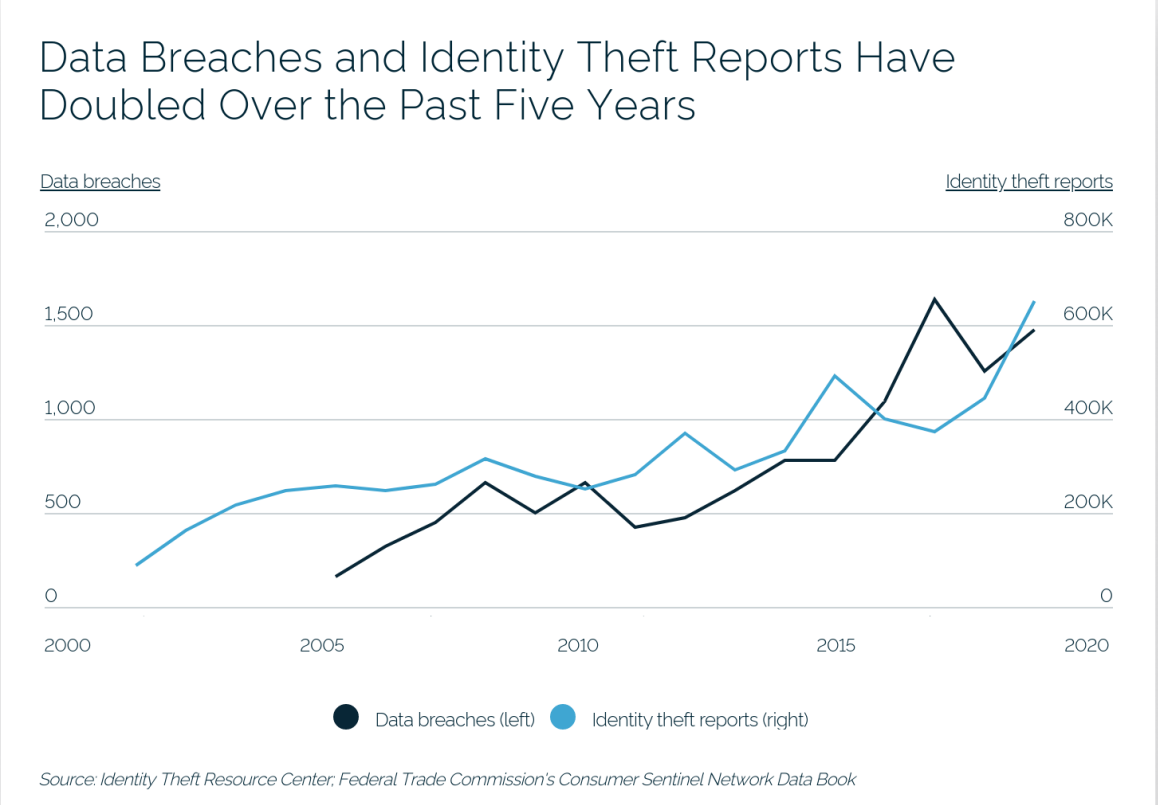
Nightfall

Guide to Data Security with the Nightfall Developer Platform

Data leakage in the modern security landscape

The last decade has seen a dramatic rise in data breach risk, with data breach incidents increasing **nearly 840% between 2005 and 2019** according to the Identity Theft Resource Center.

In response to the growth of breach risk, governments across the world have begun implementing legislation like GDPR and CCPA designed to get companies to internalize the costs of poor data security management. Gartner suggests that by 2023 **65% of the world's population** is expected to be covered by some form of data privacy legislation.



