i4 Zero Exfil

0) First Principles for Data breaches:

- Question current assumptions
- Break the problem into its most fundamental elements
- Rebuild solutions from those essential elements

1) Question current assumptions –

Assumption: Preventing penetration is protection from data breach.
Yes, Preventing penetration reduces data breach by bad actors without valid credentials.
No, valid credentials are frequently used to steal data. Evidence: data breach is daily news.

- Valid credentials can be used by disgruntled users, departing employees, contractors, 3rd parties.
- Valid credentials can be harvested by phishing or simply purchased off the dark web.
- Valid credentials can be a result of sloppy cloud credential management (Snowflake, Chegg).
- Valid credentials are then used to access systems, search and then steal sell-able data.

Conclusion: current network security and identity access security fails to prevent data breaches.

2) Break the problem into fundamental elements –

Network: data-in-motion is encrypted, always. Data breach involving network transmission is rare.

Storage: data-at-rest, is encrypted, always. Brute force access into storage, then taking encrypted data to later brute force decryption, is vanishingly rare.

Data-in-use, is NOT encrypted. Valid logins, provide system access, and valid logins provide unencrypted access. That's by design. Valid logins are the path of least resistance for cybercriminals.

With a valid login, taking the data is trivial – email, usb, g-drive, git, ftp, and many, many other utilities.

Conclusion: data-in-use, accessed by valid logins is the root cause of the majority of data breaches. Other security measures reduce data breaches, none of them prevent data breaches. By definition a valid login provides access.

Conclusion: Data Loss Protection, Endpoint detection and response, Fail too often. If they did work every system would have them and data breach would not be daily news.

Conclusion: focus on securing the data I/O; including AI training data, and AI query with attachments.

Conclusion: Provability and observability are essential.

3) Rebuild solutions from those essential elements –

First Principles problem statement: Prevent data breach, including valid login access.

Element 1) Storage: Prevent data breach (from what?)
Prevent data breach from a data **storage location; a storage volume**

This is consistent with CIS Data Management Policy template – look for “location”
https://www.cisecurity.org/insights/white-papers/data-management-policy-template-for-cis-control-3

Element 2) Access: Solution has approved valid login access to data-in-use (people gotta do their work):

Element 3) Prevent unauthorized data exfiltration: Solution includes data I/O control to allow or disallow data exfiltration (like eBPF, but for data storage, data security).
from data-at-rest (encrypted data storage) into data-in-use (non-encrypted data accessible in a virtual server or cloud); and back.
Don’t just reduce data exfiltration. Prevent data exfiltration.

Element 4) Deploy-ability, useability: Solution will be easy to deploy out-of-the-box, as a virtual machine.
Without breaking pre-existing network security or identity security.
Without requiring cybersecurity experts or infrastructure experts.
Solution preventing exfiltration, will include exfiltration tests to confirm.

Element 5) Monitor: Solution monitors data I/O, prevent unauthorized data I/O (keep the data IN) including AI training data and AI query with attachments.

Element 6) Dashboard, Log and Audit: for each secure data location, log user access, log data events, and exfil tests (proof of product promise).

Conclusion --

For Cybercriminals, the path of least resistance is valid logins.
The new cybercrime business model: Data-in-use is accessible with valid logins. Phishing exploits collect valid logins. Then, those valid logins are used to access systems, upload data-stealing malware to exfiltrate the sell-able data, such as data sets used for business analytics, sales histories, supplier histories, data analytics and increasingly AI for business.

AI magnifies the risk of data loss. Secure AI and Sovereign AI are the answer.

We hope this contributed clarity to the chronic problem of data breach. Data breach is daily news. Data breach is board-room top of mind as SEC, GRC, GDPR and similar regulations are enforced.
The CEO dilemma: Either innovate and risk data breach, or lock your data away and fail to innovate.
Our solution works now. Our exfil tests pass.

We urge you to participate in i4 Ops Hackathon:
You get access – you try to take our data. Begin your journey toward real data security.
Every participant receives free use of i4ops Zero Exfil software for 45-days.

Please know we are a Data Security Vendor and we are always happy to hear from you: i4ops.ai