elytra security

Shielding your digital world with Integrity

ETR³ 2025

Elytra Threat, Risk & Resilience Report

Published by Elytra Security Private Limited | CC BY-SA 4.0
elytrasecurity.com | info@elytrasecurity.com

2025

Introduction

Purpose

ETR3 is Elytra's annual, evidence-based assessment of the global cyber, privacy, and AI risk landscape. It synthesizes what was *actually observed in 2025* and provides a pragmatic outlook for 2026. The report is written for boards, executive teams, and operational leaders. Every technical section concludes with a short, plain-language summary labelled ***What does this mean for leaders.***

How to read this report

- Sections **I–III**: What 2025's credible reports and verified incidents really showed.
- Sections **IV–VI**: AI acceleration, privacy/governance, sector and geography outlook, expanded with design guidance.
- Sections **VII–VIII**: Predictions and operating playbooks that close the "minutes vs weeks" gap.
- **Appendix & References** are listed after the main content.

Glossary

- **3-2-1-1-0 backups**: A resilience pattern — three copies of data, on two different media, one stored offsite, one copy immutable or offline, with zero errors during restore testing.
- **Artificial Intelligence (AI) governance**: Processes that control how AI systems are selected, trained, integrated, and monitored (e.g., ISO/IEC 42001 and obligations under the European Union Artificial Intelligence Act).
- **Breakout time**: The elapsed time between an initial compromise and the first successful lateral movement inside the environment.
- **Change control**: The approvals, testing, and documentation required before making changes to production systems, identities, or network rules.
- **Cloud Access Security Broker (CASB)**: A control point that enforces enterprise policies on data moving between users and cloud services.
- **Conditional Access (Microsoft Entra ID)**: Policy engine that gates sign-in and resource access based on device compliance, user risk, and other conditions.
- **Context-Aware Access (Google Workspace/Cloud)**: Access controls that consider device posture, user identity, location, and other attributes before granting application access.
- **Data breach cost (IBM study)**: The benchmark global average total cost associated with a data breach event (planning, detection, escalation, notification, lost business, and post-breach response).
- **Data Protection Impact Assessment (DPIA)**: A structured assessment of risks to individuals' personal data and the safeguards applied, required under several privacy regimes.
- **Defense-in-depth**: Layering of controls (identity, endpoint, network, application, data, and recovery) so that failure in one layer does not cause catastrophic loss.
- **Endpoint isolation**: Automatic containment of a device (network and app access restricted) when risk exceeds a defined threshold until it is remediated.

- **European Union Artificial Intelligence Act (EU AI Act)**: Regulation establishing obligations for AI systems, including prohibitions, transparency, and controls for high-risk and general-purpose AI.
- **General-purpose AI (GPAI)**: Broad-capability AI systems used across tasks (e.g., large language models) as referenced by the EU AI Act.
- **Help desk hardening**: Scripts, controls, and approvals that prevent social engineering of support staff (e.g., verified callbacks, dual control for resets).
- **Human Risk Management**: Continuous measurement and improvement of human behaviors that create or reduce risk (reporting suspicious activity, safe data handling, AI use, change discipline).
- **Information Technology (IT)**: Compute, identity, network, and application systems that support business operations.
- **Known Exploited Vulnerabilities (CISA KEV)**: The U.S. Cybersecurity and Infrastructure Security Agency's catalogue of vulnerabilities that are known to be exploited in the wild.
- **Large Language Model (LLM)**: A machine-learning model trained on large corpora of text (and increasingly other modalities) to generate content and assist tasks.
- **Mean/Median Time To Remediate (MTTR)**: The average/median elapsed time to fix vulnerabilities or security defects after discovery.
- **OAuth 2.0 (Open Authorization)**: An industry standard for delegated authorization. In practice, "OAuth tokens" grant applications scoped access to data or APIs without sharing a user password.
- **Operational Technology (OT)**: Industrial control systems and related technology used in manufacturing, utilities, and critical infrastructure.
- **Patch-or-Isolate**: A policy where devices and services that miss critical patch service-level objectives automatically lose access to sensitive systems until compliant.
- **Phish-resistant multi-factor authentication (MFA)**: Authentication resistant to credential-phishing and replay (e.g., FIDO2/WebAuthn security keys).
- **Record of Processing (privacy)**: A register of how personal data is processed across systems, including purpose, legal basis, transfers, and retention.
- **Systematic Automated Recon (SAR)**: Attacker-style, continuous reconnaissance of an organization's external and SaaS footprint (domains, storage, integrations, tokens, keys) to preempt exploitation.
- **Token cascade**: A chain of access in which one compromised OAuth token or integration unlocks extensive downstream data and services.
- **Verizon Data Breach Investigations Report (DBIR)**: An annual analysis of breach and incident patterns across industries and geographies.

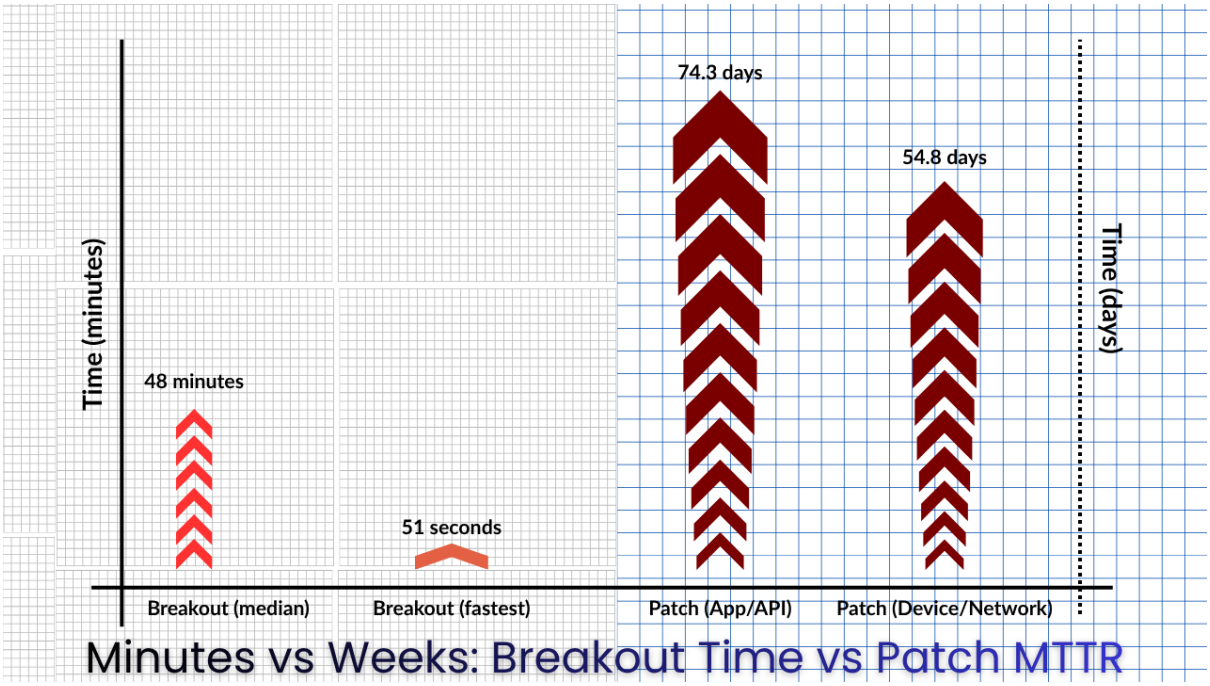
Note on writing style: Throughout this document, acronyms are expanded at their first mention in each major section.

Part I: What 2025's credible reporting said

Cost, speed, and the asymmetry that decides outcomes

- The **IBM Cost of a Data Breach 2025** benchmark places the global average total cost near **USD 4.4 million** per breach event. The **Verizon Data Breach Investigations Report (DBIR) 2025** does not publish a comparable single "average cost" figure; its value is in patterns and incident categories rather than a dollar benchmark. Read these sources together: *patterns explain how we lose; the benchmark reminds us how much we lose when we do*.
- The **CrowdStrike Global Threat Report 2025** places median **breakout time** at roughly **48 minutes**. Meanwhile, measured **time to remediate** critical internet-facing vulnerabilities is typically many days. The result is not that "the month wins." The month *loses*. **Attackers win** when defenders operate on weekly cadences against minute-scale threats.