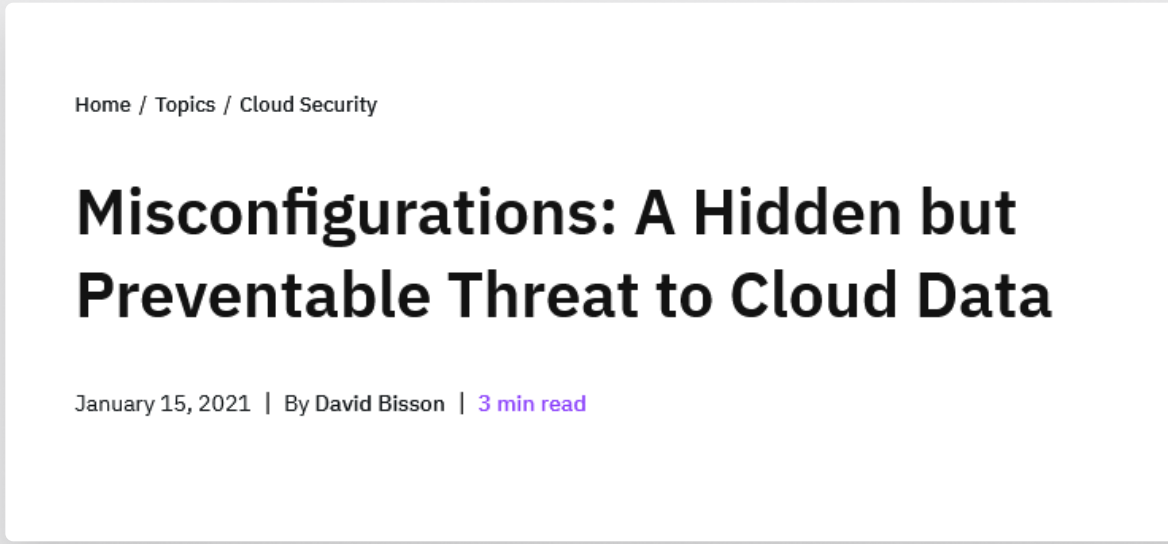
Cloud systems have increased data breach risk

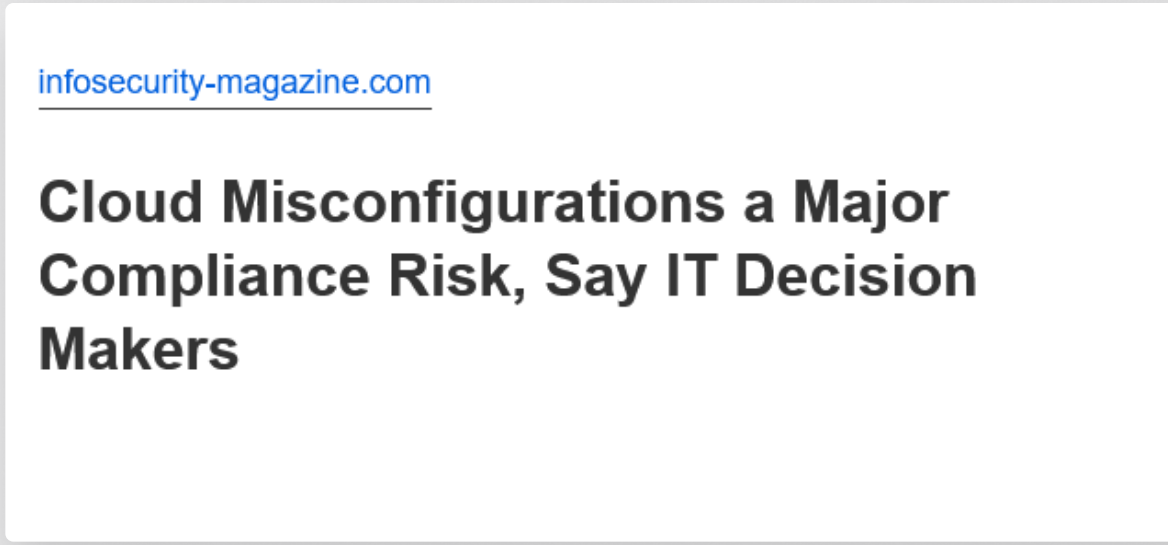
Cloud adoption has grown alongside the growth of data breach risk. By 2025 the amount of data stored in the cloud by both governments, organizations, and individuals will reach **100 Zettabytes** — an estimated 50% of the world's 200 zettabytes of data at that time.

In combination with more traditional breaches, mega breaches (breaches impacting +1 million records) and cloud misconfigurations have had sizable impacts on the cost and frequency of data exposure incidents. In its 2020 Cost of a Data Breach report, IBM found that cloud misconfigurations were among the most frequent initial threat vector in data breaches and resulted in the cost of a data breach increasing more than half a million dollars.

