

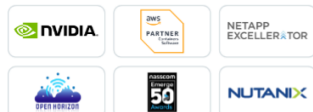


AccuKnox SIEM

Platform Overview

Unified Log Ingestion, Threat Detection, and Compliance-Ready Retention

CERTIFIED & ACCREDITED BY



AS FEATURED IN



AVAILABLE ON



Table of Contents

1	Executive Summary
2	AccuKnox SIEM: Solution Overview
3	Supported Log Sources
4	How Cloud-Native Ingestion Works
5	Technical Architecture
6	Platform Walkthrough
7	Data Retention & Storage Management
8	Product Capabilities
9	Integration & Interoperability
10	Recommended Deployment Approach
11	Security, Compliance & Auditability
12	Business Impact
13	Support & Service-Level Commitment
14	Overview Summary
15	Appendix A: Multi-tenancy & Scalability
16	Appendix B: Integration Ecosystem
17	Appendix C: Evaluation (POC) Methodology
18	Appendix D: Syslog Integration for Firewalls
19	Appendix E: Azure Integration Detail

Executive Summary

Organizations consolidating log visibility across a growing cloud, SaaS, endpoint, and network estate need a single SIEM platform that can ingest at scale, retain data long enough to satisfy audit and compliance obligations, and detect threats without drowning SOC analysts in noise. This overview describes how AccuKnox SIEM addresses that need as a platform capability — independent of any single deployment's specific source list or retention window.

Scope of the platform: log ingestion, normalization, correlation, threat detection, dashboards, alerting, and compliance-ready retention and search. Automated remediation (Cloud Detection & Response) is a related, separately-licensed capability delivered through the same cloud-connection workflow — a deployment can be scoped to detection and monitoring only, with no write-access to cloud accounts, or extended to include auto-remediation playbooks.

What AccuKnox SIEM delivers

- **Unified log ingestion:** AWS (CloudTrail, VPC Flow Logs, WAF, Config, Route 53, Network Firewall), Microsoft Azure (Activity Logs via Event Hub), GCP audit/activity logs, OCI audit logs, Google Workspace, MongoDB, Slack, Jamf, Cisco Meraki, CrowdStrike FDR, AquaSec, Palo Alto firewalls, and 70+ additional integrations across cloud, identity, SaaS, endpoint, and network sources.
- **Configurable, compliance-ready retention:** tunable per-tenant retention (e.g. 12 months) with a fast, metadata-indexed searchable window (e.g. 6 months) and on-demand audit log export.
- **Threat detection and correlation:** out-of-the-box detectors for AWS CloudTrail, Azure, GCP, and Kubernetes, custom detectors for SaaS and endpoint sources, threat intelligence enrichment, and MITRE ATT&CK mapping.
- **Purpose-built dashboards and alerting:** custom SOC dashboards, saved searches, and notifications to Slack, Jira, ServiceNow, or email.
- **Native hand-off to AccuKnox CNAPP:** SIEM findings surface in AccuKnox CNAPP's unified asset and findings view for teams already using AccuKnox CSPM/CWPP.

Why AccuKnox

- Cloud-native ingestion pipelines scale to 100K events/second and 1TB/day per tenant, with per-tenant isolation so one tenant's volume never affects another's.
- AccuKnox was founded in partnership with SRI International — the R&D lab behind the computer mouse, the modem, and some of the earliest intrusion detection research — giving the detection engine a strong technical foundation.
- A structured, time-boxed proof-of-concept (POC) lets prospective customers validate ingestion, detection, and retention against their own data before committing to a full rollout.

AccuKnox SIEM: Solution Overview

AccuKnox SIEM is a cloud-native log ingestion, correlation, and threat-detection platform, available as a SaaS deployment at siem.accuknox.com. It is a distinct product from AccuKnox CNAPP, with a native integration between the two: SIEM detections and threat-analysis alerts surface directly inside the CNAPP console, so teams already using AccuKnox for CSPM or CWPP get a single pane of glass for findings.

Core capabilities

- **Data/log ingestion:** LogStash, Bulk API, and Data Prepper connectors covering HTTP, Kafka, OTel, S3, Kinesis, DynamoDB, DocumentDB, and Fluentd inputs, in addition to native cloud log sinks and vendor APIs.
- **Extensive integration coverage:** cloud platforms (AWS, Azure, GCP, OCI), identity providers, SaaS applications, endpoint agents, firewalls (via syslog), and Kubernetes — 80+ integrations in the full platform catalog (see Appendix B).
- **Threat analysis:** multivector correlation across cloud, identity, and network events, with anomaly detection and threat hunting built in.
- **Threat intelligence enrichment:** alerts are enriched against external threat intel sources (including AlienVault) for IP and domain reputation.
- **Snapshots:** periodic snapshots of indexed data support recoverability and business continuity.
- **Native CNAPP integration:** SIEM alerts and cloud telemetry feed directly into AccuKnox CNAPP's asset and findings views — CNAPP calls SIEM APIs for CloudTrail and cloud access data, and KubeArmor runtime events flow in as a custom SIEM log type with purpose-built detectors.
- **External channel integrations:** Slack, webhooks, and Amazon SNS for downstream notification and ticketing workflows.

