CLOUDGUARD
Security Done Different

Security. Done Different.

Financial Services & Insurance

Global Threat Intelligence – Q1 2026

Document version 2.2

16/03/2026

Classification: Unclassified

Contents

Version History

Version	Author	Date	Status
1.00	CloudGuard	21/03/2025	Reviewed
2.00	CloudGuard	23/05/2025	Reviewed
2.1	CloudGuard	03/09/2025	Reviewed
2.2	CloudGuard	15/03/2026	Released

Environment Scope

The following information applies to the UK Financial Services and Insurance sector.

Executive Summary

The UK Financial Services, Insurance and private investor sector faces its highest threat level recorded by CloudGuard Intelligence since monitoring began.

The March 2026 assessment returns an overall threat **score of 84/100,** a 10-point increase from February, driven by a convergence of nation-state escalations, industrialisation of automation threat actor reconnaissance activities, surging credential theft activity on dark web markets, a wave of targeted attacks against wealth management and advisory firms globally, and elevated **FCA** and **ICO** enforcement following significant operational incidents.

Four distinct threat streams are operating simultaneously against this sector this month:

1. Financially motivated ransomware and data extortion groups (primarily DragonForce and Scattered Spider affiliates);
2. Iranian state-aligned hacktivist groups executing DDoS and mass automated vulnerability rapid exploitation campaigns against UK financial infrastructure;
3. North Korean state-sponsored actors specifically targeting UK-based cryptoasset firms and private investor platforms;
4. AI-enhanced phishing, deepfake partner impersonation, and infostealer malware are the primary delivery mechanisms across all streams.

The regulatory environment is simultaneously changing. The **FCA's** new operational incident reporting regime (in consultation since late 2024) is expected to be finalised in Q2 2026, significantly expanding disclosure obligations.

The ICO continues active enforcement against firms with inadequate controls around personal data exposed in incidents. Firms that cannot demonstrate operational resilience through documented evidence, detection telemetry, incident timelines, remediation records, face compounding regulatory and reputational exposure.

The **EU AI Act** will also feature significantly in the plans for Financial Services organisations now scaling out AI led cost and service optimisation strategies with highly innovative AI first solutions.

CLOUDGUARD

UK Financial Services & Private Investor

Cyber Threat Intelligence

Q1 2026 | Quarterly Intelligence Report

—

Threat intelligence | Dark web insights | Regulatory incidents

Sector leakage | Active threat actor tracking

Prepared by CloudGuard Threat Intelligence Unit

THREAT LEVEL

CRITICAL

Financial Services & Private Investors

Score: 84/100

▲ +10 pts vs Feb 2026

Security Done Different

Overall threat score	Active threat groups	Dark web credentials	FCA incidents (2025)
84/100	**11**	**2.1bn+**	**294**
CRITICAL	Targeting UK finance	Leaked in 2025	187 cyber-attributed

Threat landscape — Q1 2026

The UK financial sector is the single most targeted industry vertical in the country's cyber threat landscape, accounting for approximately **28%** of all UK cyber-attacks. In Q1 2025 alone, more than **70%** of London financial institutions reported attempted breaches, a figure CloudGuard Intelligence assesses as likely to have increased further through the first quarter of 2026. Three macro-level threat drivers are shaping this month's threat picture.

1. Nation-state and state-aligned threat actors

NCSC Active Alert — January 2026

On 19 January 2026, the NCSC issued a formal alert confirming persistent targeting of UK organisations by Russian state-aligned hacktivist groups. The NCSC handled 204 nationally significant cyber-attacks in 2025, more than double the 89 incidents from 2024. This represents **four major** attacks hitting UK organisations every week.

Russia (GRU/SVR affiliated groups and aligned hacktivists), China (multiple APT groups), Iran, and North Korea represent the four primary nation-state threat actors assessed by NCSC as targeting UK interests. Their relevance to the financial sector differs by actor:

- **Russian-aligned hacktivist groups** (NoName057(16), Cyber Army of Russia Reborn, Z-Pentest) are executing DDoS campaigns against UK financial infrastructure, payment platforms, and investment portals. Attacks are typically ideologically motivated, retaliation for UK policy on Ukraine, and are escalating in frequency and sophistication. Many of these are now **NCSC** explicitly warned in January 2026 that these groups are moving beyond website disruption toward operational technology targeting. Active vulnerability exploitation of zero day (many firewall technology stacks) are leveraging AI generative automation from Censys fields to escalate attack vectors from reconnaissance in minutes and hours from identification.
- **North Korean state-sponsored actors** (Lazarus Group and affiliated units) are specifically targeting UK-based cryptoasset firms and private investor platforms. NCSC confirmed in its 2025 Annual Review that UK cryptoasset firms are currently at risk of DPRK-linked hackers seeking to steal funds. Additionally, DPRK IT workers disguised as freelance contractors are almost certainly operating within UK financial services firms, creating insider threat risks.
- **Chinese APT groups** are conducting long-term espionage operations against UK financial institutions holding data on high-net-worth individuals, M&A activity, and government-related investment flows. These intrusions prioritise persistence and data exfiltration over disruption. APT10 (also known as Stone Panda, MenuPass, Red Apollo, Cloud Hopper and POTASSIUM) has specifically increased focus on MSP's supporting Financial Services, Wealth Management platforms and Private Equity companies. UNC5221 has continued to focus critical and high severity network and VPN vulnerability exploitations specifically for no day entities. APT41 (also known as Brass Typhoon, Wicked Panda, BARIUM and Double Dragon) has been the most active in detailed reconnaissance and new strain of malware TTP's.
- **Ransomware groups** with various affiliations and tactical geopolitical alignment (DragonForce, Scattered Spider affiliates) are primarily financially motivated to execute identified exploitation paths of new TTP strains giving them de facto operational freedom.

2. Financially motivated criminal threat actors

Ransomware remains the most acute and pervasive threat to UK financial organisations in 2026. Sophos data indicates **65%** of financial services organisations were hit by ransomware in 2024, the highest rate since tracking began, and **49%** had data successfully encrypted. Ransomware groups have evolved their tactics in two critical ways that elevate risk specifically for financial and investor firms:

- Extortion without encryption: groups increasingly **exfiltrate/steal data** smaller quantities of data and seek a dark settlement. The continual threat to publish (alternative TTP) without deploying encryption. This is solely evading NCSC involvement and FCA reporting particularly damaging for firms holding sensitive client financial planning data, HNW client portfolios, and personal KYC records.

- Typical settlements are within **14 days** and usually involve a dual monetisation TTP where the attack format is resold to another affiliate and repeated or mimicked within 180 days.
- Targeted timing: threat actors are now conducting **reconnaissance** over weeks or months before activating payloads, timing attacks to coincide with high-value transaction periods, M&A activity, annual reporting cycles, or regulatory submission deadlines to maximise leverage and demand compliance. There is now specific focus towards advisory firms.
- **Wealth management and RIA targeting**: ShinyHunters claimed in February 2026 to have stolen five million records from Mercer Advisors and over 100,000 from Beacon Pointe Advisors (US-based but instructive for UK equivalents). Edelman Financial Engines ($323bn AUM) confirmed a breach in January 2026. The pattern, targeting advisory firms with HNW client data, is directly applicable to UK wealth managers, IFAs and private investor platforms.

3. AI-enhanced attack capabilities

Threat actors across all categories are now generative-AI first in **Cyber Kill chain** steps 1 & 2 to enhance attack efficiency to under 60 minutes. The NCSC's 2025 Annual Review confirmed that actors linked to China, Russia, Iran and DPRK are operating large language models (LLM's) to evade detection, support reconnaissance, automate post-breach stages, and conduct AI-assisted vulnerability research and exploit development. The financial sector currently is experiencing specific AI-enhanced threats in the following areas:

- Deepfake Senior role and Partner impersonation: approximately £100 million was lost to investment scams driven by **deepfake videos** in the first half of 2025 alone (NCSC). Deloitte reports deepfake incidents increased by up to 700% in certain financial industry segments. UK Finance has specifically warned that criminals are impersonating executives to initiate fraudulent transactions, a direct threat to investment authorisation and fund transfer workflows. As Diffusion and Transformer models accelerate faster than detection capabilities, and human capabilities to accurately detect increasing more realistic deep fakes gets harder, this is an increasing exploitation gap.
- High curated, lower confidence scoring, AI-generated **spear phishing**: fully automated, highly personalised and confidence score tested phishing campaigns are now being generated at scale against financial services staff. Financial services remains the most impersonated industry for phishing at **34%** of all activity, and phishing is the initial access method in **46%** of attacks targeting the sector. Threat actors will typically analyse MX records for email security identification and confidence test highly curated emails with current topic alignment to target individuals.