Key takeaway

The rapid pace of cloud migration has exacerbated data breach risks, meaning that companies must begin looking for ways to proactively mitigate the proliferation of sensitive data.





What is Nightfall?

Nightfall is a platform to discover, classify, and protect sensitive data across cloud SaaS & cloud infrastructure. Nightfall supports compliance efforts with a number of industry standards like PCI DSS, GDPR, HIPAA, CCPA, and much more.

Nightfall works by continuously monitoring data flowing in and out of data silos and classifying that data with machine learning. Data marked as sensitive can be automatically quarantined, deleted, and redacted with workflows.

Key benefits

- Get started quickly - no setup or tuning required.
- Leverage 150+ pre-tuned, high accuracy standard detectors out of the box.

Discover

Continuously monitor data that is flowing into and out of data silos.

Classify

Machine learning classifies sensitive data & PII automatically

Protect

Automated workflows for quarantine, deletion, redaction, alerts, and more.

How does Nightfall address the proliferation of sensitive data?

Nightfall addresses the problem of data proliferation in two ways:

- **Through our native SaaS and IaaS integrations**: The Nightfall DLP platform integrates with popular services like Slack, GitHub, Google Drive, and more in literally just minutes. Use machine learning based detectors to discover, classify, and protect PII, PHI and other business critical data in your cloud environments.
- **Through the Nightfall Developer Platform**: Use our APIs to leverage our machine learning detectors in any environment. With the Developer Platform take complete control of when, where, and how you scan for sensitive data in your environments for highly tailored use cases.

About the Nightfall Developer Platform

The Nightfall Developer Platform powers data classification & protection. Nightfall's programmable application program interfaces (APIs) are a set of building blocks developers can use to discover, classify, and protect sensitive data:

- Inspect data, wherever it lives, on or off the cloud.
- Add data loss prevention capabilities to any application, including third party apps or to applications and services you're building.
- Gain visibility into the data you store and process.

Getting Started

The Nightfall Developer Platform uses API keys to authenticate request; all accounts must first generate their unique key.

You can leverage the Nightfall DLP dashboard to create the rules under which Nightfall's detectors will trigger alerts. Optionally, you can programmatically set detection rules in the body of each request.

What types of data can Nightfall detect?

Nightfall's 150+ machine learning trained detectors accurately scan & classify data that developers stream to our API. We classify an average of 8M instances of sensitive data per month, providing best-in-class accuracy on structured and unstructured data alike. Find tokens in strings, documents, images, and over 100+ file types.

Standard PII: Age, Credit Card Number, Email, Ethnic Group, Name, Location, Phone Number