Ingestion at scale, per tenant

Each tenant's ingestion runs through its own isolated pipeline inside the AccuKnox SIEM Kubernetes cluster — a tenant's data lands in its own namespace (for example, tenant.accuknox.com) with a dedicated ingestion pipeline, separate from every other tenant on the platform. Cloud telemetry, endpoint data, and syslog sources all flow through this per-tenant pipeline into the shared storage backend, which is what lets the platform scale to 100K events/second and 1TB/day per tenant without one tenant's volume affecting another's.

AskADA: GenAI-powered SOC copilot

AccuKnox AskADA is a GenAI copilot that runs on top of SIEM and CNAPP data. It performs multivector threat analysis by combining an organization's own findings and telemetry with external threat-intelligence sources, giving SOC analysts faster triage and analysis across cloud and endpoint assets without manually pivoting between tools.

Platform differentiation

- Custom rules and detectors across syslog, KubeArmor, EDR, CloudTrail, Azure, and O365 log types — not just a fixed rule pack.
- MITRE ATT&CK alignment spans Cloud, Container, and Endpoint tactics, not just cloud API calls.
- Low-cost ingestion, storage, and processing architecture, which keeps per-GB retention costs down over long retention windows.
- Correlation and prioritization are built to reduce SOC analyst hours spent triaging noise, not just to generate more alerts.

Supported Log Sources

AccuKnox SIEM ingests from a broad catalog of cloud platforms, SaaS and endpoint tools, and network appliances. Sources fall into three integration patterns: cloud platforms ingested through each provider's native logging service, SaaS/endpoint tools connected through vendor APIs, and syslog-only appliances that route through a lightweight middleware VM. The table below is a representative sample of the platform's coverage.

Log Source	Ingestion Method	Notes
AWS CloudTrail	Native — AWS CloudTrail via scoped IAM role	Management and data events; onboarded via the standard AWS CloudFormation onboarding stack.
AWS VPC Flow Logs	Native — CloudWatch Logs / S3 export	Same AWS onboarding stack as CloudTrail; no separate agent.
AWS WAF	Native — S3 / Kinesis Firehose log export	Web ACL logs delivered via existing AWS onboarding.
AWS Config	Native — S3 export of Config snapshots and history	Same AWS onboarding stack.
Azure Activity Logs	Native — Diagnostic Settings → Azure Event Hub	8 log categories (Administrative, Security, ServiceHealth, Alert, Recommendation, Policy, Autoscale, ResourceHealth); see Appendix E.
GCP Audit / Activity Logs	Native — Cloud Logging log sink to Pub/Sub	AccuKnox SIEM consumes the sink directly; no forwarder required.
OCI Audit Logs	Native — OCI Logging via Streaming / Object Storage export	Read-only export configuration in the OCI tenancy.
Google Workspace	API — Admin SDK Reports API	Login, admin, and application audit events.
MongoDB (Atlas)	API — Atlas Audit Log / Atlas Administration API	Database and project-level audit events.
Slack	API — Enterprise Grid Audit Logs API	Workspace and admin audit events.
Jamf	API — Jamf Pro API / webhook events	Device management and compliance events.
CrowdStrike FDR	Native — Falcon Data Replicator (S3-based)	AccuKnox SIEM reads directly from the FDR S3 bucket.

Log Source	Ingestion Method	Notes
AquaSec	API — Aqua Platform API / webhook	Container and workload security events.
Cisco Meraki	Syslog → Syslog VM middleware → AccuKnox SIEM	See Appendix D for the syslog-to-JSON middleware architecture.
Palo Alto Firewall	Syslog → Syslog VM middleware → AccuKnox SIEM	See Appendix D for the syslog-to-JSON middleware architecture.

This is a sample, not an exhaustive list — the full integration catalog (80+ sources) is summarized in Appendix B and kept current at accuknox.com/integrations.

