

Companies most dependent on protecting customer secrets and sensitive data

Produced by FFP One (<https://ffp.one>), an AI research tool for professional investors, built on SEC filings. A research agent wrote this report end to end. It draws mainly on the filings and market data, marks outside sources, and ends with a table showing where its figures came from.

QUESTION What companies are particularly exposed to state actor cybersecurity threats? I.e. where their business model is highly reliant on avoiding having sensitive customer data being exposed (like API keys, crypto wallet keys, financial information, etc)

MODEL GPT-6.1 Sol (OpenAI)

GENERATED 22 October 2026

Premise verdict: confirmed—with an important distinction. Some businesses are unusually dependent on preventing sensitive-data exposure because they safeguard **assets, credentials, access rights, or valuable customer datasets**. That makes them attractive targets and creates substantial consequences if security fails. It does **not** establish that their defenses are weak or that a state-sponsored breach is likely.

For your specific examples, my priority research shortlist is:

- **Keys, credentials, and access: Coinbase (COIN), Okta (OKTA), Palo Alto Networks’ acquired CyberArk business (PANW), and GitLab (GTLB).**
- **Sensitive financial and enterprise datasets: Intuit (INTU), Equifax (EFX), and Snowflake (SNOW).**
- **Especially strong filing evidence of actual state-actor targeting: Microsoft (MSFT) and Cloudflare (NET).**

This is a business-model exposure shortlist, **not a statistical ranking of breach probability**. It focuses on covered public companies.

1. Closest matches to your criteria

Company	Sensitive asset or access dependency	Why a breach threatens the business model	State-actor evidence
Okta — OKTA	Workforce and customer identity; authentication and access to connected business systems	A compromise can affect not just information held by Okta, but systems secured through its identity platforms. Trust in the security product itself is central to customer retention.	Explicit in its latest annual filing: sophisticated nation-state actors and advanced persistent threats; Okta calls itself an attractive target because it forms part of customers’ security software supply chains. [S1]
Coinbase — COIN	Private keys controlling custodied crypto assets, customer cash, and sensitive account information	Particularly direct exposure: compromised keys can lead to irreversible asset loss. Coinbase warns that it may have to reimburse customers and that certain customer contracts do not limit security-breach liability.	The cited custody passages establish high-consequence structural exposure , rather than attribution of a particular attack to a state. [S2]

Company	Sensitive asset or access dependency	Why a breach threatens the business model	State-actor evidence
Palo Alto Networks — PANW, including CyberArk	Privileged credentials, passwords, API keys, configuration tokens, and machine identities	Its current secrets-management products manage and distribute credentials, while password-management products use encrypted enterprise vaults. Failure would undermine the security promise customers purchase.	PANW's own FY2026 10-K explicitly names sophisticated nation-state actors, advanced persistent threat intrusions, and supply-chain attacks, and identifies security providers as attractive cyberattack targets. CyberArk's FY2024 standalone warning provides corroborating historical evidence. [S3]
GitLab — GTLB	Proprietary development data, software workflows, and now an explicitly disclosed hosted secrets-management product	Customer-data confidentiality and software-supply-chain integrity are central. Its latest operating release makes the credentials connection more direct than the annual report alone suggests.	Structural exposure is established; the evidence cited here does not establish a state-attributed GitLab incident. [S4]
Intuit — INTU	Tax returns, bank-account numbers, credit information, login credentials, Social Security numbers, payroll, and business financial records	These are core inputs to its products, not incidental contact data. Intuit also warns that its single-identity ecosystem can allow a security incident to expose more information across products.	Explicit in its latest annual filing: nation-states and state-sponsored organizations, alongside other attackers. It explains that well-known offerings holding sensitive financial information attract attacks. [S5]
Equifax — EFX	Consumer credit, employment/income, and other sensitive personal information	Data is a core commercial asset. Its filing describes how a prior breach damaged customer relationships and revenue, and how lost certifications caused customers and partners to stop or pause business.	Explicit: some attacks may be state-sponsored and supported by substantial financial and technological resources. [S6]
Snowflake — SNOW	Centralized enterprise datasets and access to customers' data environments	A serious exposure can damage customer trust, create contractual liability, and deter workloads—even where Snowflake did not cause the credential compromise.	The strongest cited evidence concerns data concentration and economic consequences , not state attribution. Customer-controlled credentials and configuration are an important qualification. [S7]