Health: ICD, FDA, DEA, NPI, DOB

Finance: IBAN, SWIFT, CUSIP, Routing Numbers

Crypto: Bitcoin, Ethereum, Litecoin Addresses & Private Keys

Network: IP Address, Hardware ID, MAC Address

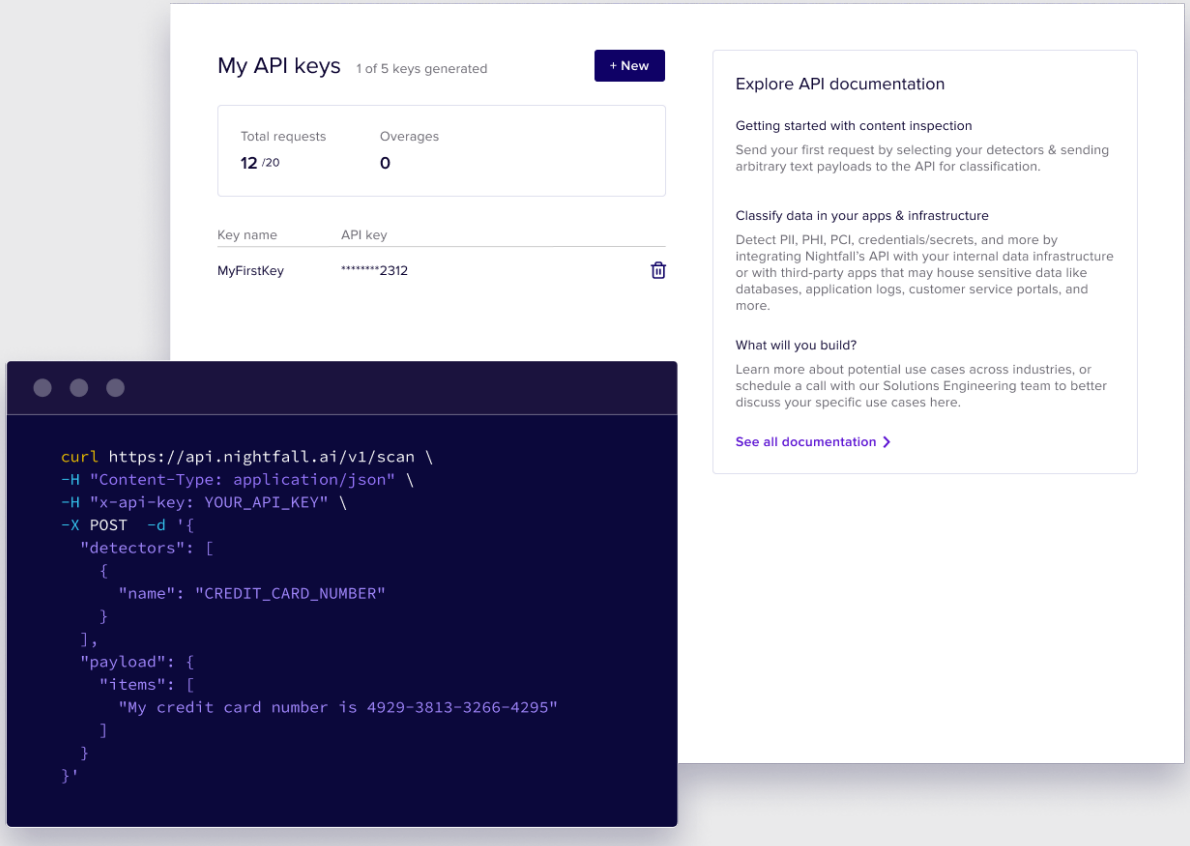
Custom: API Keys, your application UUIDs, and much more.

IDs: Driver's License Number, Taxpayer ID, Passport Number, Social Security Number, Vehicle ID

What are the key features of the Nightfall Developer Platform?

The Nightfall Developer Platform delivers a powerful set of features that provide teams the flexibility they need to reliably incorporate data protection workflows into their applications at scale.

- **REST API**: Inspect your data wherever it lives via REST API. Programmatically get structured results from Nightfall's deep learning-based detectors for things like credit card numbers, API keys, and more.
- **Seamless Integration:** The Developer Platform is built by developers, for developers. Integrate with just a few lines of code and seamlessly add data classification to your applications & workflows.
- **Customizable Detection**: Customize detectors and detection rules directly in the console UI or configure as code.
- **Best in Class Accuracy**: Deep-learning based detectors go well beyond regexes, rules, and search strings so you can make sense of your data without the alert fatigue.
- **High Efficacy**: Nightfall's machine-learning trained detectors accurately scan & classify data that developers stream to our API.



How can the Nightfall Developer Platform be used?

There are two key ways the Nightfall Developer Platform can be used:

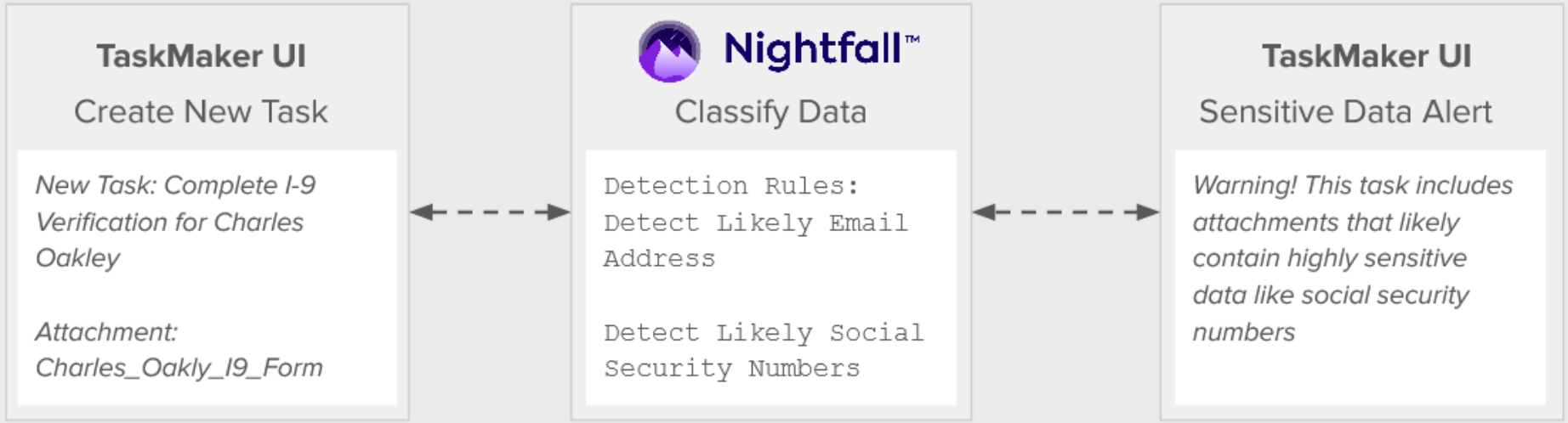
- **For product security:** Embed data protection into the services you provide your customers. Prevent mishandling sensitive data across your services without compromising performance.
- **Secure internal applications**: Protect sensitive data within applications used by employees. Enable data mobility between applications without risking sensitive data exposure across cloud and on-premise environments.

Example use case 1

Provide data protection to your users

Problem: TaskMaker (fictional) is a project management startup that allows users to create tasks associated with projects. These tasks can include description fields and file attachments that could create PII leakage risk for TaskMaker customers.

Solution: In order to reduce its own compliance risk, TaskMaker partners with Nightfall AI to scan new task attachments on creation for common types of PII like emails and social security numbers. Customers are then notified when they are publishing sensitive to their project boards.

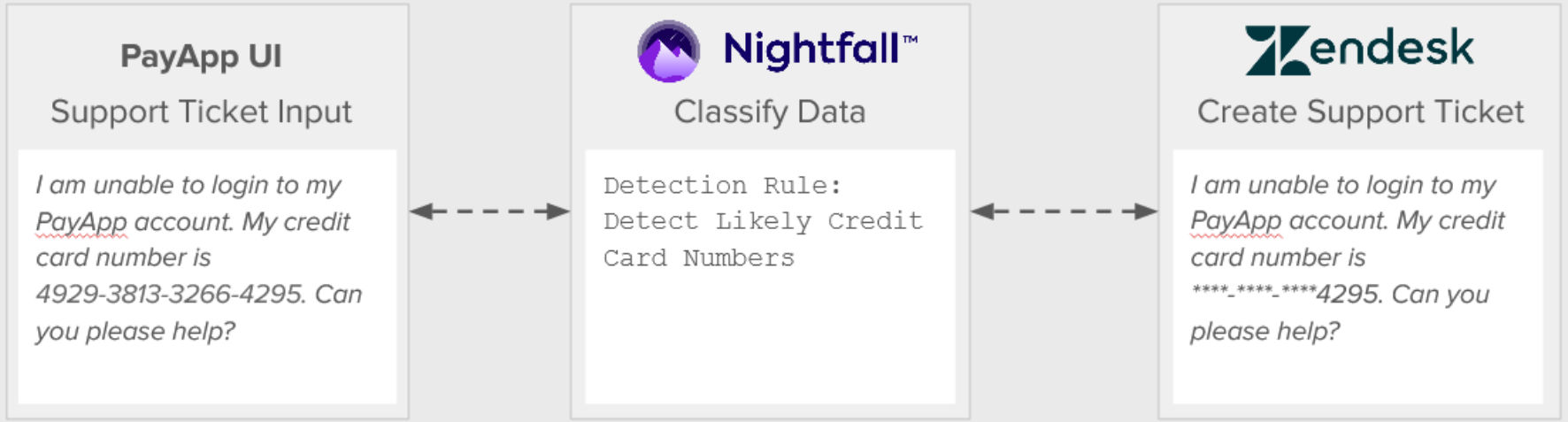


Example use case 2

Control what your users send you

Problem: PayApp (fictional) is a mobile banking app. In their app, PayApp has a Support tab that customers can submit support tickets from. These tickets are pushed to Zendesk via the Zendesk API. Customers sometimes send sensitive credit card information in these tickets, leading to security & compliance risks when this data is accessed by support agents.