How Cloud-Native Ingestion Works

For AWS, Azure, GCP, and OCI, AccuKnox SIEM ingests logs directly through each provider's native logging and monitoring service — CloudTrail for AWS, Activity Logs via Event Hub for Azure, Cloud Logging log sinks for GCP, and the Logging service for OCI. No forwarders or agents run on customer infrastructure for these platforms (Azure's Event Hub relay and the syslog middleware VM, described below, are the only pieces of onboarding infrastructure a customer runs). Onboarding follows AccuKnox's standard SIEM onboarding workflow, with guides for each cloud provider (AWS, Azure, GCP).

AccuKnox uses one shared cloud-connection workflow for both log ingestion and (where separately licensed) automated response, so the same onboarding steps apply regardless of which capability is enabled. A deployment can be scoped to detection and monitoring only, with no remediation actions enabled on the customer's cloud accounts.

Azure ingestion at a glance

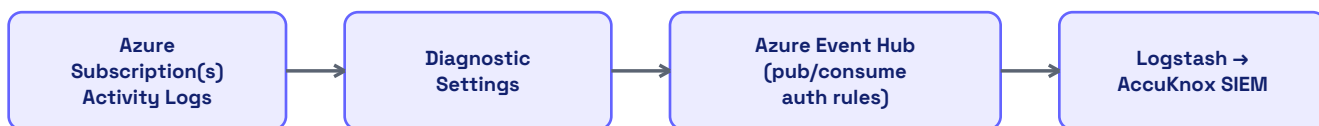


Figure — Azure Activity Logs ingestion pipeline (see Appendix E for full detail).

Azure Activity Logs are exported via Diagnostic Settings into an Azure Event Hub, which AccuKnox SIEM (via Logstash) consumes using a dedicated authorization rule — separate from the rule Azure uses to publish. This pattern extends cleanly to multiple subscriptions by scripting diagnostic settings across subscription IDs into a single Event Hub. Full step-by-step detail is in Appendix E.

Technical Architecture

AccuKnox SIEM ingests events from cloud accounts, SaaS applications, and network appliances, normalizes them into a common schema, and runs them through detectors, correlation, and threat-intelligence enrichment before surfacing results in dashboards and external channels.

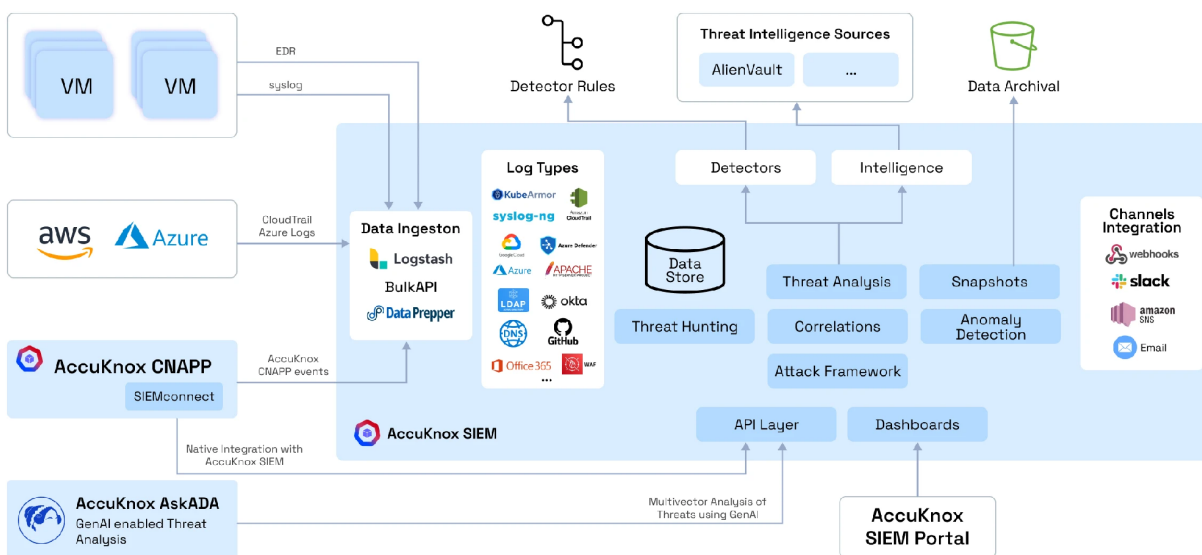


Figure — AccuKnox SIEM architecture: sources, ingestion, detection and intelligence, and downstream channels, with archival branch.

