Panther Labs

Generation Digital

Transform cloud noise into security signal

Take control of security operations with Panther — ditch unreliable legacy SIEMs and empower your team to move fast.

Scale autonomously

Your cloud, your security, your control – augmented with production-ready AI

Open Security Data Lake

Unlock the power of a modern data platform with no vendor lock-in.

AI from Detection to Resolution

Free your team for strategic work and rapidly scale threat coverage.

Code-Driven Real-Time

Automate security monitoring and detect threats in real time.

Private

Deploy in your cloud or ours for full control over data privacy and isolation.

Secure

Single-tenant environments ensure strict data isolation and maximum security.

Compliant

Meets SOC 2, PCI, ISO-27001, and HIPAA standards for robust compliance.

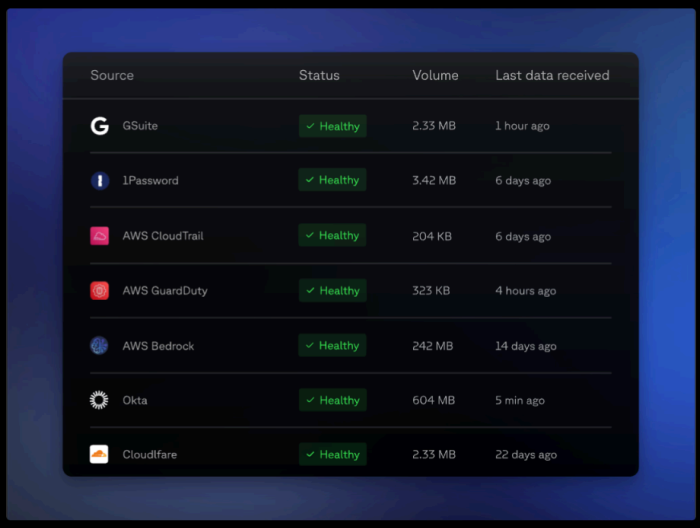
Everything you need to power modern SecOps

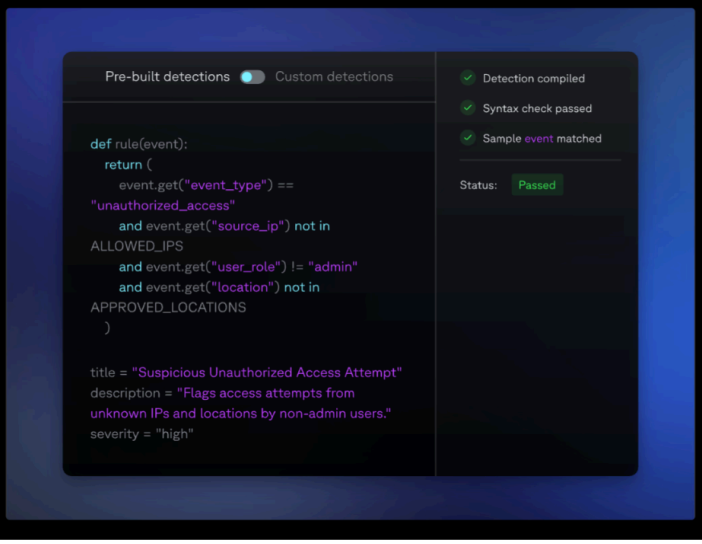
From ingestion to investigation — Panther gives you the control, visibility, and flexibility to stay ahead of threats.

Ingest and normalize all data into a security data lake

- Ingest any source, any format — at scale
- Normalize fields like IP address for consistent, reliable data
- Transform and filter logs to drive smarter security

Learn more about ingestion →





Get full security coverage with pre-built and custom detections

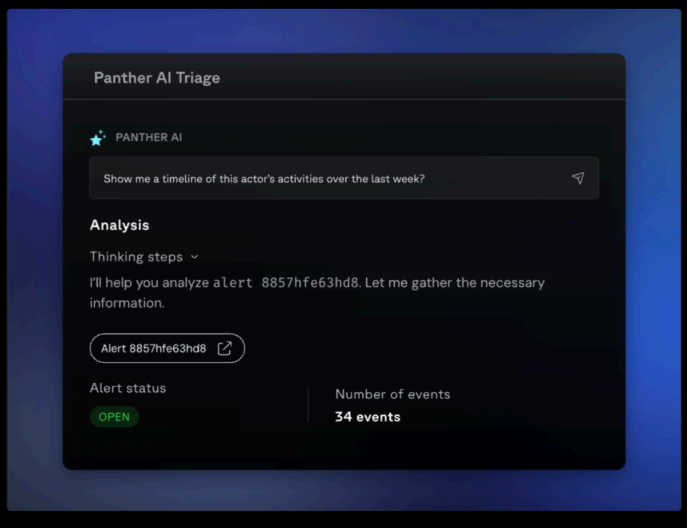
Bootstrap security monitoring fast and create actionable alerts tailored for your environment – manage alerts in Panther, Slack, Jira, or anywhere else.

Learn more about detection & alerting →

Search and visualize data to spot anomalies and triage incidents

- Visualize security trends with interactive, real-time dashboards
- Search and filter data seamlessly across multiple sources
- Quickly identify root causes with efficient data correlation

Learn more about search and analytics →



Accelerate your investigations with AI you can trust

Ditch manual investigation — use AI to triage faster with clear steps, context, and references you can trust and verify in production.

See Panther AI in action →

SOC2 (Type2) Compliant

Panther meets the Trust Services Criteria for Security, Confidentiality, and Availability.

PCI Compliant

Panther meets the Payment Card Industry standards for credit card processing and encrypted Internet transactions.

ISO27001 Certified

Panther is ISO27001 certified, meeting ISMS standards in both design and execution.

Serverless

Panther's architecture scales instantly and requires zero administration.

Single-Tenant

Customer data is isolated in dedicated instances for improved uptime, performance, and security.

Availability

We maintain 99.9% uptime through our SLA-backed commitment to system availability.

Data Security

All data is encrypted in transit and at rest, with continuous S3 backups for seamless recovery.

Application Security

Security is built into our core with SAST in CI and post-deploy, plus regular penetration testing.

IT Security

All laptops use full-disk encryption, MDM, and NGAV + EDR/EPP with 24/7/365 monitoring.

Internal Applications

Our identity provider (IdP) governs access to internal applications, which requires multi-factor authentication.

Cloud Resources

Access is managed through AWS IAM with strict least-privilege controls, and MFA is enforced across the board.

Review

All vendors undergo security control reviews before engagement.

Authorized Third Party Vendors

We also maintain a list of subprocessors and notify our customers of any changes.

ISO 27001

SOC 2 Type 2

PCI ROC

PCI Responsibility Matrix

Penetration Test

PCI AOC