What does this mean for leaders: Plan, resource, and measure around *minutes*, not *months*. If a device or application falls behind on critical patches, it must automatically lose access until it is fixed.



Initial access is industrialized

- Public advisories for edge software, network gear, and remote access tools are converted into exploitation within hours or days. The **Known Exploited Vulnerabilities (CISA KEV)** catalogue is a running ledger of realities that cannot be deferred to a backlog.

What does this mean for leaders: Treat every new high-severity advisory on internet-facing technology as a production event.

Ransomware, extortion, and the human element

- Ransomware and multi-stage extortion dominated incident impact. The enabling steps remain human: rushed exemptions, reused credentials, broad OAuth scopes, and support workflows that can be social-engineered.

What does this mean for leaders: Your program is ***only*** as strong as its **human risk** habits: approvals, simulations, and incentives that make the right action easy and the wrong action difficult.

Part II: 2025 incidents to learn from verified events

Scope note: This section attributes events conservatively and avoids speculation. We use incidents as *representative case studies* that shape 2026 readiness.

1. **Salesforce ecosystem — OAuth token abuse via third-party connectors (e.g., Drift/Salesloft)**
   In late-2025, adversaries used compromised **OAuth 2.0** tokens to exfiltrate Customer Relationship Management data at scale. The lesson is durable: **integration scopes** and **token governance** are now first-class controls.

One high-scope OAuth token can act as signed hall pass across multiple systems

2. **Marks & Spencer (United Kingdom)**
   In April 2025, a cyber incident led to suspension of online orders and disruption to customer-facing services. This is **not** the Salesforce OAuth campaign; it stands on its own as a reminder that retail and logistics dependencies convert third-party issues into first-party pain.

3. **Jaguar Land Rover (United Kingdom)**
   In September 2025, a cyberattack disrupted operations and logistics. Modern manufacturing and automotive environments are **Operational Technology (OT)** dependent on **Information Technology (IT)** identity and upstream services; when IT falters, shop-floor impact follows.

4. **Healthcare at national scale**
   In 2025, the Change Healthcare breach illustrated how one identity failure on a remote system and weaknesses in segmentation can cascade across a nation's **electronic data interchange** and claims rails, affecting patient care and revenue cycles.

5. **Backup hygiene and cloud object storage (EY case)**
   Reports described exposure of multiple terabytes of data, including database backups, in a cloud storage environment. **The number of accesses prior to takedown is indeterminate** from public sources. The risk lesson is clear: backups and data lakes are **crown-jewel systems** and require isolation, immutability where appropriate, and routine restore testing.

What does this mean for leaders: Tokens, vendors, and backups concentrate risk. Inventory them, restrict them, and rehearse your response.

Part III: The Human Core (cause, not footnote)

Shadow AI and "free" endpoints
Staff used public or trial AI tools to accelerate work, often pasting contracts, code, and personal data into prompts. Few organizations maintained an approved-provider list, an **AI use standard**, or a technical gateway to enforce it. This created an unlogged, cross-border data egress path.

Help desk workflows under pressure
Attackers exploit urgency to obtain password resets, factor resets, and temporary bypasses. **Help desk hardening** requires verified callbacks, dual control for sensitive roles, and scripts that make "no" the default absent strong verification.

Culture, simulations, and near-miss reporting
Annual training does not change behavior. Weekly, department-specific micro-simulations do — short exercises tied to coaching and safe reporting. Reward near-misses to surface issues before they become incidents.

Separation of duties and privilege drift
Standing privileges accumulate. Emergency accounts linger. Cloud permissions drift without automated attestation and pruning. These conditions convert small mistakes into material breaches.

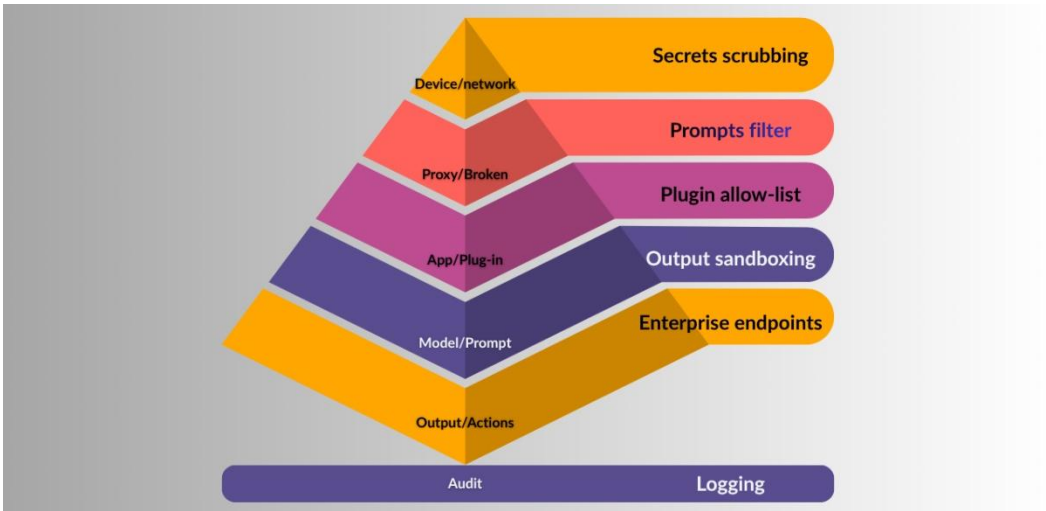
What does this mean for leaders: Technology fails last. People fail first. Make guardrails visible, practice often, and measure behaviors you want more of.

Part IV: AI acceleration, model abuse, and SAR at scale

Proof-of-concept capability: "RedGotham.exe"
A Windows sample posted to a public sandbox (labelled "RedGotham.exe," 2 November 2025) exhibited modern loader behavior: use of **PowerShell** and **Windows Management Instrumentation**, attempts to tamper with Microsoft Defender settings, persistence via scheduled tasks and services, and low early anti-virus consensus. We treat this as a **feasibility signal**, not as evidence of widespread in-the-wild deployment. The risk is **speed of iteration** when model output is combined with operator craft.

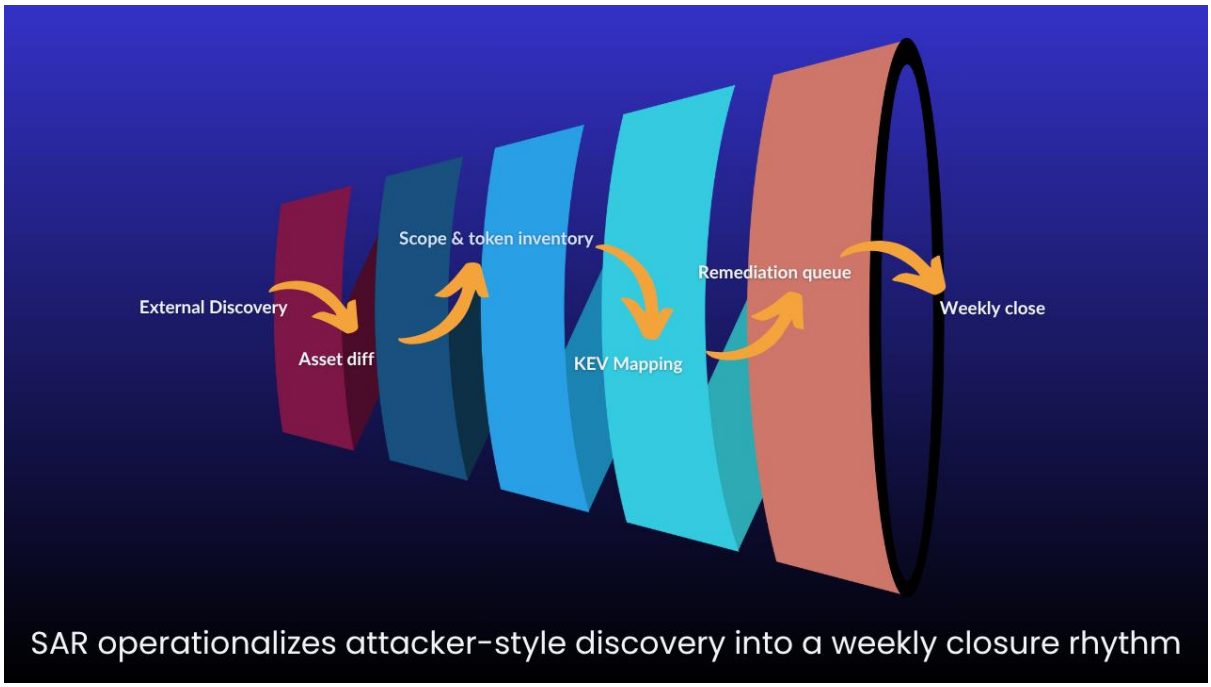
AI-scaled social engineering and reconnaissance
Well-formed phishing lures and mass reconnaissance are now routinely generated or assisted by **Large Language Models (LLMs)**. That raises click-through rates and compresses time from targeting to exploitation.