Architecture layers

- **Sources:** cloud platforms, SaaS applications, and the AccuKnox CNAPP events feed connect through their native APIs; VMs, EDR tools, and syslog-only appliances (Cisco Meraki, Palo Alto) forward through syslog.
- **Data ingestion:** LogStash, Bulk API, and Data Prepper receive and normalize events across all supported log types before they are written to the data store.
- **Data store:** logs are indexed with enriched metadata (source, timestamp, event type, severity, account, region), which is what makes the searchable window fast without scanning raw log volumes.
- **Detectors and intelligence:** detection rules and threat-intelligence sources (including AlienVault) run continuously against ingested data, feeding threat analysis, correlations, threat hunting, and MITRE ATT&CK mapping.
- **Dashboards and API layer:** the AccuKnox SIEM Portal and API layer expose search, dashboards, and snapshots; AccuKnox AskADA adds GenAI-assisted multivector threat analysis on top of the same data.

- **Channels:** detections and snapshots can notify out to Slack, webhooks, and Amazon SNS for SOC workflows.
- **Data archival:** logs beyond the searchable window move to archival storage and remain retrievable through the end of the retention period.

Platform Walkthrough

Two layers make up the day-to-day workflow: the SIEM backend, where logs are stored, queried, and visualized, and the AccuKnox UI, where alerts are triaged.

SIEM backend — log storage & query layer

The SIEM backend is where ingested logs are stored and queried directly. Access is tenant-scoped and authenticated per user.

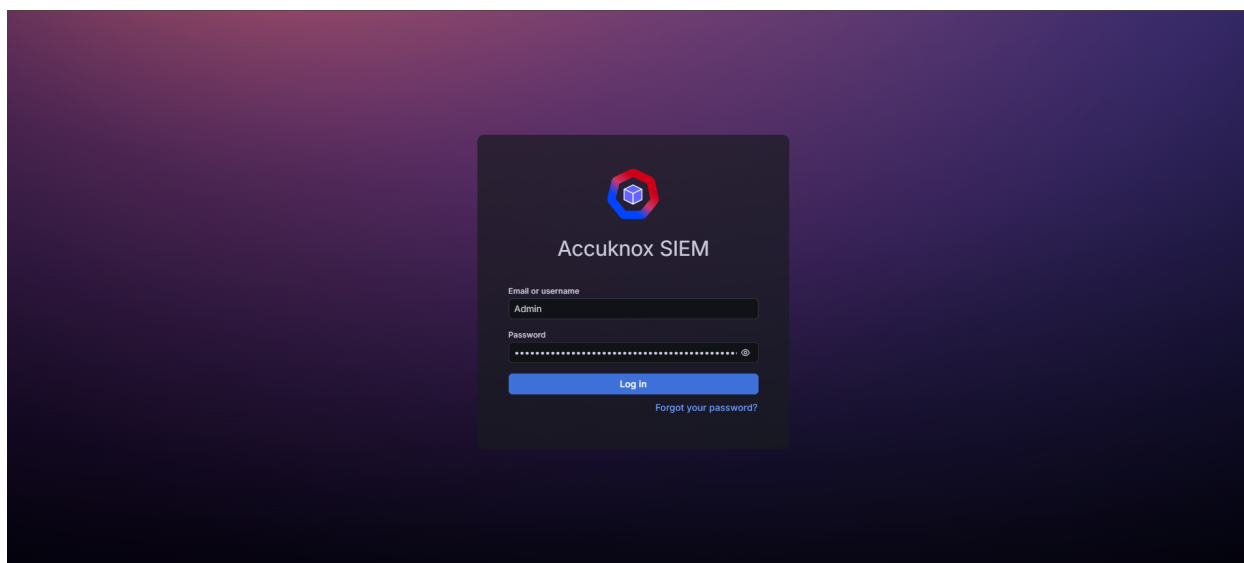


Figure — AccuKnox SIEM backend login.

Once logged in, the backend exposes purpose-built dashboards per log source — for example, an AWS CloudTrail operations dashboard showing total event volume, error/access-denied counts, unique identities, and activity trends over a selected time window.

