Addressing the Threat of Secrets Sprawl

The number of secrets is growing exponentially

62%
Don't know how many secrets they have
(Keyfactor 2023 State of Machine Identity Management)

42%
Growth in machines (workloads and devices)
(2021 Global CIO Survey)

100K
Widespread secrets leaks
(2021 Global CIO Survey)

61%
Breaches involve hacked credentials
(Verizon 2022 Data Breach Report)

Why are secrets so hard to secure?

20%
In 2020, over 5,000 secrets were found on open Github repositories per day, marking a 20% increase compared to 2019. Of these, 85% involved developers' personal accounts, and 15% were on organizationally managed accounts.[1]

350
Developer secrets were exposed for 350 days, requiring a costly investigation into over 100,000 files.[2]

9x
Researchers found the records of 150,000 to 200,000 patients of nine healthcare-related organizations in GitHub repositories.[3]

10 Proven Steps to Gain Control

1. centralize secrets management
2. apply role-based access control
3. regularly rotate secrets
4. utilize strong encryption
5. monitor and audit
6. automate secrets use
7. implement MFA
8. regularly review and update policies
9. establish a lifecycle management process
10. conduct security assessments

Key Insights

1. Secrets sprawl makes it difficult to maintain control and visibility, expanding an organization's attack surface.
2. Secrets are often hardcoded into applications and devices, making them vulnerable to exposure.
3. The challenges of secrets management include a lack of visibility, limited access control, and difficulties in remediation strategies.

1 https://www.gitguardian.com/state-of-secrets-sprawl-on-github-2021
2 https://www.openraven.com/blog/automate-data-classification-to-combat-secret-sprawl
3 https://www.techtarget.com/searchsecurity/tip/How-to-manage-and-reduce-secret-sprawl

thalesgroup.com

THALES
Building a future we can all trust