Govern AI like production systems
Adopt **ISO/IEC 42001** practices (inventory, risk controls, testing, audit) and align roadmaps with **EU AI Act** timelines. Route prompts through an **AI egress broker** that blocks secrets and protected data classes. For highly sensitive use cases, use enterprise AI endpoints and log prompts and outputs.



Control stack for AI use—from device posture to prompt and output governance.

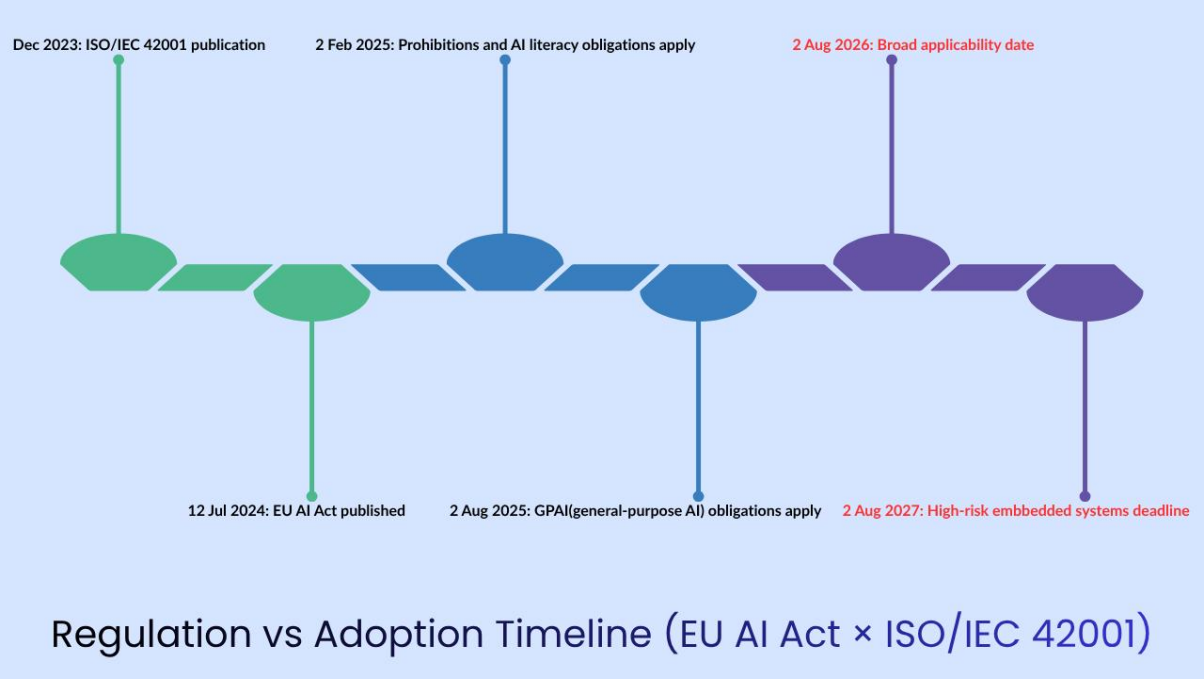
SAR — Systematic Automated Recon
Run attacker-style, **continuous** recon on your own estate: domains and subdomains, exposed services, cloud storage, code repositories, SaaS connectors, **OAuth 2.0** scopes, and leaked keys. Prioritize by **Known Exploited Vulnerabilities (CISA KEV)** and blast radius. Close findings weekly.



What does this mean for leaders: Assume attackers have tireless interns — they are called models. Let people use AI, on **your** terms. **Find the issues yourself before they do.**

Part V: Privacy/Governance: rules exist; avoidance persists

Enforcement signals in 2025
Regulators in Europe, China, South Korea, and India showed increased tempo and scale in enforcement and rulemaking. Cases against high-profile brands emphasized unlawful cross-border transfers, weak consent, and outdated systems.

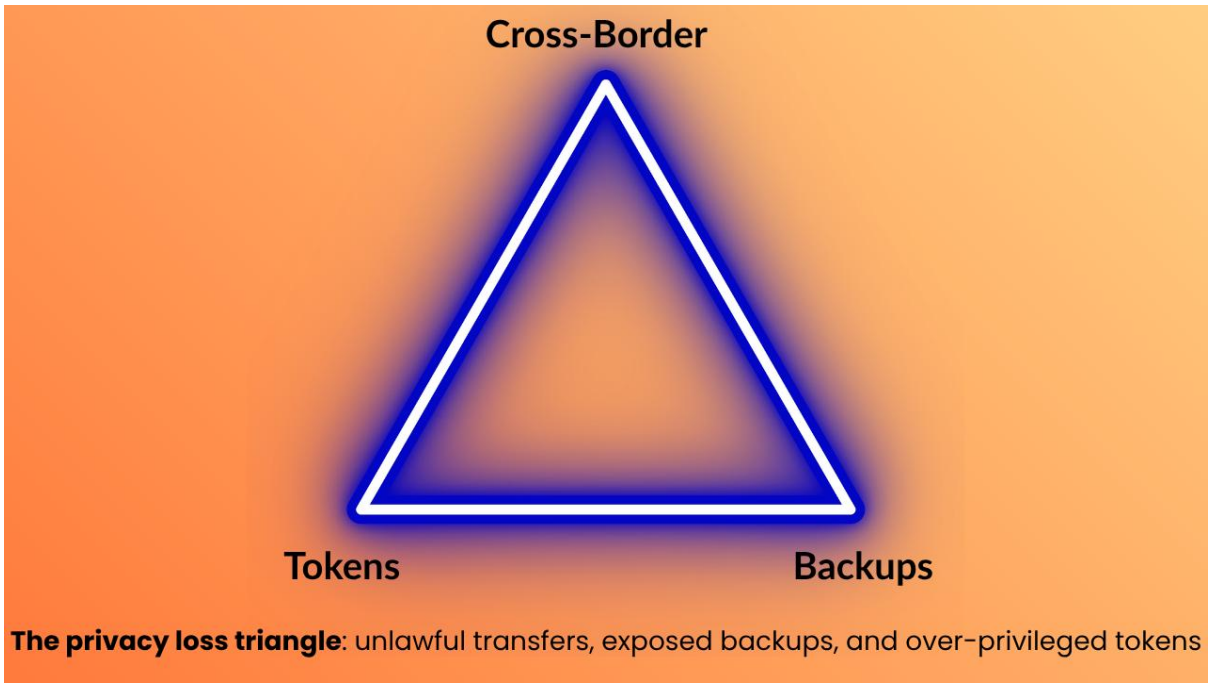


Regulation vs Adoption Timeline (EU AI Act × ISO/IEC 42001)

The three failure patterns

1. **Cross-border before controls**: Transfers conducted prior to legal and technical safeguards (standard contractual clauses, security assessments, minimization).
2. **Backups and object stores**: Public or weakly permissioned storage, including backups and logs, amplified blast radius.
3. **Opaque tracking patterns**: Consent that fails legal standards or retention that exceeds declared purposes.