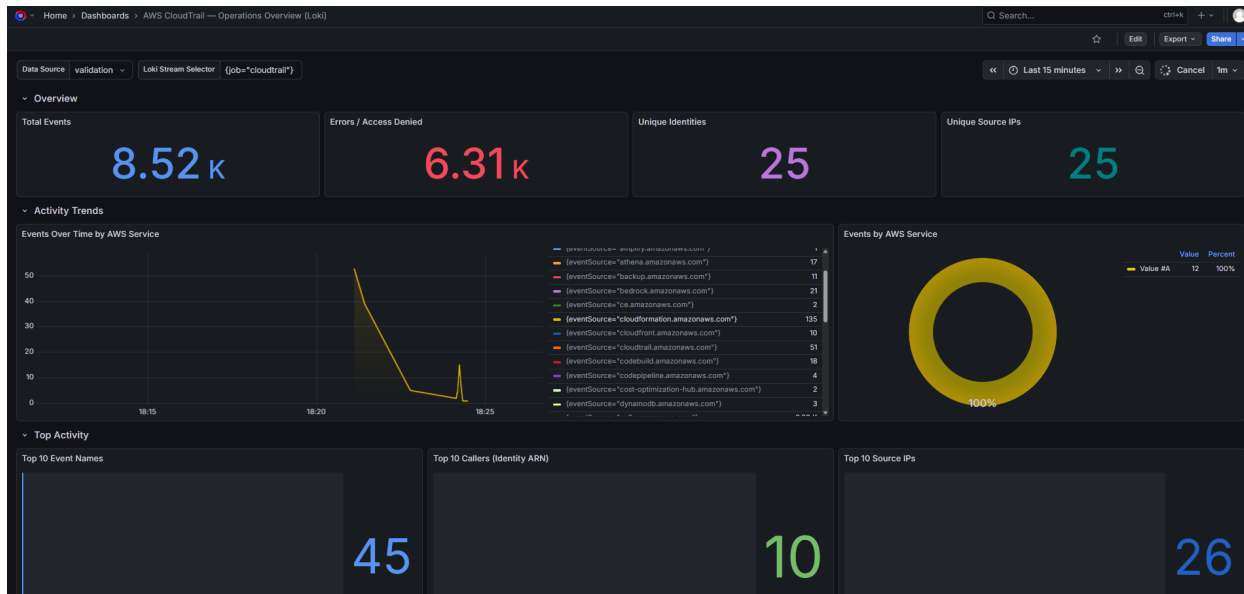


Figure — AWS CloudTrail operations dashboard on the AccuKnox SIEM backend.

AccuKnox UI — alerts

Detections surface as alerts in the main AccuKnox UI, where SOC teams triage them day to day — filterable by module, status, log source, and severity, with saved filters and export.

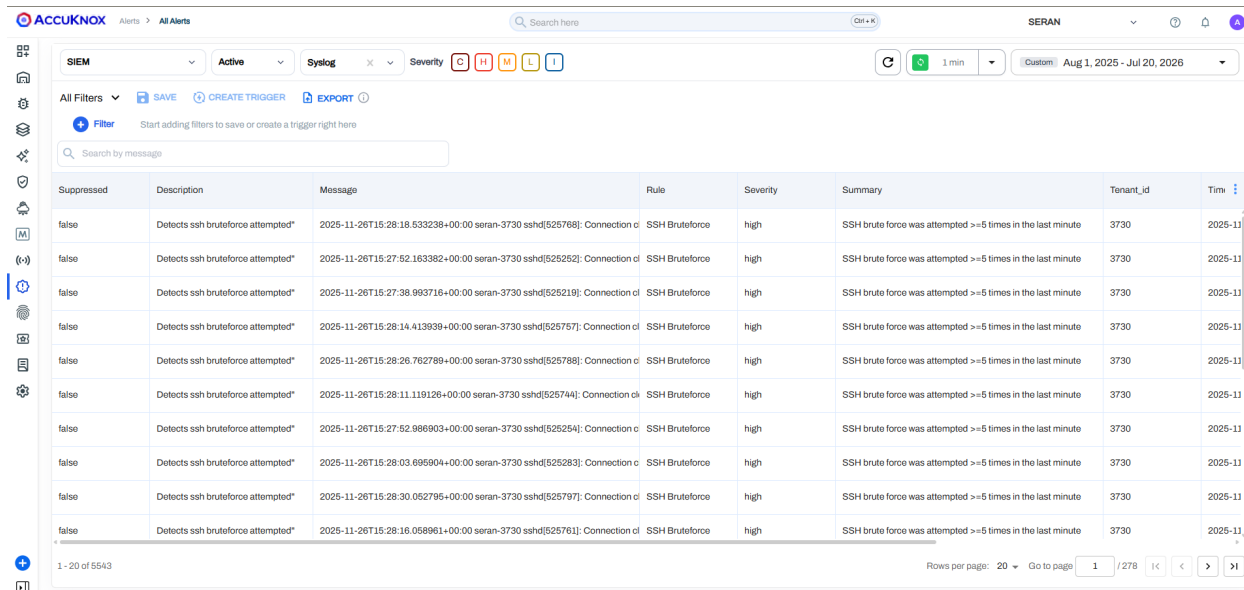
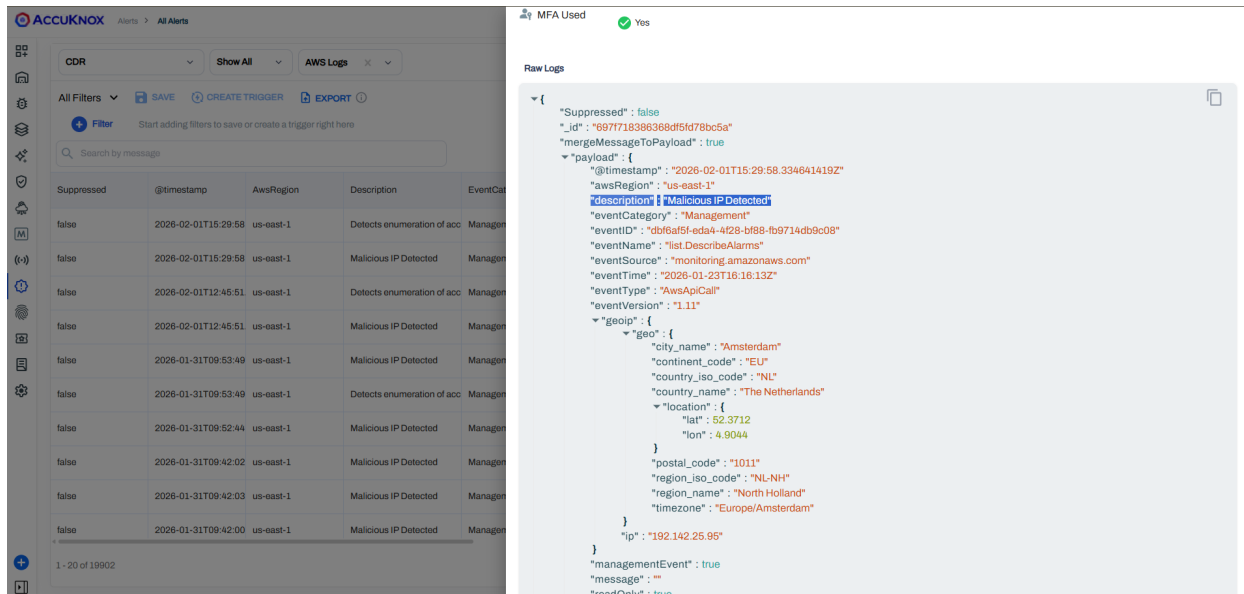