My interpretation

Okta is one of the clearest overall matches. It combines security-dependent revenue, access into customer environments, and explicit state-actor disclosure. Its latest annual filing says:

“As a provider of independent and neutral cloud-based identity solutions that form a part of our customers' security software supply chain, we pose an attractive target for such attacks.” **[S1]**

Coinbase is the clearest match for irreversible financial consequences. Its filing states:

“The theft, loss, or destruction of private keys required to access any crypto assets held in custody for our own account or for our customers may be irreversible.” [S2]

That is materially different from losing a replaceable customer-contact database. Coinbase also has realized customer-data exposure: its FY2025 10-K, Item 1C, describes the Data Theft Incident disclosed in May 2025 and reports \$311.2 million of 2025 cash payments for voluntary customer reimbursements and direct legal costs. It states: “No passwords or private keys were compromised as a result of this incident.” This demonstrates customer-data and social-engineering consequences, not a state-attributed key theft. The same filing describes protective controls; high exposure should not be confused with an absence of safeguards. [S2]

Intuit and Equifax are especially close fits for your financial-information example. Their products depend on handling information whose confidentiality is fundamental to customer, consumer, supplier, and regulatory trust. Equifax’s disclosures provide particularly concrete evidence that security failures can interrupt commercial relationships—not merely generate remediation expenses.

2. Newer disclosures that materially affect the shortlist

GitLab now has a more direct secrets-management connection

The **September 1, 2026 8-K**, including its earnings-release exhibit, says GitLab:

“Launched GitLab Secrets Manager, which is now available as a usage-based add-on for Premium and Ultimate customers on GitLab.com”

The release says the product is intended to make credentials easier to rotate and less likely to leak, under the same permissions and audit trail as the code using them.

Why this matters: GitLab belongs on the list not just because development platforms handle proprietary data. Its newer disclosure explicitly places it in customer secrets management. The qualification is deployment scope: this disclosure concerns the GitLab.com add-on, not proof that every GitLab customer entrusts credentials to GitLab’s hosted environment. [S4]

CyberArk should not be treated as a current standalone exposure

Palo Alto’s **FY2026 annual filing** confirms its acquisition of CyberArk and describes current password, secrets, and credential-management capabilities. Its Business section explicitly discusses **API keys, configuration tokens, credential rotation, and dynamic secret provisioning.**

Why this matters: CyberArk is an excellent operational match for your question, but **PANW is the relevant public-company parent.** PANW also has a broader business, so this is not a pure-play exposure to secrets custody. CyberArk’s FY2024 state-actor warning is useful historical evidence, not a substitute for the parent’s latest filing. [S3]

3. Microsoft and Cloudflare: stronger evidence of state targeting, less concentrated exposure

These deserve separate treatment because their filings describe actual state-associated activity, rather than merely listing possible attackers.

Microsoft — MSFT

Microsoft's **FY2026 10-K** describes a nation-state-associated actor compromising a legacy test account through password spraying, gaining access to Microsoft email accounts, and subsequently accessing some source-code repositories and internal systems. It states that the incident harmed reputation and customer relationships.

Its cloud, productivity, developer, and security businesses make it relevant to customer-data and access risk. However, Microsoft is a **broader, diversified exposure**, rather than a narrowly focused secrets custodian. Its newer **September 2, 2026 8-K** updates reporting structure and explicitly brings together Microsoft 365, GitHub, and Azure infrastructure; it does not remove the underlying security dependency. [S8]

Cloudflare — NET

Cloudflare's **FY2025 10-K** describes a **likely nation-state actor** obtaining unauthorized access to an internal system. It also says hostile parties, including nation-states and their agents, have sought employment or attempted to manipulate employees or contractors.

This is unusually direct targeting evidence. Importantly, Cloudflare says it believes it cut off the identified intrusion before significant impact on customer data or systems. **That is evidence of targeting—not evidence that a catastrophic customer-data compromise occurred.** Its business depends on customers trusting the security, performance, and reliability of its network and products. [S9]

4. The distinctions that matter most

The most useful way to refine this list is by **what compromise permits**, rather than how often a filing mentions cybersecurity:

- **Control of assets:** Coinbase's key exposure can translate into irreversible customer financial loss.
- **Control of access:** Okta and CyberArk-related capabilities sit close to authentication, privileged access, and credential distribution.
- **Control of software workflows and secrets:** GitLab combines proprietary development data with a newly disclosed hosted secrets product.
- **Concentration of sensitive records:** Intuit, Equifax, and Snowflake have substantial confidentiality and trust dependencies.

