PLATFORM OVERVIEW

End-to-End Security Visibility with Panther

Moving Beyond Traditional SIEMs

ALERTS
SECURITY DATA LAKE
aws
REAL TIME MONITORING
okta
SURICATA

panther

Executive Summary

As organizations move to the cloud and increase their usage of SaaS services, security teams lack the visibility needed to detect and respond at scale to a growing number of attacks.

Security data needs to be collected from a variety of cloud and on-prem sources, detections need to be high-fidelity to prevent alert fatigue, and large volumes of data need to be organized and indexed to power investigations for years to come.

With Panther, security teams can leverage code-driven security best-practices, big data primitives, and cloud-first workflows to solve security and compliance challenges at scale.

Highlights

Founded in 2018

Headquartered in San Francisco

Native Integrations with Popular Services

Introduction

Panther is a security and engineering first company. Our roots come from building tools at scale for some of the largest technology companies in the world, including Amazon Web Services and Airbnb. In this Platform Overview, you'll learn how your organization can detect, investigate, and remediate threats at cloud scale using Panther's comprehensive security platform.

PLATFORM

- **Log Analysis**: Create detections as code and identify threats in real-time.
- **Cloud Security**: Continuously audit your AWS cloud configurations with policies as code.
- **Data Analytics**: Search normalized data to power investigations and baseline behaviors.

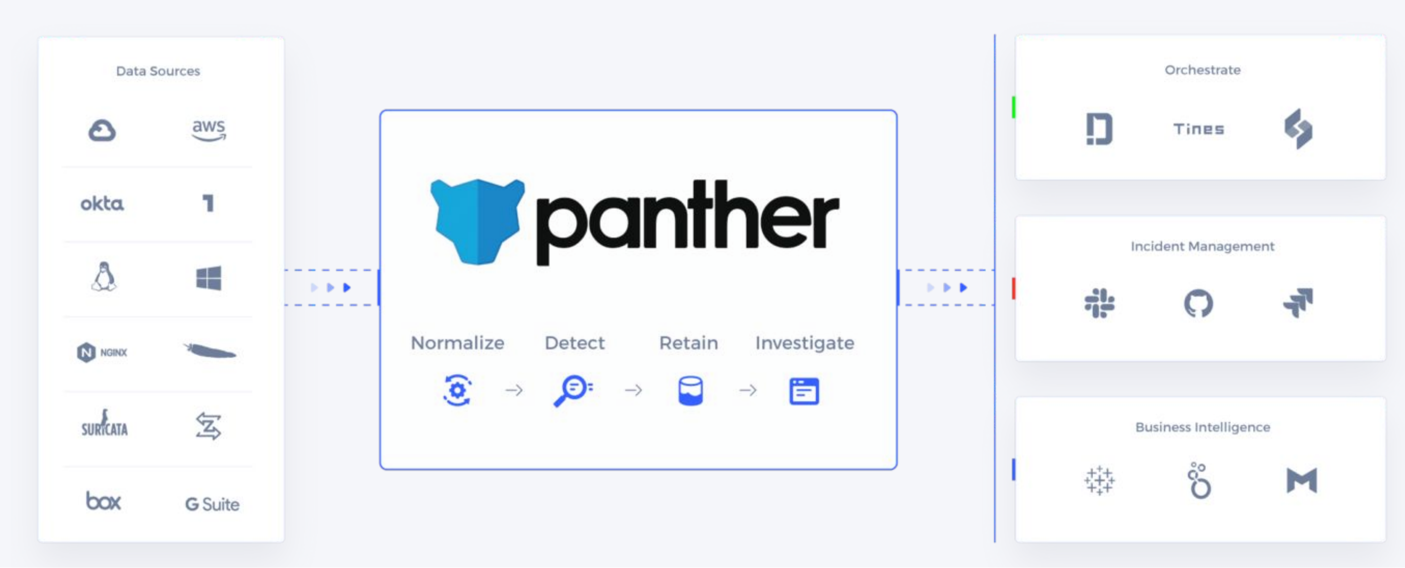
Panther was built from the ground up to help organizations collect, analyze, and alert upon terabytes of security log data to achieve greater visibility across cloud and on-prem infrastructure. With a growing ecosystem of native integrations and 200+ built-in detections, seasoned security engineers and new analysts alike can use Panther to quickly bootstrap a modern, flexible, and cloud-native security operations program.

