Built for Security Practitioners, by Security Practitioners

The shift to the cloud has resulted in an explosion of data that security teams need to collect, analyze, and retain to detect threats. But, traditional security monitoring tools were never built with cloud-scale in mind and cannot meet the demands of today's modern workloads.

Panther was founded by a team of veteran security practitioners who faced the challenges of security operations at scale and set out to build a platform to solve them. The result is Panther, a refreshingly practical platform for threat detection and response.

Trusted by Leading Organizations

cedar · Dropbox · DOMINO · HubSpot · Airtable · Mattermost

Framer · VGS · zapier · snowflake · coinbase · Teleport

auth0 · earnin · GitLab · stedi · CIRCLE · LaunchDarkly

SCRIBD

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

Joy Sakai
Director of Core Infrastructure and Security, Scribd

How It Works

Panther is a cloud-native threat detection platform that transforms terabytes of raw logs per day into a structured security data lake to power real-time detection, swift incident response, and thorough investigations.

Data Collection

Panther collects security logs from cloud and on-premise data sources via GCS / AWS S3 / SQS / SNS or direct API integrations.

Log Normalization

Logs are parsed and normalized upon ingestion, ensuring a consistent structure for time and IoC fields to support fast detections and queries.

Real-Time Analysis

Detections are run against log data as it is ingested, providing the fastest possible time to alert.

Security Data Lake

Normalized data is aggregated in a security data lake where it is readily available for querying without the hassles of managing cold storage.

Detection-as-Code

Customize, create and harden detections leveraging Python, unit tests and standard CI/CD workflows, and get started quickly with 300+ built-in detections.

Automated Response

Add context to alerts dynamically with Python and dispatch alerts to your existing automation workflows.

Architecture

Panther runs as a completely serverless architecture built for scale and fast 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 a growing ecosystem of native integrations and 200+ built-in detections, seasoned security engineers and new analysts alike can use Panther to quickly adopt a modern, powerful, and cloud-native approach to security operations.

Benefits

Panther was purpose-built to power threat detection and response at cloud scale, giving security teams a modern security platform to build upon for years to come.

Detect threats immediately by analyzing logs as soon as they are ingested, giving you the fastest possible time to detection.

Get answers quickly with the ability to immediately query months of data in minutes and efficiently search for IoCs across all logs.

Reduce false positives with Python Detection-as-Code, and CI/CD workflows for creating, testing, and deploying detections.

Expedite incident response by adding dynamic context to alerts to power more efficient routing, triage, and automation.

Focus on security, not ops with a cloud-native architecture that eliminates the need to manage servers, storage and updates.

Reduce SIEM costs dramatically while gaining lightning-fast query speeds, with an efficient, highly scalable data lake architecture.

Panther vs. SIEM

Traditional SIEM platforms have not kept pace with the demands of today's cloud workloads, resulting in poor performance, exorbitant licensing costs and heavy operational burdens on security teams.

Panther provides a refreshingly practical platform for threat detection and response to solve the challenges of security operations at scale.

	Panther	Traditional SIEM
Data Ingestion	**Effortless ingestion** with built-in integrations for dozens of high-priority data sources and easy data mapping for custom log sources.	**Take on overhead** to build and maintain a log-ingestion pipeline, with manual effort required each time a new log source must be added.
Log Aggregation	**Gain full security visibility** by collecting, normalizing, and storing all security-relevant data in a cost-effective and high-performance data lake.	**Tolerate undue risk** by picking and choosing which logs you really need to ingest, in order to keep cost and performance at acceptable levels.
Threat Detection	**Detect threats in real-time** by analyzing logs as they are ingested, giving you the fastest possible time to detection.	**Delay running detections** until data has come to rest, extending the time that attackers have to pivot and exfiltrate data.
Investigation Speed	**Get answers quickly** with the ability to query months of data, get results in minutes, and efficiently search for IoCs across all log types.	**Wait hours or even days** to access historical data, and wait even longer for queries to complete, impeding critical investigation and response activities.
Detection Fidelity	**Write flexible, powerful detections** using Python and standard CI/CD workflows that give you the alerts you need, while reducing noise.	**Accept the limitations** of proprietary detection languages that make writing, testing and maintaining complex detections challenging and inefficient.
Licensing Cost	**Reduce SIEM costs dramatically** while gaining lightning-fast query speeds, with an efficient, highly scalable serverless architecture.	**Pay exorbitant costs** to keep up with the growth of cloud app data, due to expensive, legacy server-based architecture.
Operational Cost	**Focus efforts on security** rather than infrastructure management with a threat detection platform delivered with no operational overhead.	**Divert time and energy** away from security to grapple with burdensome system administration, DevOps, and capacity planning.

What our customers are saying

cedar

"Panther's architecture is perfect for modern technology organizations: easy to roll out, scalable, and with an interface that helps us centralize and expand several of our core security & compliance operations."

Aaron Zollman
CISO, Cedar

snowflake®

"Panther turns your Snowflake into a cloud-native SIEM so you can focus on creating high fidelity detections instead of worrying about log management costs and engineering headaches."

Omer Singer
Head of Cybersecurity Strategy, Snowflake

See Panther in Action

Learn how to secure your cloud, network, applications and endpoints with Panther Enterprise.

Request a Demo