

# Voice of Practitioners 2024 Report Examining the Current State of Secrets in Appsec

*Joint GitGuardian and CyberArk Report Reveals Growing Concern and Increased Investment in Secrets Security*

PARIS, FRANCE, October 30, 2024 /EINPresswire.com/ -- [GitGuardian](#), the end-to-end secrets security leader, today announced the findings of their “Voice of Practitioners 2024” report, an in-depth study conducted in partnership with [CyberArk](#), the identity security company. It examines the current state of application security (AppSec), particularly focusing on secrets management and code security. The report, based on a survey of 1,000 IT decision-makers in organizations with over 500 employees across the US, UK, Germany, and France, reveals a significant rise in awareness and concern regarding the risks associated with secrets sprawl.

## Key Findings:

- Secrets leaks are on the rise: 79% of respondents reported having experienced or been aware of secrets leaking within their organization, up from 75% in the previous year. This highlights the growing pervasiveness of this security challenge.
- Investment in secrets management is increasing: 77% of respondents are currently investing in or planning to invest in secrets management tools by 2025, with 75% focusing on secrets detection and remediation tools. This demonstrates a commitment to tackling the issue head-on.
- Organizations are moving towards mature strategies: 74% of respondents have implemented at least a partially mature strategy to prevent secret leaks. However, 23% (down from 27% in 2023) still rely on manual reviews or lack a defined strategy, indicating a concerning absence of awareness or proactive measures among some organizations.
- Confidence in secrets security remains high: 75% of respondents expressed moderate to high confidence in their organization's ability to detect and prevent hardcoded secrets in source code. This confidence level is even higher in the US, reaching 84%. On average, respondents also said they're able to rotate 36% of their secrets on an annual basis.
- Remediation times remain a challenge: The average time to remediate a leaked secret stands at 27 days. However, GitGuardian's data suggests that implementing secrets detection and

remediation solutions can significantly reduce this time to approximately 13 days within a year.

□ Concerns regarding AI and supply chain risks are growing: 43% of respondents concerned about the potential for increased leaks in codebases highlighted the risk of AI learning and reproducing patterns that include sensitive information. Additionally, 32% identified the use of hardcoded secrets as a key risk point within their software supply chain.

"The findings of our 2024 report underscore the escalating threat of secrets leaks and the need for robust, automated solutions to mitigate these risks," said Eric Fourrier, GitGuardian CEO. "While the increasing investment in secrets management is encouraging, organizations must prioritize implementing comprehensive strategies that encompass early detection, rapid remediation, and a strong focus on developer education and best practices. It is crucial for businesses to proactively address these concerns and strengthen their security posture to safeguard their sensitive data and maintain their competitive edge."

"It is encouraging that security leaders increasingly recognize the importance of securing machine identities and eliminating hardcoded secrets," said Kurt Sand, general manager Machine Identity Security at CyberArk. "However, almost a quarter of the respondents still use manual systems to address leaks, highlighting the need to improve security, remediation and efficiency with automation. As the appetite for AI continues to drive the increase in machine identities, enterprises require automated machine identity security approaches that scale."

Download the Voice of Practitioners study [here](#).

A webinar presenting the results of the study will be held at the end of November.

Additional resources

GitGuardian - Website - <https://www.gitguardian.com/>

State of Secrets Sprawl 2024 - <https://www.gitguardian.com/state-of-secrets-sprawl-report-2024>

Secrets Management Maturity Model - <https://www.gitguardian.com/secrets-management-maturity-questionnaire>

About GitGuardian

GitGuardian is the end-to-end secrets security leader. GitGuardian helps organizations take control of their secrets' security by discovering all their secrets, prioritizing and remediating leaks at scale, protecting non-human identities, and reducing breach exposure. Widely adopted by developer communities, GitGuardian is used by over 350 thousand developers and leading companies, including Snowflake, Orange, Iress, Mirantis, Maven Wave, ING, BASF, and Bouygues Telecom. To learn more about GitGuardian, visit <https://www.gitguardian.com>.

About Sapio Research

Sapio Research (<https://sapioresearch.com/>) is an award-winning, international full-service market research consultancy. Sapio can help in all areas of quantitative and qualitative research and welcome complex, challenging briefs. They work in the specific fields of audience

understanding, brand research, and content research.

Holly Hagerman

Connect Marketing

+1 801-373-7888

hollyh@connectmarketing.com

Visit us on social media:

[Facebook](#)

[LinkedIn](#)

[YouTube](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/756020466>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.