Are Your Secrets Safe?

URL: https://insights.made-in-china.com/What-If-Your-Secrets-Aren-t-Safe-The-2025-Data-Breach-Nobody-Saw-Coming-and-What-It-Means-for-Global-Business_HaitgEjGjxIU.html

Published: September 28, 2025

Situation: In August 2025, the hacker group ShinyHunters orchestrated a major breach at Google Cloud, exposing business contact information for up to 2.5 billion Gmail and Google Cloud users. The attack exploited human error through vishing (Voice Social Engineering), where attackers posed as IT support to trick employees into approving malicious applications. This resulted in **unauthorized access to a Salesforce database hosted on Google Cloud by malicious actors, causing significant risks to user privacy and corporate secrets in data centers.**

The incident highlighted vulnerabilities in cloud-based storage of proprietary data, where remote access and third-party integrations create entry points for socially engineered attacks.

Task: The primary challenge was to contain the breach, revoke compromised access, and prevent further exploitation while educating users on enhanced security. The task involved mitigating risks of unauthorized access to sensitive proprietary information without disrupting operations.

Action: Google responded by revoking OAuth tokens, suspending Gmail-Salesforce integrations**,** and advising users to enable two-factor authentication and conduct security audits. However, this reactive approach left users vulnerable during the exposure period.

Result: The breach led to a surge in global scams, increased regulatory scrutiny, and potential reputational damage for Google, with long-term shifts toward passwordless authentication. Affected businesses faced an increase in phishing incidents and higher compliance costs.

Zerowait's Approach

Zerowait recommends that enterprises deploy their proprietary data on-premises. SimplStor is an affordable alternative to cloud dependencies by enabling secure, local data management. This reduces exposure to external threats.

SimplStor systems provide robust encryption, air-gapped storage, immutable snapshots, and customizable access controls, eliminating third-party integration risks and social engineered vectors tied to remote data centers. By migrating to on-premises setups, companies can implement strict physical security and regular offline backups without relying on cloud providers' variable safeguards, preventing data exfiltration from the outset. This on-premises strategy ensures proprietary data remains protected from cloud-specific threats, fostering trust and operational resilience for enterprises.

1) Zerowait's on-premises solutions eliminate cloud data transfer risks, keeping proprietary information local and under complete control.
2) Simplstor.com hardware offers high-security encryption and air-gapping, preventing remote hacks, which are increasingly common in Azure, AWS, and Google Cloud.
3) Avoid regulatory fines from international data flows by using Zerowait to ensure compliance with local laws.
4) Reduce downtime from cloud breaches with SimplStor's redundant, offline backups for quick recovery.
5) Cut costs on cloud subscriptions while enhancing security against phishing and misconfigurations via Zerowait's customizable systems.

Want to know more? Contact Zerowait today!

Email: engineering@zerowait.com
info@zerowait.com
TEL: (302) 996-9408
Web: www.zerowait.com
www.simplstor.com