Solution: PayApp would like to ensure any sensitive credit card information is redacted prior to creating a ticket in Zendesk. In their business logic, PayApp sends raw user input to Nightfall (API), Nightfall detects sensitive information, PayApp redacts this information, and then sends scrubbed user input to Zendesk (API).



Example use case 3

Review application logs for PII

Problem: PII in logs proves to be a tough challenge for many security teams to fully address. For example access logs can contain resources that might identify sensitive data accessed by a user. This can allow sensitive data to proliferate in places like Datadog, Sumo Logic, and Splunk.

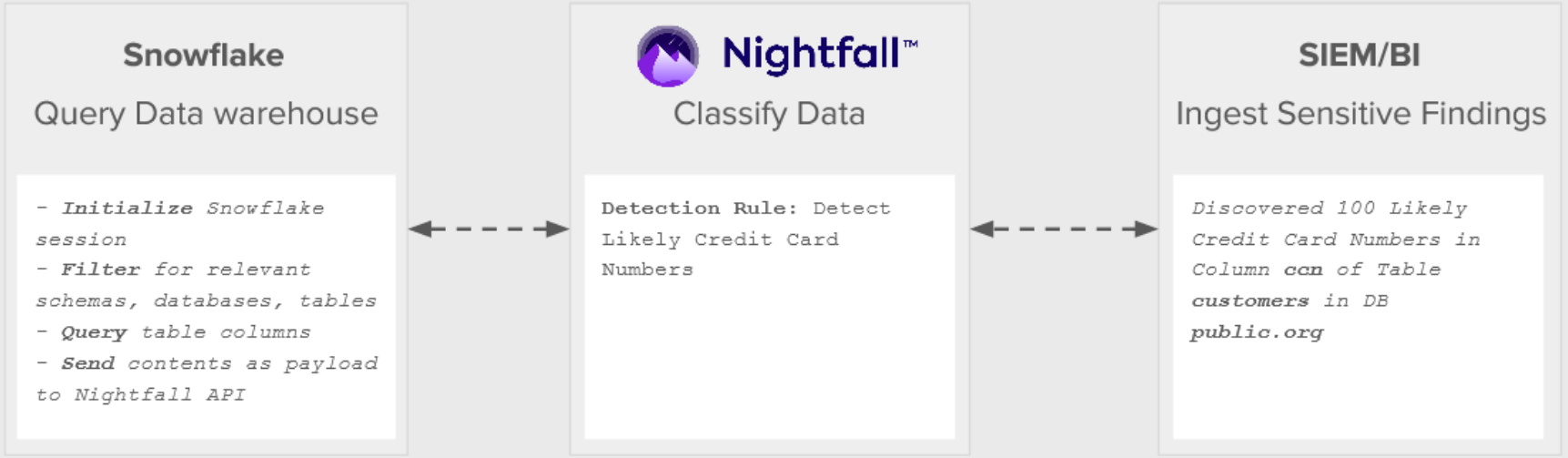
Solution: With the Nightfall Developer Platform, logs can be scanned as they're written for PII and redacted.

Example use case 4

Scan data warehouses for sensitive data

Problem: Data warehouses and databases may contain sensitive structured and unstructured data that is publicly or overly accessible, causing security & compliance risks.

Solution: Query database contents, scan contents with Nightfall for sensitive data, pipe results to SIEM or BI tool for analysis.



Want to learn more about Nightfall?

To get started with Nightfall, request a demo or email us at **sales@nightfall.ai** with any questions.

Request a demo

About Nightfall

Nightfall is the industry's first cloud-native DLP platform that discovers, classifies, and protects data via machine learning. Nightfall is designed to work with popular SaaS applications like **Slack**, **Google Drive**, & **GitHub** as well as IaaS platforms like **AWS**.

Nightfall