- Infostealer malware acceleration: infostealers (RedLine, Lumma, RaccoonStealer variants) are now deployed via **AI-assisted targeting**, dramatically reducing the time between initial infection and credential harvesting. Stolen credentials appear on dark web markets within hours of compromise.

Dark web intelligence — financial services exposure

> **CloudGuard dark web monitoring — Q1 2026 snapshot**
>
> The following intelligence reflects patterns observed across dark web marketplaces, ransomware leak sites, infostealer Telegram channels, and breach repositories monitored by CloudGuard's Intelligence Unit during Q1 2026. Specific client domain monitoring data is available on request.

Credential markets and infostealer activity

Threat researchers compiled over 2 billion unique leaked credentials from **dark web combo lists** in 2025, a figure that continues to grow into early 2026. These credentials include email/password combinations, sometimes using federated synthetis and session tokens harvested by infostealer malware, with financial services domain credentials commanding significant premiums on underground markets. Key observations this month:

- Initial Access Broker (IAB) listings for UK financial services firm VPN and remote access credentials averaged approximately **£2,700 per listing** in 2025, with **71%** of listings including elevated privileges, effectively providing ransomware operators with turnkey network access.
- Infostealer malware logs containing financial services employee credentials are appearing on dark web Telegram channels within hours of infection. The rapid monetisation cycle means credential compromise to active exploitation can now **occur within 24–48 hours**, well inside the detection window of firms without continuous monitoring.
- Infostealer malware is targeting personal mobile devices via generative AI social media exposure scanning of **target individuals** as well as instant messaging channels. Highly curated Infostealer packages are created which sneek and hijack session tokens from various cache locations on grey or shadow IT devices.
- Infostealer infestations via Agentic logic and malware embedded into **Generative AI tools** and mobile applications. These are proving very difficult to detect and protect as user behavioural analysis may not fully cover all devices or areas of the memory or devices.
- Corporate VPN credential leaks from UK financial institutions are appearing on dark web search platforms before victim firms are aware of the compromise. Several

2024–2025 ransomware incidents in the financial sector were directly initiated by **VPN credentials** stolen via infostealer malware purchased for under £50.

- Session token theft (rather than password theft) is increasingly prevalent, allowing attackers to **bypass MFA** by stealing authenticated session cookies directly from browser memory. This is specifically relevant to wealth management portal access, trading platform sessions, and back-office financial systems.

Financial data dark web marketplace trends

Dark web marketplaces continue to trade in **high volumes** of financial sector data. The following data types are most actively traded in relation to UK financial services and private investor targets:

Data type	Dark web value	Primary threat vector
Full KYC identity packages ("fullz")	**Very High — £200–£2,000+**	Account takeover, identity fraud, APP scams
Investment account credentials	**High — £50–£500 per account**	Unauthorised trading, fund transfers
Client financial planning data	**High — leverage for extortion**	Ransomware targeting, BEC fraud
Corporate banking login credentials	**Very High — often auctioned**	Business fund transfers, authorised push payment fraud
HNW client PII and portfolio data	**Very High — targeted sale**	Spear phishing, social engineering, investment fraud
Pension and ISA account details	**Medium-High**	Pension liberation fraud, account recovery abuse
Staff Microsoft 365 credentials	**Medium — £10–£50 per account**	BEC, lateral movement, data exfiltration
Session tokens / browser cookies	**High — MFA bypass value**	Portal takeover, trading platform access

Ransomware leak sites — financial sector victims

Ransomware groups operating leak sites published financial sector victims at an elevated rate in Q4 2025 and Q1 2026. The pattern shows a strategic shift toward wealth management firms, insurance intermediaries and financial advisory businesses, organisations holding **high-value client data** but historically less well-defended than major banks. Active ransomware groups targeting UK financial services this month:

Threat group	Threat level	Primary targeting profile
DragonForce	**Critical**	Broad financial sector; responsible for Co-op attack (6.5m records). Expanding to mid-market wealth managers and payment processors.
Scattered Spider / UNC3944	**Critical**	Social engineering specialists. Targeted UK retail 2025 via third-party. Actively reconnoitring UK financial services supply chains.
ShinyHunters	**High**	Wealth management and RIA firms. Claimed 5m records from Mercer Advisors Feb 2026. Extortion model — threatens data publication without encrypting.
LockBit 3.0 affiliates	**High**	Broad; preference for firms with cyber insurance (higher ransom compliance). Double-extortion. ERP and banking system targeting.
Fog ransomware operators	**High**	Financial institutions specifically. May 2025: exploited employee monitoring software to harvest credentials over 2 weeks before deploying ransomware.
BlackBasta affiliates	**Medium**	Mid-market financial services. Phishing and MFA fatigue primary entry. Active against UK asset managers and independent advisors.
NoName057(16)	**High**	Russian hacktivist. DDoS against UK financial infrastructure, payment portals, investment platforms. Ideologically motivated.