Two qualifications are particularly important:

1. **Hosting data is not the same as having unrestricted access to it.** Encryption, customer-managed keys, deployment architecture, and access controls matter. The filings reviewed do not support a standardized cross-company measure of those protections.
2. **Customer fault does not eliminate vendor economic exposure.** Snowflake explicitly warns that it can suffer liability or reputational harm even where customer credential exposure or inadequate controls

caused the incident. Conversely, that does not mean every customer incident represents a compromise of Snowflake's platform. [S7]

[WEB] External context — separate from company filing evidence

The FBI's **February 26, 2025** advisory attributed the theft of approximately **\$1.5 billion** in virtual assets from Bybit to North Korea. This supports the broader relevance of state-backed asset-theft risk to crypto businesses.

It is **not evidence of an equivalent incident at Coinbase**, and it is not used to estimate Coinbase's breach probability.

Source: [FBI attribution advisory](#).

Bottom line

For a focused watchlist, I would start with **OKTA, COIN, GTLB, INTU, EFX, and SNOW**, plus **PANW specifically for its CyberArk-derived identity and secrets business**.

If your emphasis is **documented state-actor attention**, rather than concentrated business-model dependency, add **MSFT and NET** prominently.

The evidence supports identifying these businesses as unusually sensitive to confidentiality or credential failures. It does **not** support declaring which will be breached next, which has the weakest defenses, or which would experience the largest shareholder loss.

Methodology, freshness, and provenance

Latest-year verification

The latest annual fiscal years and period ends were verified against the cited filings. The latest annual fiscal year across the selected companies is **FY2026**.

Ref.	Company	Latest annual fiscal year / period end verified in filing	Filing evidence
S1	OKTA	2026 / 2026-01-31	10-K , Item 1A; August 26, 2026 8-K body and exhibit
S2	COIN	2025 / 2025-12-31	10-K , Item 1A and Item 1C; July 30, 2026 8-K body and available exhibit text
S3	PANW	2026 / 2026-07-31	10-K , Item 1, Item 1A, and Item 7; September 1, 2026 8-K. Historical CyberArk evidence: FY2024 20-F, Item 4
S4	GTLB	2026 / 2026-01-31	10-K , Item 1A; September 1, 2026 8-K and exhibit , Business Highlights
S5	INTU	2026 / 2026-07-31	10-K , Item 1A, Operational Risks

Ref.	Company	Latest annual fiscal year / period end verified in filing	Filing evidence
S6	EFX	2025 / 2025-12-31	10-K , Item 1A, Technology and Data Security Risks; July 21, 2026 8-K body and exhibit; October 20, 2026 8-K body and Exhibit 99.1 , retrieved directly from SEC via web
S7	SNOW	2026 / 2026-01-31	10-K , Item 1A; September 2, 2026 8-K body and exhibit
S8	MSFT	2026 / 2026-06-30	10-K , Item 1A; September 2, 2026 8-K body and exhibit
S9	NET	2025 / 2025-12-31	10-K , Item 1A; August 6, 2026 8-K body and exhibit

Screening: Used published concepts including *Nation-State Cyber Threats*, *Cryptographic Key Management*, and sensitive-data/breach-liability concepts as discovery aids—not risk scores. Corresponding narrative summaries were read to identify business dependencies, then original filing passages were retrieved. All summaries were not quoted as filing text.

Freshness limitations: Reviewed recent company filings for every shortlisted company and read newer relevant operating-update bodies. The review identified **no material events after September 9, 2026** for Intuit; targeted filing-text and web checks did not resolve that coverage gap. Equifax's **October 20, 2026** 8-K body and Exhibit 99.1 were retrieved directly from the SEC website, resolving its filing-text retrieval gap. The release reiterates sensitive-information security and certification risks and ongoing legal costs related to the prior cybersecurity incident; it does not disclose a new cybersecurity incident. The remaining coverage limitations prevent a blanket claim that no newer cyber development exists, but do not negate the business-model exposures established in the annual filing bodies.