Figure — AccuKnox UI, Alerts page: active syslog-sourced alerts filtered by severity.

Each alert opens into full detail, including the raw log payload, for investigation and audit purposes.



The screenshot displays the AccuKnox SIEM interface. On the left, a table lists alerts with columns: Suppressed, @timestamp, AwsRegion, Description, and EventCa. The table shows several alerts, with the last one selected. On the right, the 'Raw Logs' section displays the JSON payload for the selected alert. The payload includes fields such as 'Suppressed', '@timestamp', 'awsRegion', 'eventCategory', 'eventName', 'eventSource', 'eventTime', 'eventType', 'eventVersion', 'geoip', 'managementEvent', 'message', and 'readOnly'.

Suppressed	@timestamp	AwsRegion	Description	EventCa
false	2026-02-01T15:29:58	us-east-1	Detects enumeration of acc	Manager
false	2026-02-01T15:29:58	us-east-1	Malicious IP Detected	Manager
false	2026-02-01T12:45:51	us-east-1	Detects enumeration of acc	Manager
false	2026-02-01T12:45:51	us-east-1	Malicious IP Detected	Manager
false	2026-01-31T09:53:49	us-east-1	Malicious IP Detected	Manager
false	2026-01-31T09:53:49	us-east-1	Detects enumeration of acc	Manager
false	2026-01-31T09:52:44	us-east-1	Malicious IP Detected	Manager
false	2026-01-31T09:42:02	us-east-1	Malicious IP Detected	Manager
false	2026-01-31T09:42:03	us-east-1	Malicious IP Detected	Manager
false	2026-01-31T09:42:00	us-east-1	Malicious IP Detected	Manager

```

{
  "Suppressed": false,
  "_id": "697718386368df5d78bc5a",
  "mergeMessageToPayload": true,
  "payload": {
    "@timestamp": "2026-02-01T15:29:58.334841419Z",
    "awsRegion": "us-east-1",
    "eventCategory": "Malicious IP Detected",
    "eventID": "dbf6af5f-ed34-4f28-bf98-fb9714db9c08",
    "eventName": "list.DescribeAlarms",
    "eventSource": "monitoring.amazonaws.com",
    "eventTime": "2026-01-23T16:16:13Z",
    "eventType": "AwsApiCall",
    "eventVersion": "1.11",
    "geoip": {
      "city_name": "Amsterdam",
      "continent_code": "EU",
      "country_iso_code": "NL",
      "country_name": "The Netherlands",
      "location": {
        "lat": 52.3712,
        "lon": 4.9044
      },
      "postal_code": "1011",
      "region_iso_code": "NL-NH",
      "region_name": "North Holland",
      "timezone": "Europe/Amsterdam"
    },
    "ip": "192.142.25.95"
  },
  "managementEvent": true,
  "message": "",
  "readOnly": true
}

```

Figure — AccuKnox UI, alert detail view with raw log payload.