Brand impersonation and investment fraud

> Lookalike domains impersonating UK financial services firms and investment platforms circulate across dark web forums and are used to harvest credentials from targeted victims. CloudGuard Intelligence has observed this pattern specifically deployed against wealth management portals, online trading platforms, and SIPP/ISA providers. Monitoring for domain registration variants and brand impersonation is a critical defensive measure that most mid-market financial firms do not have in place.

FCA & ICO regulatory incidents — reported activity

The regulatory picture for UK financial services in 2025–2026 reflects a sector under significant incident pressure. The FCA has noted a **significant increase** in cyber incidents from the 166 material cyber incident reports from regulated firms in 2024, a record high, of which **89 were attributed to cyber attacks** and 33 involved confirmed data breaches. These figures represent only reported incidents; the actual number is substantially higher. Dark settlements remain untracked and UK parliament has yet to approve the latest Cyber Security and Resilience Bill.

FCA incident reporting landscape

2024 FCA material cyber incidents

166

Material incidents reported to FCA

89 attributed to cyber attacks

33 involved confirmed data breaches

Key regulatory context

- The FCA and PRA have proposed new operational incident reporting rules (CP24/28) expected to be finalised in Q2 2026. This will expand mandatory reporting thresholds and create parallel obligations alongside existing GDPR/ICO requirements.
- Firms must report material operational incidents under SUP 15 of the FCA Handbook. Cyber attacks that also involve personal data trigger concurrent ICO notification obligations under UK GDPR within 72 hours.
- The FCA and ICO operate under a Memorandum of Understanding for coordinated investigations. A single significant cyber incident can therefore trigger dual regulatory enforcement.
- DORA (Digital Operational Resilience Act) applies from January 2025 for firms with EU operations, adding a third regulatory reporting stream with its own ICT incident classification and timeline requirements.

Significant regulatory enforcement actions — 2025–2026

The following enforcement actions and incidents are directly relevant to the current risk environment for UK financial services and private investor firms:

FCA **Nationwide Building Society** *December 2025* **Fine of £44,078,500**	FCA issued a final notice imposing a fine of **£44,078,500** for inadequate financial crime systems and controls. While primarily a financial crime enforcement action, it signals the FCA's continued appetite for large-scale enforcement in the financial services sector and the expectation of robust, documented control frameworks.
FCA **UK Financial Sector (multiple firms)** *2024 (reported May 2025)* **166 material cyber incidents filed**	FCA data confirmed 166 material cyber incident reports for 2024, the highest recorded total. Of 89 cyber-attack incidents, attack types included ransomware, BEC, credential attacks, and third-party supply chain compromises. The FCA noted that incident reporting delays mean some 2024 reports relate to incidents occurring in prior periods.
FCA / PRA **UK Operational Resilience Regime** *March 2025 (implementation deadline)* **Mandatory implementation deadline passed**	All FCA and PRA regulated firms were required to implement operational resilience frameworks, including impact tolerances, important business service mapping, and scenario testing, by 31 March 2025. In 2026, the FCA's supervisory focus shifts to testing and enforcement, firms that cannot demonstrate compliance with documented evidence face enforcement action.
BoE / PRA / FCA **Critical Third Parties (CTP) regime** *January 2025 (effective)*	The CTP oversight regime became effective from January 2025, imposing operational resilience, incident reporting, and disclosure obligations on major technology providers serving the financial sector. This means that cloud providers, data vendors, and managed service providers supporting financial

New regulatory regime commenced	firms are now directly regulated, changing the risk profile of third-party dependencies.

Sector threat leakage — recent financial services incidents

The following incidents, drawn from publicly reported cases and intelligence sources, represent the threat patterns most directly applicable to UK financial services and private investor firms in Q1 2026. Each carries direct lessons for how **CloudGuard-protected firms** should position their defences.