FEATURES

- **Real-Time Detections**: Get notified immediately when suspicious activity occurs.
- **Extreme Scalability**: Process, analyze, and retain terabytes of security data at low costs.
- **Rich Integrations**: Ingest popular security logs, alert into incident management/SOAR pipelines, and connect with business intelligence platforms like Tableau.
- **Open to the Core**: Open source, open standards, and open data formats so you can build a future-proofed SecOps pipeline.

Architecture

Panther runs as a completely Serverless architecture built for scale, flexibility, and quick time-to-value. By leveraging AWS services like Lambda, DynamoDB, and S3, Panther can handle massive workloads with zero-hassle administration. In addition, our modular and open approach to detections and data storage makes Panther easy to integrate into a modern security operations pipeline.



With Panther, your organization can take a holistic approach to SIEM and cloud security, where infrastructure can be easily joined to normalized log data to power both incident investigations and detection and response workflows.

HOW IT WORKS

1. Panther collects security logs from cloud and on-premise data sources via AWS S3 / SQS / SNS or direct API integrations
2. Panther scans your AWS infrastructure to understand the state of your cloud configurations
3. All of your data is parsed, normalized, analyzed, and stored in a security data lake to power future investigations
4. Alerts are generated and dispatched to your team in real-time
5. Optional automatic remediations are applied to fix misconfigured infrastructure

Key Differentiators

PANTHER BENEFITS

- Born in the cloud — serverless, scalable, cost-effective, fast
- Rich integrations for critical security data and workflows
- Near real-time visibility of threats and cloud misconfigurations
- Built on big-data primitives for Petabyte scale
- Simple, elegant, and developer-friendly

Panther is designed to help small security teams analyze large amounts of data with code-driven best practices and cloud-first workflows. By providing capabilities for early threat detection, flexible log analysis, and robust incident investigations, Panther offers forward-thinking organizations a scalable and modern security platform to build upon for years to come.

PANTHER VERSUS THE COMPETITION

	Panther	Splunk ES	Elastic SIEM	Sumo Logic
Serverless & Cloud-Native	Yes	-	-	-
Stream Alerting	Yes	-	-	-
Cloud Security Scanning	Yes	-	-	-
Detections as Code	Yes	-	-	-
Detection Syntax	Python	Proprietary	Apache Lucene	Proprietary
Data Format	Parquet	Proprietary	Proprietary	Proprietary
Analytics Syntax	SQL	Proprietary	Proprietary	Proprietary
Single-Tenant SaaS Deployment	Yes	Yes	-	-
Snowflake Support	Yes	-	-	-
Turnkey Security Data Lake	Yes	-	-	-
Automatic IOC Extraction	Yes	-	-	-

Customer Testimonials

cedar

“Panther’s architecture is perfect for a modern technology organization: easy to roll out, scalable, and with an interface that helps us centralize and expand several of our core security and compliance operations.”

- Andrew Zollman, CISO

SCRIBD

“Panther has proved incredibly easy for a small security team to roll out to a multi-account enterprise environment, and we’re confident we have an easily scalable roadmap for the future.”

- Patrick Hagan, Security Analyst

PagerDuty

“Panther bridges the gap between security event detection and the platforms operations teams already use to mount structured and fast responses. It’s a must-have for any business adopting a DevSecOps mindset.”

- Andrew Miklas, Founding CTO

panther

Panther helps security teams detect and respond to security breaches at cloud scale. By leveraging cloud-native services and a modern, Serverless architecture, Panther provides security practitioners a powerful solution to solve SIEM and cloud security challenges at scale.

Learn more at https://runpanther.io/