black box,” but as a controlled component with clear roles, limited permissions, and human review - a model best described as human augmentation, not replacement. Some speaker said that AI can accelerate triage, evidence collection, and investigation, but its level of autonomy should reflect the risk and potential impact of each action. Routine, low-risk tasks may be automated, while higher-risk actions should require human oversight and approval. The critical driver is speed: when attacks can escalate in minutes, any process that assumes a human has time to review every alert before impact is already outmatched, making fast, partly automated detection and response essential.

Overall Recommendations

Based on these 3 trends, we recommend that readers review the following five priorities. They map directly to the trends above: visibility and identity address the industrialized, identity-driven threat, while detection, resilience, and AI discipline support the shift toward detection and response.

1. Improve asset and risk visibility:

Inventory internal assets, IoT devices, Active Directory, cloud identities, SaaS applications, and non-human accounts. Organizations cannot protect what they do not know exists. Beyond a one-time assessment, Continuous Threat Exposure Management (CTEM) approach can help continuously identify, assess, and prioritize exposures as environment changes.

2. Put identity at the centre of Security Architecture:

Apply least privilege and strong MFA (such as passkeys/FIDO2⁶ or security keys, especially for privileged accounts), strengthen approval processes for password and MFA resets, review privileges regularly, and monitor unusual account-attribute changes, authentication workflows, and privileged activity.

3. Detect and respond across data sources:

Correlate activity across identity, endpoints, and cloud. If AI is introduced, automate routine investigation but decide in advance which decisions AI can make alone and which require a human.

4. Assume breach and prepare for recovery:

⁶ FIDO2 is an open authentication standard that enables password less, phishing-resistant sign-in using public-key cryptography, with the private key securely held in the user’s device or hardware authenticator.

Run incident-response exercises, test recovery procedures, centralize logging with longer retention, and assign clear risk ownership.

And of course, none of this works without people. Security awareness training keeps employees ready to recognize and report attacks. Together, these form the foundations of operational resilience.

5. Adopt AI with discipline

Define where AI can act on its own, where human review is required, how results are validated, and how AI vendors and their security claims are independently evaluated.

AI should be introduced first in areas where processes, data quality, and operational ownership are already mature.

Closing

“Perfect protection is not a realistic goal.” (Stephanie Domas, Locknote Closing Panel Discussion)

Instead, organisations should aim to build sufficient and resilient security to limit the impact of attacks. Even when an intrusion occurs, systems should recover quickly and ensure business continuity. AI adoption should be implemented effectively and responsibly to support business objectives.

Suggestions

Protection, Prevention and Takeaways

1

Implement phishing-resistant MFA, device trust policies, and conditional access controls. Although an employee approved a malicious MFA request, ReliaQuest's device-trust controls prevented the attacker from accessing internal applications and customer data and this should be used to highlight the importance of having the appropriate security measures.

2

Customer-facing e-commerce platforms remain attractive targets for attackers. Even when payment data is protected, exposure of names, email addresses, phone numbers, and purchase histories can still lead

to phishing, account takeover attempts, and identity fraud.

Reduce the attack surface by implementing strong access controls, continuous monitoring of web platforms, regular security testing, and secure configuration management. Organisations should also minimise stored customer data and review data retention policies to reduce the impact of a compromise.

3

Maintain a risk-based patch management programme and prioritise actively exploited vulnerabilities. CVE-2026-68820 was exploited in the wild before patches were applied, highlighting the need for rapid deployment of vendor security updates and continuous monitoring for privilege-escalation activity

Common Vulnerabilities and Exposures (CVEs)

Every month a CVE is selected at the discretion of the report's author to be discussed. This month it is a vulnerability affecting Microsoft windows Desktop and servers that has actively been exploited in the wild.

CVE-2026-68820| EUVD-2026-56468 ^[10]

Vendor	Microsoft
Product	Windows 11 & 10, Windows Server 2012, 2016, 2019, 2022 & 2025
Publish Date	Aug 11, 2026
Platform	-
CVSS (v3.1)	7.0

Description

Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.

What does this mean for you?

An attacker who gains an initial foothold through phishing, malware, or stolen credentials may be able to obtain full administrative control of affected Windows devices.

What should you do about it?

Where affected Windows versions remain within Microsoft's support lifecycle or are covered by Extended Security Updates (ESU) programmes, deploy the August 2026 security updates immediately. For unsupported versions which may not have released a security update, upgrade to a supported Windows release and apply the latest available security updates.

References

1. ReliaQuest Threat Research (2026) A Social Engineering Attempt Against ReliaQuest: What We Found. ReliaQuest, 22 August. Available at: <https://reliaquest.com/blog/threat-spotlight-social-engineering-attempt-against-reliaquest-what-we-found/> (Accessed: 26 August 2026).
2. Oz Hair & Beauty (2026) Important Update About A Cyber Incident. Oz Hair & Beauty. Available at: <https://www.ozhairandbeauty.com/pages/official-statement-regarding-cyber-incident> (Accessed: 26 August 2026).
3. Ionix (2026) *Dangling DNS: the most overlooked attack surface in the AI era*. Available at: [Dangling DNS in the AI Era: The Silent Attack Surface Expanding Beneath Your Feet - IONIX](#) (Accessed: 24 August 2026).
4. SecurityWeek (2026) *'DangleGeddon': AI could weaponize forgotten DNS records at global scale*. Available at: <https://www.securityweek.com/danglegeddon-ai-could-weaponize-forgotten-dns-records-at-global-scale/> (Accessed: 25 August 2026).
5. Silent Push (2026) *DangleGeddon research disclosure*. Available at: [Danglegeddon: The Full Research Report Is Now Available - Silent Push](#) (Accessed: 28 August 2026).
6. KDDI Europe (2026) *Global Threat Intelligence Report Volume 16: Cyber Resilience Act: New Commission Guidance Clarifies the Road to September 2026 Reporting Obligations*. Article by Monica Galiano.
7. European Parliament and Council of the European Union (2024) *Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements*. Available at: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> (Accessed: 31 August 2026).
8. European Commission (2026) *Commission publishes new guidance to support timely Cyber Resilience Act implementation*. Available at: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation> (Accessed: 31 August 2026).
9. European Commission (2026) *Cyber Resilience Act - Reporting Obligations*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting> (Accessed: 31 August 2026).
10. European Union Agency for Cybersecurity (ENISA) (2026) CVE-2026-68820. EU Vulnerability Database (EUVD). Available at:

<https://euvd.enisa.europa.eu/vulnerability/CVE-2026-68820> (Accessed: 26 August 2026).

Let's Secure the Future — Together



KDDI America

KDDI America is the North American headquarters of KDDI Corporation, a Fortune Global 500 company, delivering cloud, networking, cybersecurity, and managed IT services. Through innovative ICT solutions, KDDI America helps organisations connect, transform, and grow in an increasingly digital world.

KDDI Europe

KDDI Europe is the European headquarters of KDDI Corporation, a Fortune Global 500 company, delivering trusted ICT and cybersecurity solutions backed by Japanese quality and reliability. With over 70 years of global expertise, we help organisations build secure, scalable infrastructure and strengthen their cyber resilience.

Whether you're looking to strengthen your cybersecurity posture or scale your global operations, we are your partner, your enabler, your platformer.

Security of Tomorrow, Today.

Contact Information

KDDI Europe



[Website](#)



[LinkedIn](#)



[Enquiry](#)

KDDI America



[Website](#)



[LinkedIn](#)



[Enquiry](#)