Global wealth management and advisory firm targeting

Pattern alert: ShinyHunters targeting advisory and wealth management firms

In February 2026, the ShinyHunters cybercrime group issued final-warning extortion notices to Mercer Advisors and Beacon Pointe Advisors (both US-based), claiming theft of five million and 100,000+ records respectively. Edelman Financial Engines ($323bn AUM) confirmed a breach on 7 January 2026 where an unauthorised third party accessed client personal and financial planning information. Multiple smaller RIA firms reported data incidents in the same period. The common thread: advisory firms managing extensive personally identifiable information and detailed financial records of affluent clients are being systematically targeted. The UK equivalent, independent financial advisers, wealth managers, multi-family offices, and boutique asset managers — carries identical risk characteristics.

UK retail sector attack — lessons for financial services

The coordinated **DragonForce** ransomware campaign against Marks & Spencer, the Co-op, and Harrods in 2025, executed by Scattered Spider affiliates via a compromised third-party service provider, produced lessons that are directly transferable to financial services firms. The Co-op alone saw 6.5 million member records stolen. The attack demonstrated:

- Shared vendors and cloud integrations create **single points of failure** across entire sector ecosystems. Financial services firms using common fintech infrastructure, data providers, or managed service providers face the same cross-firm exposure.
- Third-party access management, specifically the management of vendor remote access, privileged credentials, and session monitoring, was the primary exploited weakness.

- The shift from encryption-focused ransomware to data exfiltration-first extortion is specifically relevant to financial firms where data publication can trigger **regulatory consequences** (ICO notification, FCA reporting) and reputational damage to HNW client relationships that is disproportionate to the operational impact.

Infostealer campaigns targeting financial services credentials

A May 2025 ransomware attack on an Asian financial institution (attributed to Fog ransomware operators) revealed a new attack pattern: attackers used a legitimate employee monitoring system (Syteca) to harvest credentials via keylogging over a two-week period before deploying ransomware. This represents the maturation of a "slow burn" approach where attackers establish privileged access, harvest credentials from multiple accounts, and map the environment thoroughly before the attack becomes visible. This pattern is specifically relevant to:

- Financial firms using remote monitoring and management (RMM) software or employee monitoring tools that can be **weaponised** by an attacker with initial access.
- Organisations where the interval between credential compromise and detection exceeds two weeks, the industry average detection time for financial sector incidents is currently **241 days**.
- Firms where privileged account credentials (especially those for core banking, trading, and back-office systems) are not rotated regularly or monitored for anomalous use.

OCC email breach — supervisory data exposure precedent

> In April 2025, the US Office of the Comptroller of the Currency (OCC) disclosed that executive emails containing highly sensitive supervisory information had been hacked. The breach was attributed to longstanding vulnerabilities and involved access to regulated firm examination data, financial institution risk assessments, and confidential supervisory correspondence. This incident is significant for UK financial services because it establishes a documented precedent for the targeting of regulatory supervisory data — information held both by regulators and by financial firms themselves as part of their regulatory submissions and correspondence. UK firms holding detailed FCA correspondence, PRA supervisory letters, and internal audit reports should treat this data category as high-value and apply appropriate access controls.

DPRK insider threat in UK financial firms

The NCSC confirmed in its **2025 Annual Review** that UK firms are almost certainly being targeted by IT workers from the DPRK, disguised as freelance third-country IT staff, generating revenue for the North Korean regime. The financial services and technology sectors are primary targets. This threat manifests in three ways:

- Contracted developers or technical staff who are in fact North Korean state employees, using legitimate employment channels (freelance platforms, recruitment agencies, remote contractor models) to gain system access.
- Deliberate introduction of backdoors, data exfiltration capabilities, or access to internal systems under the cover of legitimate development or IT support work.
- For private investor platforms, trading technology firms, and cryptoasset businesses specifically: DPRK actors are seeking to steal funds through illicit means, this is an active, confirmed threat category for UK-based crypto and fintech firms.

Prioritised recommendations — Q1 2026

The following recommendations are prioritised by threat relevance to the UK financial services and private investor risk profile this month. They are structured around **CloudGuard's 3Rs framework**: Enhanced Readiness, Optimised Responsiveness and Maximised Resilience.