Security and privacy are one agenda
Security incidents become privacy incidents the moment personal data moves. Programs must therefore map **systems of record and backups**, enforce **3-2-1-1-0**, keep a live **Record of Processing**, and include **OAuth 2.0** application scopes inside privacy reviews and **Data Protection Impact Assessments**.



What does this mean for leaders: Treat privacy like uptime. The board should see cross-border status, backup isolation measures, token inventories, and **Data Protection Impact Assessment** coverage.

Part VI: Sector and geography outlook for 2026

Banking, Financial Services, and Insurance (BFSI)
High monetization and dense vendor ecosystems keep BFSI exposed. Expect **OAuth 2.0**-based data theft (Customer Relationship Management, marketing stacks), improved social engineering of finance workflows, and faster fraud loops.
90-day plays: Gate access by device compliance; monthly token and scope reviews in core SaaS; require publisher-verified applications; test stop-payment and fraud response with banking partners.

Healthcare
Payment rails and clearinghouses are single points of national-scale failure. A single credential or remote access weakness can ripple across claims, billing, and care delivery.
90-day plays: Alternative rails for billing; segmentation of clinical and claims networks; phish-resistant multi-factor authentication for sensitive roles; joint tabletops with critical service providers.

Manufacturing and Automotive
Operational disruption follows IT identity failures, as seen in 2025 incidents.
90-day plays: Exercise "identity failure to shop-floor impact"; ensure degraded-mode procedures; enforce just-in-time remote access for maintenance vendors with session recording.

Retail, Luxury, and Cosmetics
Customer loyalty and marketing systems combine high-value personal data with cross-border processing, inviting both criminals and regulators.
90-day plays: Inventory all integrations into Customer Relationship Management and loyalty platforms; minimize scopes; revoke stale tokens; run **Data Protection Impact Assessments** for cross-border data flows.

Geographies
Expect sustained targeting across the United States, United Kingdom, European Union, and India, with state-aligned and financially motivated actors active. Focus where regulators and value concentrate.

What does this mean for leaders: Do not spread effort evenly. Put disproportionate attention where risk and regulators are densest: identity, tokens, backups, and cross-border flows.

Sector	Patch-or-Isolate	OAuth Hardening	Backup Hygiene	AI Governance	Vendor Controls
BFSI	High	High	High	High	High
Healthcare	High	Medium	High	Medium	High
Manufacturing/Auto	High	Medium	Medium	Medium	High
Retail/Luxury/Cosmetics	Medium	High	Medium	Medium	High

Sector Heat Map (Threat Drivers × Controls)

Part VII: Predictions for 2026

1. **OAuth 2.0 and SaaS-to-SaaS abuse becomes a top-three initial access path**. Expect at least one token-cascade event at “Salesforce scale,” even if the target stack differs.
2. **AI-assisted phishing, reconnaissance, and loader iteration materially raise breach likelihood** in the early hours post-release.
3. **Edge technology and remote access remain soft underbellies** without automation and isolation; opportunistic exploitation will continue to outpace change boards.
4. **Backups become primary extortion targets**. Expect more cases where the root cause is a misconfigured backup or log bucket rather than a classic intrusion.
5. **Healthcare and BFSI stay in the crosshairs** due to concentrated value and vendor sprawl.
6. **Privacy penalties rise, deterrence still lags harm**. Cross-border and dark-pattern cases continue; early **European Union Artificial Intelligence Act** obligations begin to bite.
7. **Shadow AI becomes a board-level risk item**. Expect at least one regulatory case citing AI access-control failures or ungoverned data handling.

What does this mean for leaders: Expect attacks that look less like a forced entry and more like someone arriving with your keys and a moving truck.

Part VIII — Strategy that closes the gap (Playbooks)

A. Patch-or-Isolate by default

- **Policy**: Devices and services that miss critical patch service-level objectives automatically lose access to sensitive systems until compliant.
- **Microsoft**: Use **Conditional Access** "require device to be marked compliant," deployment rings, and expedited quality updates; enable automatic isolation in **Microsoft Defender for Endpoint** when correlated high-confidence signals fire.
- **Google**: Use **Context-Aware Access** to restrict application access to compliant devices and approved networks; route access through BeyondCorp-style gateways.
- **Measurement**: Median and 90th-percentile time to isolate; percentage of assets compliant; exception volume and age.

What does this mean for leaders: If it is risky, it does not log in. If that breaks a process, fix the process.

B. Harden OAuth 2.0 and connected applications

- Centralize connected-app approval in Customer Relationship Management and service platforms.
- Minimize scopes, rotate tokens on schedule, require publisher-verified applications, and alert on new high-privilege grants.
- Maintain a rehearsed "OAuth kill switch" runbook for Customer Relationship Management and email platforms.

C. Govern AI like any other production system

- Adopt **ISO/IEC 42001** patterns for inventory, controls, red-teaming, and audits.
- Publish a one-page **AI Use Standard**.
- Route prompts through an **AI egress broker** that blocks secrets and protected data classes.
- For sensitive workflows, use enterprise AI endpoints; log prompts and outputs.

D. Backup hygiene that survives contact

- Enforce **3-2-1-1-0**; isolate backup networks; require private endpoints and deny public access at the organization policy level.
- Use immutable or offline tiers for critical data; perform monthly canary restores and quarterly full restores with evidence.
- Manage backup credentials in a privileged-access vault with just-in-time elevation.

E. Identity, segmentation, and the "48-minute defense"

- Enforce phish-resistant multi-factor authentication for administrators and finance; remove standing administrative rights; micro-segment critical paths.
- Tune endpoint detection and response to auto-contain on multi-signal correlations (e.g., Defender configuration change + scheduled task + service creation).

F. Human Risk Management that changes behavior

- Replace annual classes with weekly micro-simulations tailored by role (e.g., “safe AI prompting” for sales; “OAuth scope review” for Customer Relationship Management owners).
- Reward near-miss reporting; run blameless reviews focused on system fixes.

G. Supplier and data-sharing discipline

- Inventory and minimize data exchanged with third parties; include **connected applications** and **OAuth 2.0** scopes in **Data Protection Impact Assessments**.
- Scan code repositories for keys; break builds on secret discovery; rotate credentials automatically.

Table 2 (design): *Board-Level KPI Pack* — Patch MTTR by severity; percentage of access gated by device compliance; time-to-isolate; high-risk OAuth grants; blocked AI prompts with sensitive content; restore success rate; vendor risk deltas; **Data Protection Impact Assessment** coverage.

Executive Scorecard Mockup (Board KPIs)

Appendix A: 2025 Breaches and CVEs (Jan–Oct)

Scope: Disclosure or confirmation during 2025 Jan–Oct. CVE list restricted to CVSS 9+ and widely exploited items. Supply-chain OAuth abuse entries included though not CVE-driven. ATT&CK and DEFEND are indicative mappings.