Data Retention & Storage Management

AccuKnox SIEM's storage model is built around a common compliance pattern — a long retention window with a shorter, fully-indexed searchable window — and is configurable per tenant to match a customer's specific audit and compliance requirements. A typical configuration looks like this:

- **Configurable retention:** ingested logs from every onboarded source can be retained for a full year (or another period agreed with the customer).
- **Fast searchable window:** the most recent months of data (commonly 6) are indexed and fully searchable through metadata-based storage, so investigations and audits query fast without scanning raw log volumes.
- **Metadata-based indexing:** logs are enriched with source, timestamp, event type, severity, account, and region metadata at ingestion, which is what keeps the searchable window performant.
- **Data archival:** logs beyond the searchable window move to cold, S3-compatible archival storage and remain restorable on demand through the end of the retention period.
- **Ingestion and storage controls:** per-tenant ingestion limits and storage quotas are configurable, so upper limits are enforced and costs stay predictable.
- **Snapshots and backup:** periodic snapshots of indexed data protect against data loss and support recoverability.
- **Audit log exports:** scheduled or on-demand export of logs in JSON or CSV format for compliance reviews and regulatory submissions.
- **Tenant isolation:** log data is isolated from other AccuKnox tenants at the storage layer — separate index namespaces and separate database collections/tables.

Product Capabilities

Capability	Details
Log Ingestion & Retention	LogStash, Bulk API, Data Prepper (HTTP, Kafka, OTel, S3, Kinesis, DynamoDB, DocumentDB, Fluentd) plus native cloud and vendor-API connectors. Up to 100K events/sec, 1TB/day/tenant, with configurable retention and searchable-window sizing.
Threat Detection & Rules	Out-of-the-box detectors for AWS CloudTrail, Azure, GCP, and Kubernetes, plus custom detectors authored for CrowdStrike, AquaSec, MongoDB, Google Workspace, Meraki, and Palo Alto sources.
Correlation & Analytics	Multivector correlation, anomaly detection, and threat hunting across cloud, identity, and network sources, with MITRE ATT&CK framework alignment.
Threat Intelligence	Alerts enriched against external threat intelligence sources (including AlienVault) for IP and domain reputation.
Dashboards & Reporting	Custom dashboards, saved searches, metadata-based log storage, and scheduled or on-demand audit log exports.
Alerting & Notifications	Slack, webhook, and Amazon SNS notification channels for SOC workflows. No automated remediation actions are configured — alerts are informational and route to the customer's own response process.
Native CNAPP Integration	SIEM alerts and cloud telemetry feed into AccuKnox CNAPP's asset and findings views for teams already using AccuKnox CSPM/CWPP.
RBAC & Multi-tenancy	Multi-tenant architecture with granular role-based access control and SSO/SAML/MFA support; per-tenant custom views and reports.

Integration & Interoperability

AccuKnox SIEM offers 80+ integrations across cloud, SaaS, identity, endpoint, network, and Kubernetes sources, grouped into four patterns:

- **Cloud platforms — native onboarding:** AWS (CloudTrail, VPC Flow Logs, WAF, Config, Route 53, Network Firewall) via CloudFormation; Azure Activity Logs via Diagnostic Settings and Event Hub; GCP audit/activity logs via Cloud Logging log sink; OCI audit logs via the OCI Logging service.
- **SaaS and endpoint — API connectors:** identity & collaboration (Google Workspace, Slack, Jamf); data & workload (MongoDB Atlas, CrowdStrike FDR, AquaSec).
- **Network appliances — syslog middleware:** Cisco Meraki, Palo Alto, and any syslog-capable firewall forward Syslog to a dedicated Syslog VM, which converts events to JSON before AccuKnox SIEM ingests them via Bulk API (Appendix D).
- **Notification & ticketing:** Slack, webhooks, and Amazon SNS route alerts into existing SOC workflows; automated remediation and write-back actions are configured only when separately licensed.

Recommended Deployment Approach

A time-boxed, three-phase rollout is recommended for most deployments. Each phase is scoped to minimize risk and validate results before moving to the next.

Phase 1 — Log Source Onboarding & Ingestion

- Onboard cloud platforms (AWS, Azure, GCP, OCI) via their respective native onboarding templates and log-export services.
- Connect SaaS and endpoint sources (identity providers, collaboration tools, EDR, workload security platforms) via their APIs.
- Deploy the Syslog VM middleware for syslog-only network appliances.
- Validate ingestion rates and confirm the agreed retention and searchable-window configuration is indexing correctly.