Immediate — Enhanced Readiness — address active threat vectors

- **Deploy dark web credential monitoring** across all firm domains and executive email addresses. Given the 2 billion+ leaked credentials active in markets, assume compromise until monitoring confirms otherwise. Rotate any credentials identified as exposed immediately.
- **Audit and restrict** all third-party vendor remote access. Every vendor with system access should be using MFA, time-limited sessions, and monitored connections. Unmonitored vendor access is the primary attack vector used by Scattered Spider and DragonForce affiliates.
- **Test DDoS resilience** and mitigation coverage ahead of expected NoName057(16) campaign escalation. Confirm ISP and hosting provider mitigation is active and test failover to backup systems.
- **Review all freelance and contractor IT staff,** specifically those working remotely on development, infrastructure, or back-office systems, against NCSC guidance on DPRK insider threat indicators.

Urgent (7 days) — Optimised Responsiveness — strengthen detection and response

- Implement **Microsoft Sentinel alerts** specifically tuned to financial services attack patterns: infostealer C2 communications, session token theft, lateral movement from third-party VPN connections, and anomalous trading or banking system access.
- **Configure MFA fatigue** (push-bombing) detection and automatic blocking in Entra ID. MFA bypass is the primary initial access technique used by Scattered Spider and BlackBasta affiliates targeting financial firms.
- Establish an **out-of-band executive communication channel** for high-value financial authorisation. Deepfake CEO impersonation targeting fund transfers requires a verbal or out-of-band verification step that cannot be bypassed through email or messaging platform compromise.
- Validate **FCA and ICO incident reporting procedures** are documented and tested. The 72-hour ICO notification window and FCA SUP 15 reporting requirements are not met by firms that have not rehearsed the process. A cyber incident is the wrong time to discover the reporting workflow.

Short term (30 days) — Maximised Resilience — operational and regulatory posture

- Commission a FCA operational resilience self-assessment against the March 2025 requirements. In 2026, FCA supervisory attention shifts from implementation to testing and evidence. Firms that cannot produce documented impact tolerance testing, important business service mapping, and scenario testing records face enforcement exposure.
- Conduct a third-party supply chain cyber risk review. Verizon's 2025 DBIR reported third-party involvement in breaches doubled to 30%. Map all vendors with data access or system connectivity and confirm they operate appropriate cyber controls — including their own incident notification obligations to your firm.
- Implement immutable backup architecture for core financial data and client records. Ransomware groups are specifically targeting backup systems. Immutable, air-gapped or cloud-isolated backups are the primary technical control preventing catastrophic data loss from ransomware.
- Engage CloudGuard external exposure assessment or Red Teaming event. Many of the attack vectors active this month, exposed services, session vulnerabilities, email security misconfigurations, are **identifiable from outside your perimeter**. An external scan establishes your current attack surface before attackers exploit it.

Talk to CloudGuard — Security Done Different

The threats in this report are not theoretical. They are active, documented, and targeting firms like yours right now.

CloudGuard's MXDR Intelligence Unit monitors these threat groups, credential markets, and attack patterns continuously, so your firm doesn't have to. We translate raw intelligence into protective action: tuned detections, closed exposures, rehearsed responses, and the regulatory evidence trail that demonstrates your firm takes security seriously.

Threat Intelligence Briefing

Book a 30-minute threat intelligence briefing with a CloudGuard analyst. We will walk through the findings most relevant to your firm's specific risk profile — sector, size, technology stack, and regulatory exposure.

External Exposure Scan

Receive a free **External Analysis Assessment** report for your domain. See what attackers see when they look at your firm from the outside, before they use it against you. No agents. No disruption. Results within 24 hours.

Managed MXDR Service

CloudGuard's **managed detection and response service** provides 24/7 monitoring, expert-led incident response, continuous threat intelligence, and the documented evidence trail required by the FCA, ICO, and cyber insurers.

Contact CloudGuard today

hello@cloudguard.ai | cloudguard.ai | Security Done Different

Manchester & Belfast SOCs | UK-based MXDR specialists | Microsoft security partner

Intelligence sources and disclaimer

This report draws on intelligence from the NCSC (Annual Review 2025, January 2026 alert), FCA incident data (May 2025 FOI release), ENISA threat landscape reports, Verizon DBIR 2025, IBM Cost of a Data Breach 2025, Sophos State of Ransomware 2025, Recorded Future threat intelligence, dark web monitoring sources, CloudGuard AI Threat Intelligence, CloudGuard Dark Web marketplace monitoring and publicly disclosed incident reports. Intelligence is accurate as of the report date of 15 March 2026. The threat landscape changes rapidly — threat actor capabilities and targeting may have evolved since compilation. This report does not constitute legal or compliance advice. CloudGuard recommends engaging qualified legal and regulatory advisors for specific compliance obligations.