Confirmed breaches and incidents

Month	Organization	Sector and Geo	Summary	ATT&CK examples	DEFEND notes
Jan–Feb	SimonMed Imaging	Healthcare US	Intrusion and exfiltration with later notifications approximately 1.27M impacted	T1486 Data encrypted T1041 Exfiltration	Backups immutability IR drillbooks data loss prevention
Jan–Feb	Episource	Health SaaS US	Intrusion and data theft approximately 5.4M affected	T1190 Exploit public app T1041 Exfiltration	Network segmentation web app hardening log review
Apr–May	LexisNexis Risk Solutions	Data broker US	Repo or developer exposure approximately 364k affected	T1552 Unsecured creds T1530 Cloud data from storage	Secrets scanning rotation scoped tokens
May	Dior	Luxury retail FR CN	Customer database access confirmed payment not indicated	T1190 T1078 Valid accounts	Access governance least privilege vendor oversight
Jun	Louis Vuitton HK KR multi	Luxury retail APAC	HK disclosure approximately 419k affected related APAC notices	T1190 T1078	Geo segmentation regulator reporting playbook
Jun disc Sep	Kering Gucci Balenciaga McQueen	Luxury retail EU global	Customer PII theft media reports cite millions	T1190 T1041	Egress monitoring and anomaly detection
Jul	Allianz Life	Insurance US	Third party cloud CRM accessed majority of 1.4M customers	T1566 Phishing T1078 Valid accounts T1530 Cloud data	Token scope hygiene phishing resistant MFA vendor controls
Aug–Sep	Salesforce Drift Salesloft OAuth campaign Cloudflare Zscaler HackerOne Proofpoint PagerDuty Tanium others	Multi sector global	OAuth tokens for connected app abused to export Salesforce tenant data	T1528 Steal app access token T1078 T1567 Exfil over web	App allow lists token revocation short TTL audit of connected apps
Sep	Panama Ministry of Economy and Finance	Government finance PA	INC ransomware exfil claim greater than 1.5 TB	T1486 T1041	Network isolation offline backups tabletop exercises
Sep	Harrods	Retail UK	Third party provider breach basic identifiers only	T1195 Supply chain	Vendor due diligence breach notification plan

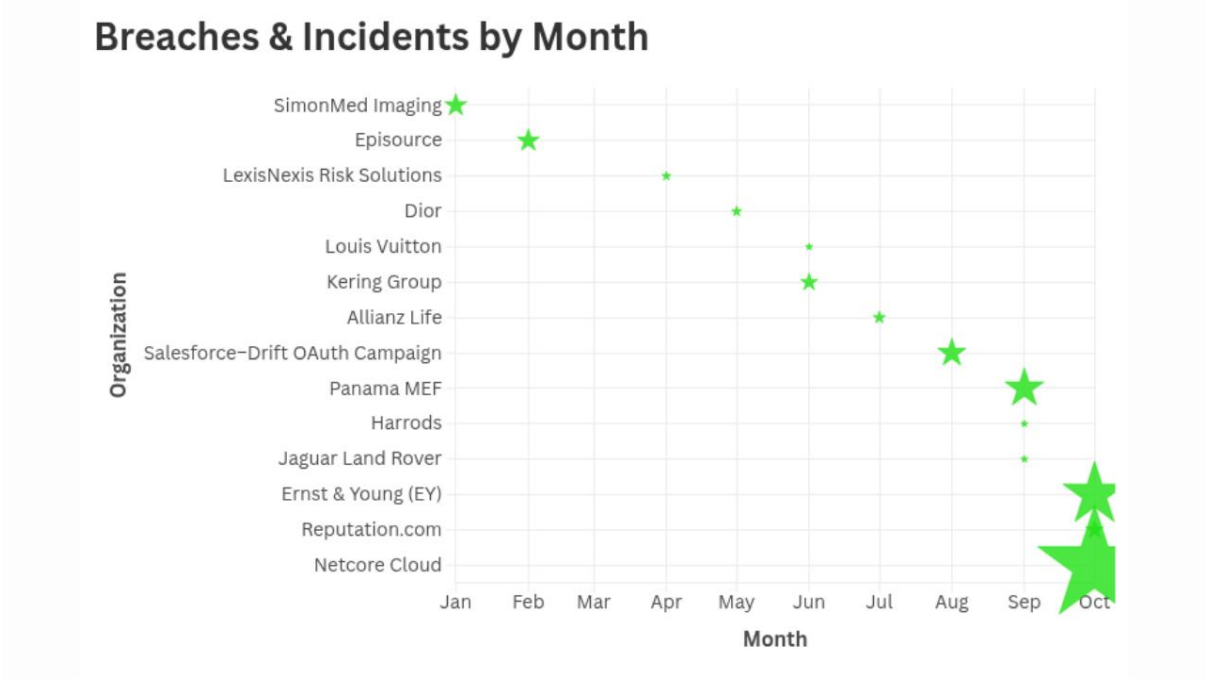
Month	Organization	Sector and Geo	Summary	ATT&CK examples	DEFEND notes
Sep–Oct	Jaguar Land Rover	Automotive UK	Enterprise compromise and production disruption some data affected	T1489 Service stop T1490 Inhibit recovery	OT IT segmentation operational continuity plans
Oct	Ernst and Young EY	Professional services global	Approx 4 TB SQL Server backup publicly exposed on cloud	T1552 Credentials in backups	Secret vaulting backup access control cloud posture
Oct	Reputation dot com	SaaS US	Approx 120M log records approximately 320 GB exposed session cookies at risk	T1552 then T1078	Session cookie protections log minimization secrets in logs
Oct	Netcore Cloud	Email MarTech IN	Misconfigured database exposure approximately 13 TB approximately 40B records	T1530 Cloud data T1552	Data minimization public exposure checks CSPM

Major CVEs CVSS 9 plus and widely exploited

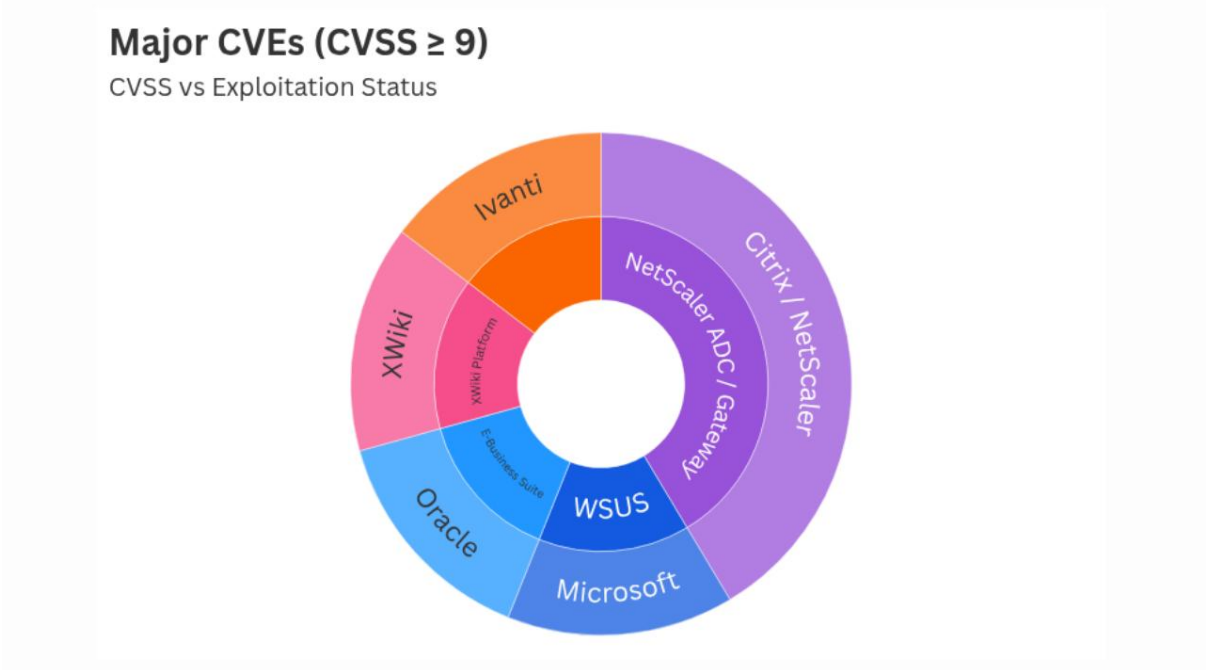
CVE	Product and component	CVSS	Exploited in the wild	ATT&CK tie in	One liner and mitigation cue
CVE-2025-59287	Microsoft WSUS	9.8	Yes KEV	T1190 Exploit public app T1068 Priv esc follow on	Unauth RCE via deserialization apply OOB patch isolate WSUS restrict 8530 8531
CVE-2025-61882	Oracle E Business Suite	9.8	Yes highly exploited	T1190 T1567 Exfil over web	Unauth RCE emergency Oracle patch mass extortion activity harden EBS internet exposure review
CVE-2025-5777	NetScaler ADC Gateway	9.3	Yes	T1190 T1550 Use stolen tokens	Pre auth info leak and session hijack urgent upgrade rotate sessions
CVE-2025-6543	NetScaler ADC Gateway	9.2	Observed exploits	T1190	Memory overflow leading control flow or DoS update firmware monitor exploitation
CVE-2025-7775	NetScaler ADC Gateway	9.2	Yes	T1190	Pre auth overflow RCE DoS especially IPv6 configs patch immediately
CVE-2025-24893	XWiki Platform	9.x	Yes	T1190 T1059 Command execution	Unauth RCE via template injection live abuse remove exposure and patch enable WAF rules

