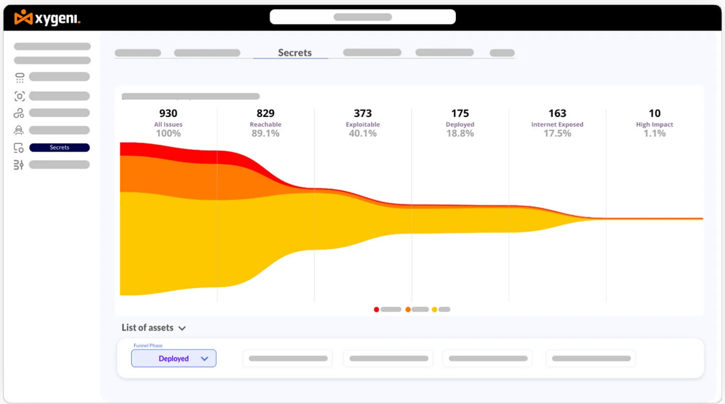
Secrets Security

Solution Brief

Block Secrets Leakage at All Stages of Development

Robust defense against secret leakage within the software development lifecycle. Our advanced solution scans, detects, and blocks the publication of sensitive information such as passwords, API keys, and tokens in real-time.



About Company

Xygeni specializes in enhancing software development security and efficiency with our Application Security Posture Management (ASPM) platform. We offer complete control over application risks, a unified security view from code to cloud, and eliminate noise to prioritize risks effectively. Our advanced malware detection and early warning system makes Xygeni a leader in protecting applications from emerging threats, ensuring rapid and secure software delivery.

Recent statistics reveal a troubling increase in secret leakage within software development. In 2023, a 28% rise was reported, totaling 12.8 million instances. This escalation highlights the need for enhanced security measures across various industries.

Even after detection, the persistence of exposed secrets poses significant risks, as 90% remain active for days. Furthermore, 3.11% of the secrets originally leaked were also exposed in public repositories. This ongoing vulnerability highlights the importance of swift and effective security protocols to mitigate potential cyber threats. Adopting advanced AI-driven security solutions is becoming increasingly vital in protecting sensitive information efficiently.

Xygeni Secrets Security acts as your reliable protector, designed to prevent the leakage of critical secrets like passwords, API keys, and tokens. As cyber threats constantly evolve, it's vital to have a solution that not only detects but actively prevents leakages before they lead to a breach. Xygeni enables your teams to work with confidence, ensuring that your development secrets are kept secure. Adopt Xygeni's proactive approach and transform your security strategy into a strong asset that builds trust and supports business continuity.

$4.35m
was the global average cost of a data breach last year

IBM

Copyright © 2024 Xygeni Security SL. All Rights Reserved.

Secrets Security

Solution Brief

Xygeni's innovative approach to secret management redefines the security posture within the software supply chain. Recognising that traditional security measures often fall short against the nuanced and evolving threat of secret leakage, Xygeni Secrets Security introduces a multifaceted strategy rooted in prevention, detection, and remediation.

Comprehensive Secret Detection

Xygeni Secrets Security uses sophisticated scanning algorithms to identify over 100 types of secrets with unparalleled accuracy meticulously. Our integration with Git hooks allows for seamless detection and immediate remediation, embedding essential security practices directly into your developers' workflows.

Real-Time Protection and Instant Feedback

By integrating with development processes via Git hooks, Xygeni Secrets Security offers an immediate line of defense. If secrets are detected before committing to repositories, the process is halted, and developers are guided to secure the exposed data. This proactive approach prevents secrets from entering version history, which can be challenging to fully remove.

Intelligent Validation and Alert Management

Our intelligent validation process effectively differentiates real threats from false positives, reducing 'alert fatigue.' This precision ensures that developers receive notifications only for genuine vulnerabilities, promoting a culture of swift and accurate security responses.

Tailored Secret Detection

Central to Xygeni's strategy is the ability for customers to customize secret detectors, allowing the definition of specific secret patterns and their locations. This tailored approach ensures that the detection of secret leakage is perfectly aligned with your unique business requirements.

Empower Developers with Actionable Insights

Xygeni's non-intrusive tools enhance the developer experience by providing actionable insights through an intuitive WebUI. Developers receive immediate guidance on handling and remediating identified secrets, fostering a secure development culture, and enabling real-time learning and adoption of best practices.

Unmatched Efficiency and Cost-Effectiveness

Xygeni's systematic risk assessment and prioritization of key vulnerabilities allows teams to focus only on the most critical secrets, reducing unnecessary remediation efforts. Early detection capabilities accelerate remediation, reducing time and costs and preventing expensive impacts of security breaches in production.

Copyright © 2024 Xygeni Security SL. All Rights Reserved.

Secrets Security

Solution Brief

Xygeni's platform supports an extensive range of detectors for various secret types commonly found in software development environments. Our broad spectrum of secret detection capabilities ensures that almost any type of secret embedded within code, pipelines, and infrastructure configurations can be identified and managed effectively.

Comprehensive Protection Across Platforms

1 API Tokens and Keys

- Detection of diverse API tokens and keys, including Amazon MWS Tokens, Alibaba Cloud Keys, Artifactory API Keys, and Azure Personal Access Tokens.
- Coverage extends to service-specific tokens such as GitHub tokens, GitLab Personal Access Tokens, and Google API Keys.

2 OAuth and Access Tokens

- Comprehensive scanning for OAuth tokens and other access tokens such as Facebook App Keys, Google OAuth2 Keys, and Slack Access Tokens.
- Specialized detectors for platform-specific OAuth implementations like Atlassian OAuth2 Client Secrets and Bitbucket OAuth Access Tokens.

3 Cloud Provider Credentials

- Detectors for credentials specific to major cloud providers like AWS, Azure, and Google Cloud, including Google Cloud Service Account Keys and Azure Storage Access Keys.
- Includes detection for less common providers like IBM Cloud and Tencent Cloud.

4 Cryptographic Keys

- Identification of cryptographic private keys, including general cryptographic keys and specific formats like Cryptographic Private Key Putty.

5 Database and Data Storage Credentials

- Scanning for credentials across various database systems such as MySQL, PostgreSQL, and Redis.
- Detection of other data storage-related secrets like RabbitMQ Passwords and LDAP Credentials.

6 Miscellaneous Credentials

- Detectors for credentials specific to major cloud providers like AWS, Azure, and Google Cloud, including Google Cloud Service Account Keys and Azure Storage Access Keys.
- Includes detection for less common providers like IBM Cloud and Tencent Cloud.

7 Cryptographic Keys

- Broad coverage for other types of secrets, such as SSH Passwords, SMTP assignments, and credentials embedded in configuration files like Maven pom.xml or .htpasswd.

Book Your Demo Now - Transform Your Approach to Cybersecurity!

Copyright © 2024 Xygeni Security SL. All Rights Reserved.