Nightfall™

Contact us at sales@nightfall.ai

Automated Protection of Secrets and Credentials

Exposed secrets and credentials are the most common cause of data breaches and are often left unmanaged. Because of this, there is a compelling need for reliable, accurate, and actionable secrets detection for modern organizations across all cloud applications. Nightfall offers best-in-class detection for diverse datasets, labeling secret findings by vendor and service type as well as identifying those credentials that are an active risk. Unlike offerings from traditional DLP solutions, Nightfall provides ML-based detectors trained on million lines of code, that protect company software, services, and data. The result is accurate, actionable intelligence for SecOps and Security teams.

How Nightfall Protects Secrets and Credentials

Discover

Historical audits to view secrets sprawl; apply policies to define a secret

Classify

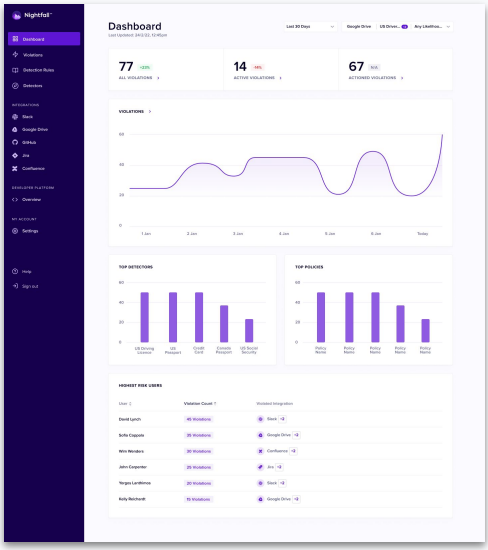
Machine learning-based detectors identify the service of the credential and exposes active risks

Protect

Real-time alerts and automated remediation. End user education, with customized notifications.

Key Features

- Easy to use, low overhead. Use automation to reduce time spent on security and compliance maintenance.
- High-accuracy, machine learning based detectors to scan hundreds of file types for sensitive data. Scan your cloud apps for API keys, passwords, and more to prevent attackers accessing your information.
- Leverage context-rich alerts in remediation workflows. See which API keys are live & which services they belong to.
- Enable employee security education with minimal overhead with customizable notifications and coaching.
- Confidently meet key data privacy and compliance mandates such as SOC 2, CCPA, GDPR, and more.



Trusted By

GENESYS™ klaviyo flatfile UserTesting