Timelines

Breach and incident timeline Jan to Oct 2025



Major CVEs Jan to Oct 2025



2025 Incidents × Geography Matrix (Jan–Oct)

Region / Sub-Region	Country (HQ or impact)	Notable 2025 Incidents	Sectors Involved	Estimated Records / Impact Scope	Commentary / Themes
North America	US United States	Allianz Life • LexisNexis Risk Solutions • SimonMed Imaging • Episource • Reputation.com • EY (global ops) • Salesforce tenants (Cloudflare, Tanium, PagerDuty, HackerOne, Proofpoint)	Insurance Healthcare Data Brokerage Professional Services SaaS Technology	≈ 9–10 M+ individuals (aggregate)	Dominant vector = cloud misconfig / 3rd-party / OAuth token abuse; high regulatory attention (FTC HIPAA SOX).
Latin America / Caribbean	PA Panama	Ministry of Economy & Finance (MEF)	Government / Finance	> 1.5 TB data exfil claimed	Ransomware and data extortion growing across LATAM; limited public forensics.
Europe	FR France	Kering (Gucci etc.) • Dior • LVMH group linkages	Luxury Retail / Cosmetics	Millions customers	Targeted brand breaches highlight supply-chain and marketing platform exposure.
	GB United Kingdom	Harrods • Jaguar Land Rover • EY (global ops UK region)	Retail • Automotive • Professional Services	Operational impact > data volume	OT/IT blend attacks emerging (industrial impact beyond data loss).
	EU Cross-EU	Salesforce OAuth campaign affecting multi-tenant EU customers	SaaS / Cloud	Varies	Pan-EU supply-chain campaign shows OAuth token risk as new frontier.
Middle East & Africa	—	No confirmed public breach of major visibility Jan–Oct 2025	—	—	Region still under-reported; likely undisclosed state / oil sector incidents.
Asia-Pacific	HK Hong Kong / KR Korea	Louis Vuitton regional incidents • APAC CRM system leak	Luxury Retail • CRM SaaS	≈ 419 k (HK) + unknown (KR)	APAC regulators increasing privacy enforcement (PCPD PIPC).
	IN India	Netcore Cloud misconfigured DB (~40 B records)	Email / MarTech SaaS	40 B records (~13 TB)	Largest 2025 data exposure by volume; root cause = open Elasticsearch endpoint.
	JP / SG Regional	Minor APAC OAuth tenants hit via Salesforce Drift vector	SaaS	Limited	OAuth abuse visible but no large national impact reports.
Global / Multi-region	🌐 Multi-tenant SaaS ecosystem	Salesforce-Drift OAuth campaign (Cloudflare et al.) • Oracle EBS CVE-2025-61882 exploitation wave	SaaS / Enterprise Apps	Varies by tenant	Demonstrates interconnected risk and shared attack surface of global cloud stacks.

Observations

8. **Americas ≈ 60 %** of all confirmed disclosures by count (US dominant).
9. **Europe ≈ 25 %**, driven by luxury retail and industrial cases.
10. **APAC ≈ 10 %**, though Netcore alone drives > 80 % of records exposed globally by volume.
11. **LATAM & EMEA gov sectors** rising in ransomware impact (Panama MEF prototype).
12. **Cross-region campaigns (SaaS OAuth / Oracle EBS)** show a shift from endpoint RCE to identity and application-layer exploitation.

2025 Data Volume × Geography Matrix (Jan–Oct)

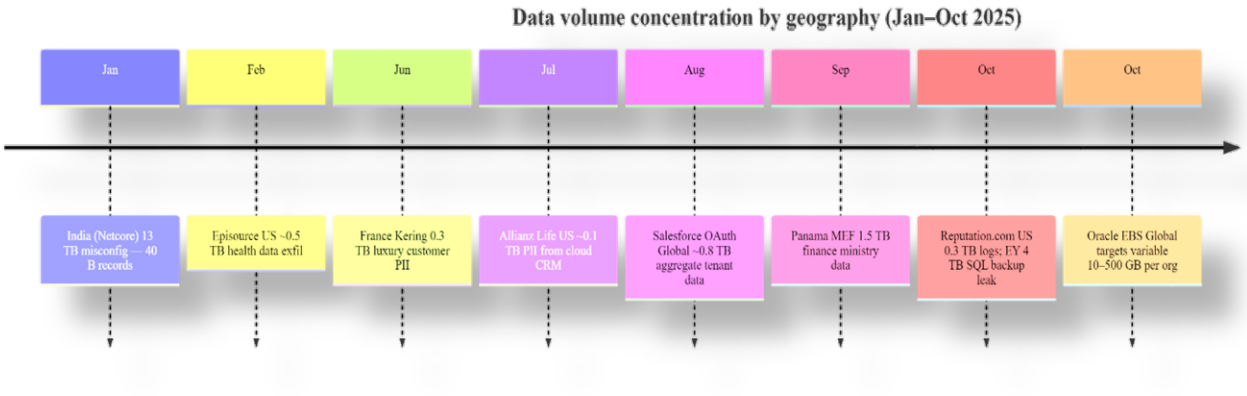
Rank	Region / Country	Representative Incidents	Estimated Volume Exposed / Exfiltrated	Volume Tier	Dominant Vector(s)	Notes / Interpretation
1	IN **India**	Netcore Cloud misconfigured DB (~13 TB ≈ 40 B records)	**13 TB (≈ 40 billion records)**	**Extreme (>10 TB)**	Misconfiguration / Open Elasticsearch	Largest known 2025 exposure by volume; marketing telemetry logs without auth.
2	PA **Panama**	Ministry of Economy & Finance (MEF) – INC ransomware	**1.5 TB (confirmed exfil)**	Very High (>1 TB)	Ransomware / Data Extortion	First LATAM ministry breach of this scale; likely target of data-leak markets.
3	🌐 **Multi-Region (SaaS OAuth Campaign)**	Salesforce ↔ Drift / Salesloft abuse (Cloudflare + others)	**0.5–1 TB aggregate tenant data**	High (0.1–1 TB)	OAuth token abuse / supply-chain	Campaign spanned EU, US & APAC; shows identity layer risk.
4	US **United States**	Allianz Life (1.4 M records) • LexisNexis (364 k) • SimonMed (1.27 M) • Episource (5.4 M) • Reputation.com (~320 GB logs) • EY (4 TB backup)	**~6 TB (aggregate data volume)**	High (1–10 TB)	Mixed vectors (3P cloud, misconfig, RCE)	60 % of breach count but moderate volume vs APAC spike.
5	GB **United Kingdom**	Harrods (undisclosed) • Jaguar Land Rover (ops impact > data)	**<0.5 TB (operational impact higher)**	Medium (50–500 GB)	Supply chain / OT IT convergence	Illustrates business continuity impact over records count.
6	FR **France / EU Luxury**	Kering (“millions” records) • Dior (customer DB)	**0.2–0.3 TB (≈ 2–3 M records)**	Medium (100–500 GB)	Phishing + WebApp Exploit + Data Exfil	High-value data targets vs volume targets.
7	HK / KR **Hong Kong / Korea (APAC)**	Louis Vuitton regional incident (~419 k HK records)	**~50 GB (≈ 400 k records)**	Low (<100 GB)	Credential reuse / CRM exploit	Regulatory oversight focus (PPCD HK).
8	🌍 **Global**	Multiple orgs	**Variable (10–**	Variable	CVE-2025-61882	Extortion wave

Rank	Region / Country	Representative Incidents	Estimated Volume Exposed / Exfiltrated	Volume Tier	Dominant Vector(s)	Notes / Interpretation
	Enterprises (Oracle EBS CVE-2025-61882)	worldwide exploited via Oracle EBS zero-day	**500 GB per org)**	(0.1–1 TB class)	unauth RCE / data exfil	not fully quantified yet; EBS core records high value.

Volume Summary by Region

Continent	Aggregate Volume Range (est.)	% of Total Global Exposed Volume	Primary Breach Type
Asia-Pacific	~13–14 TB	~65 %	Misconfiguration / Cloud Exposure
North America	~6 TB	~25 %	3rd-Party / Cloud Vendor / CRM
Europe	~1 TB	~5 %	Luxury Retail / Phishing / Credential Abuse
Latin America	~1.5 TB	~5 %	Ransomware / Data Extortion
Other Regions (EMEA/MEA)	<0.1 TB (reported)	<1 %	Minimal public disclosures

Volume map by month



Insights

- **APAC dominates by sheer bytes**, largely due to Netcore's exposure.
- **North America leads by incident count** but smaller average payloads per case.
- **Europe's luxury sector** incidents are reputationally high-impact but volumetrically modest.
- **Ransomware in LATAM** (Panama MEF) introduces TB-scale leaks to a region historically under-represented.

- **Global SaaS & Oracle EBS exploitation** blur geographic boundaries — data residency now a critical disclosure parameter.

2025 Sector × Data Volume Matrix (Jan–Oct)

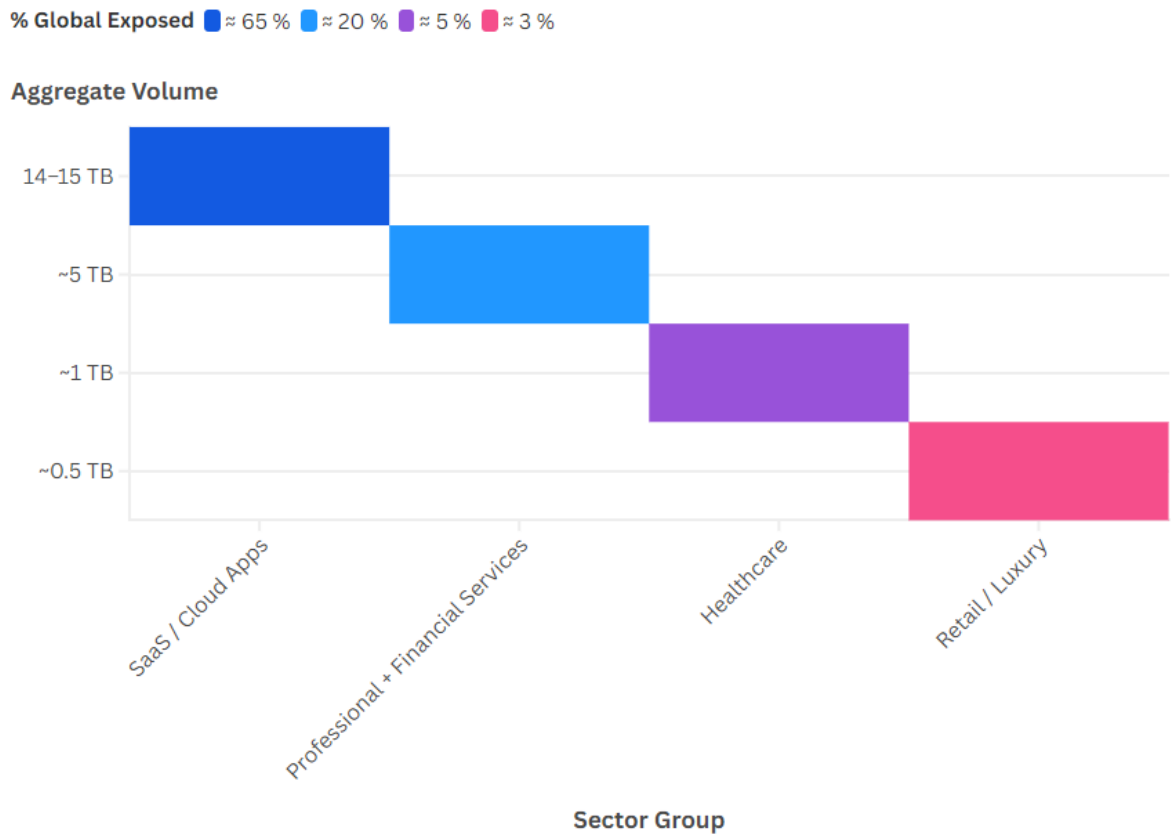
Rank	Sector	Representative 2025 Incidents	Approx. Records / Data Volume	Volume Tier	Dominant Attack Vector(s)	ATT&CK / DEFEND Focus
1	**Email / MarTech SaaS**	Netcore Cloud (IN) – 13 TB (~40 B records)	**13 TB (≈ 40 B records)**	**Extreme (>10 TB)**	Misconfiguration / Open Elasticsearch	T1530 (Cloud Data) · T1552 (Creds in Files) → M1047 (Audit Logs) · M1051 (Update Software)
2	**Government / Finance**	Panama MEF (1.5 TB)	**1.5 TB exfil**	Very High (>1 TB)	Ransomware / Data Extortion	T1486 (Data Encrypted) T1041 (Exfil) → M1040 (Encrypt Sensitive Data)
3	**Professional Services**	Ernst & Young (4 TB SQL backup exposed)	**~4 TB (≈ 200 M records)**	High (1–10 TB)	Cloud misconfiguration / Backup exposure	T1552 (Creds in Backups) → M1054 (Secure Backup)
4	**Healthcare**	SimonMed Imaging (1.27 M) · Episource (5.4 M)	**~6.7 M records (≈ 1 TB)**	High (1–10 TB)	Ransomware / Phishing	T1566 (Phish) T1078 (Valid Accounts) → M1032 (Network Segmentation)
5	**Insurance / Financial Services**	Allianz Life (1.4 M records)	**~0.15 TB (≈ 1.4 M)**	Medium (100 GB–1 TB)	Third-party CRM Compromise	T1566 (SE) T1530 (Cloud Data) → M1038 (Application Isolation)
6	**Luxury Retail / Cosmetics**	Kering · Dior · Louis Vuitton · Harrods	**≈ 0.5 TB (≈ 5 M records)**	Medium (100–500 GB)	WebApp Exploit / Credential Reuse	T1190 (Exploit App) T1078 (Valid Accounts) → M1041 (Encrypt PII)
7	**Automotive / Industrial OT**	Jaguar Land Rover (ops shutdown)	**Ops impact; data < 0.1 TB**	Low (< 100 GB)	OT/IT compromise / Service Stop	T1489 (Service Stop) T1490 (Inhibit Recovery) → M1053 (Data Backup)
8	**Technology / SaaS Ecosystem**	Salesforce ↔ Drift OAuth Campaign (global)	**0.5–1 TB aggregate**	Medium (100 GB–1 TB)	OAuth token abuse / supply-chain	T1528 (Steal App Token) T1078 → M1042 (Disable Orphaned Accounts)

Aggregate Sector Totals (rounded)

Sector Group	Aggregate Volume	% Global Exposed	Typical Breach Vector
SaaS / Cloud Apps	14–15 TB	≈ 65 %	Misconfiguration / OAuth Abuse

Professional + Financial Services	~5 TB	≈ 20 %	Backup Exposure / Vendor Access
Healthcare	~1 TB	≈ 5 %	Phishing / Ransomware
Retail / Luxury	~0.5 TB	≈ 3 %	Credential Reuse / Web Exploit
Government / Public Sector	~1.5 TB	≈ 7 %	Ransomware / Extortion
Industrial / OT	< 0.1 TB	< 1 %	Service Disruption / Impact

Sector–volume

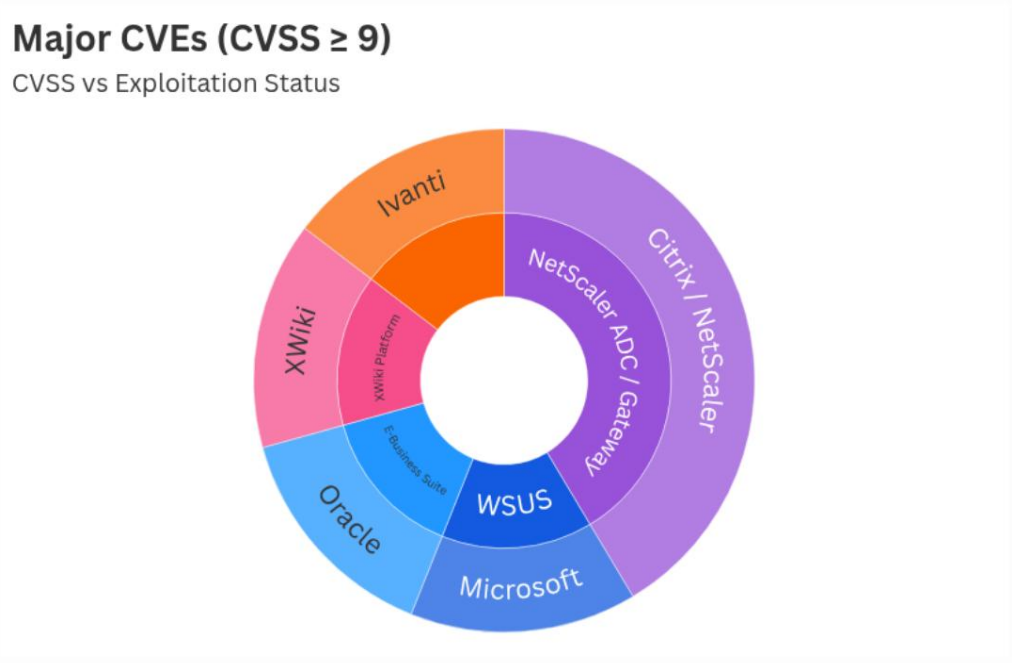


Key Interpretive Insights

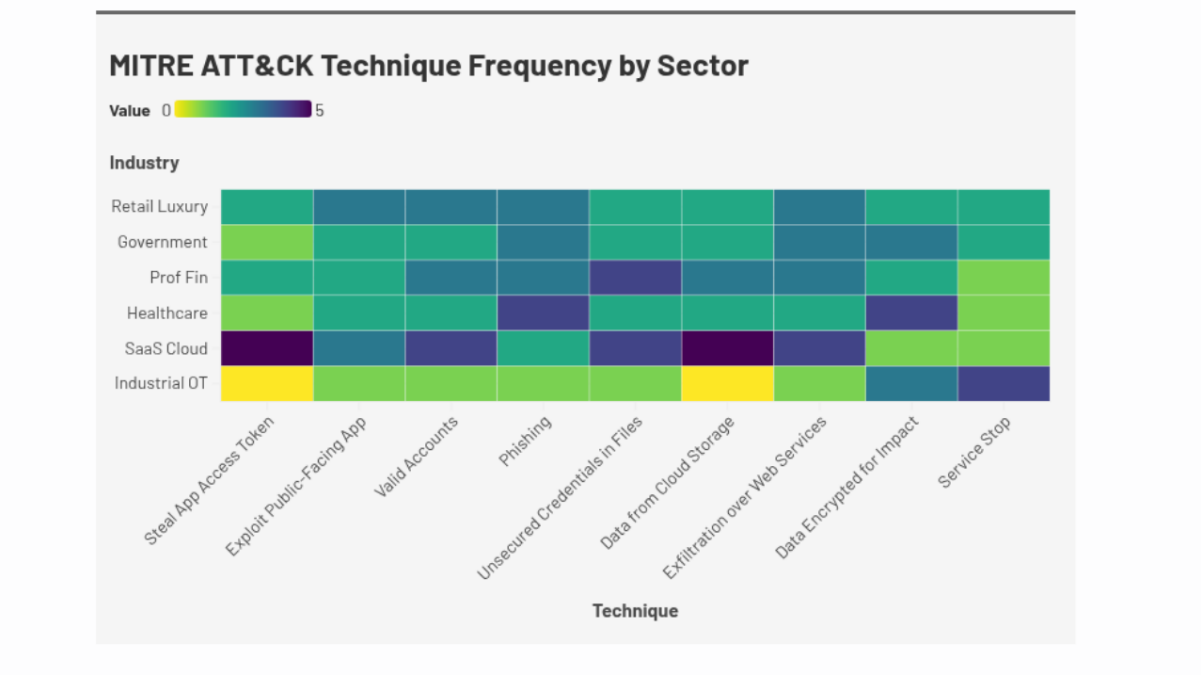
13. **Data gravity shift:** 70 % of 2025 exposed bytes reside in SaaS/Cloud services; local IT breaches declining in relative impact.
14. **Regulatory asymmetry:** APAC + India breaches massive in volume but slow in notification; EU breaches low in volume but high in transparency.
15. **Sector risk divergence:** Luxury and Professional Services show targeted precision; Healthcare and Gov show bulk data loss.
16. **Identity layer threat surface:** OAuth abuse campaign and EBS RCE prove attackers pivot toward application and credential federation points.

Data volume by region TB

Major CVEs (CVSS > 9)



Heat map — MITRE ATT&CK technique concentration by sector



Sources and Caveats

- **Attribution**: We avoid speculative attribution.
- **Marks & Spencer (United Kingdom)** is treated separately from the Salesforce OAuth abuse campaign.
- **EY exposure**: Volume reported; **number of accesses prior to takedown is indeterminate** from public sources.
- **"RedGotham.exe"**: Proof-of-concept sample analyzed in a public sandbox on 2 November 2025; cited as a capability signal, not as an in-the-wild campaign.
- **Observation cut-off**: All 2025 observations are **as of 2 November 2025 (IST)**.

References

1. **IBM** — *Cost of a Data Breach Report 2025*.
2. **Verizon** — *Data Breach Investigations Report 2025*.
3. **CrowdStrike** — *Global Threat Report 2025*.
4. **Microsoft** — *Digital Defense Report 2025*.
5. **CISA** — *Known Exploited Vulnerabilities (KEV) Catalog* and 2025 alerts.
6. **ENISA** — *Threat Landscape 2025*.
7. **Salesforce** and **Google Cloud Threat Intelligence** — 2025 advisories on OAuth token abuse against Salesforce connectors (e.g., Drift/Salesloft).
8. **Public statements and press reports** — Marks & Spencer cyber incident (April 2025); Jaguar Land Rover disruption (September 2025).
9. **United States Department of Health and Human Services breach portal** — Change Healthcare (UnitedHealth Group) impact reporting.
10. **Public reports** — EY cloud backup exposure (October 2025).
11. **European Union** — *Artificial Intelligence Act* (Official Journal publication and staged obligations).
12. **International Organization for Standardization (ISO)** — *ISO/IEC 42001:2023 — Artificial Intelligence Management System*.
13. **OWASP** — *Top 10 for Large Language Model Applications* (2024–2025 materials).

elytra security

Shielding your digital world with Integrity

About Elytra Security

Elytra Security Private Limited is a cybersecurity and compliance company helping enterprises strengthen digital resilience through its advisory & implementation services, complemented by its suite of products — Elytra Shield, Secure, Vault, SIG, and Nexus.

Our mission is to enable trust, transparency and integrity in a rapidly evolving threat landscape.

2025

github.com/venkatmangudi-elytra/elytraetr3 | elytrasecurity.com | info@elytrasecurity.com