Phase 2 — Threat Detection & Threat Intelligence

- Enable out-of-the-box detection rules for AWS CloudTrail, Azure, GCP, and Kubernetes.
- Author and tune custom detectors for onboarded SaaS, endpoint, and network log patterns.
- Enable threat-intelligence enrichment (AlienVault and others) and MITRE ATT&CK mapping.
- Configure anomaly-detection baselines and multivector correlations across identity, cloud, and network sources.
- Push detection alerts into AccuKnox CNAPP for a unified findings view, where applicable.

Phase 3 — Dashboards, Alerting & Compliance Reporting

- Build environment-specific dashboards: SOC overview, per-source detections, MITRE heatmap, and compliance widgets.
- Configure alerting to Slack, Jira, ServiceNow, or email with tuned thresholds and de-duplication.
- Enable scheduled audit log exports (JSON/CSV) for compliance reviews and validate retention exports end to end.

Security, Compliance & Auditability

AccuKnox SIEM's retention, search, and export model is built to support standard audit and compliance workflows. The platform's design aligns with:

- **ISO/IEC 27001** — information security management
- **SOC 2** — security, availability, and confidentiality trust principles
- **PCI DSS** — logging and monitoring requirements for cardholder data environments
- **GDPR** — data protection and audit-trail requirements
- **NIST SP 800-207** — Zero Trust architecture principles

For a specific compliance program, applicable frameworks should be confirmed during onboarding or a POC so dashboards and audit-export formats can be tuned accordingly from day one.

Business Impact

- **Tool consolidation:** replace fragmented log tooling across cloud, SaaS, and network appliances with a single cloud-native SIEM — one platform, one retention policy, one search experience.
- **Reduced infrastructure overhead:** cloud-native ingestion pipelines scale to 100K events/sec and 1TB/day per tenant without forwarder farms or heavy on-prem infrastructure — a syslog VM and/or Event Hub relay are typically the only pieces of infrastructure a customer needs to run.
- **Operational efficiency:** correlation and MITRE-aligned prioritization reduce alert noise, cutting the time SOC analysts spend triaging low-value alerts.
- **Faster investigations:** metadata-based indexing keeps the searchable window fast, so audits and incident investigations don't wait on raw log scans.
- **Audit and retention cost reduction:** configurable retention with a fast searchable window and one-click audit log exports cut audit-preparation time.
- **Scalable for growth:** per-tenant RBAC, dashboards, and ingestion controls scale cleanly as an organization adds business units, environments, or geographies.

Support & Service-Level Commitment

- 24/7 product support, per agreed commercial terms.
- A dedicated Technical Account Manager (TAM).
- Quarterly health checks and improvement recommendations.

Overview Summary

AccuKnox SIEM unifies log ingestion, threat detection, and compliance-ready retention across cloud, SaaS, endpoint, and network sources — including AWS, Azure, GCP, and OCI as first-class cloud platforms.

- **Log ingestion & search:** AWS, Azure, GCP, OCI, Google Workspace, MongoDB, Slack, Jamf, Cisco Meraki, CrowdStrike FDR, AquaSec, Palo Alto, and 70+ more — ingested at scale (up to 100K events/sec, 1TB/day/tenant).
- **Threat detection & MITRE ATT&CK:** out-of-the-box detection rules for major cloud platforms plus custom detectors, enriched with threat intelligence.
- **Retention & search:** configurable retention, a fast searchable window, metadata-based indexing, and on-demand audit log export.
- **Native CNAPP hand-off & multi-tenancy:** SIEM alerts feed AccuKnox CNAPP's asset/findings views; per-tenant RBAC and dashboards.

A structured POC can validate ingestion, detection, and retention against real data before a full commercial rollout — see Appendix C for a representative timeline.

Appendix A: Multi-tenancy & Scalability

AccuKnox is built on a multi-tenant architecture from the ground up, which allows an environment to scale horizontally without a dedicated control plane per business unit.

Isolation model

- **Hard isolation:** a dedicated instance of the app and database per customer — strong isolation, higher operational cost.
- **Soft isolation:** customers share a database, but each has its own set of tables — a balance of isolation and cost. This is the default for most deployments.

Layered architecture

- **Layer 1:** Users, RBAC, and tenants.
- **Layer 2:** Backend jobs and execution management.
- **Layer 3:** Data isolation between tenants.
- **Layer 4:** Custom reporting, dashboards, and layouts per tenant.

A single user can belong to multiple tenants with different permissions in each — useful if, for example, a security team needs read access across two regional business units while engineering teams stay segregated.

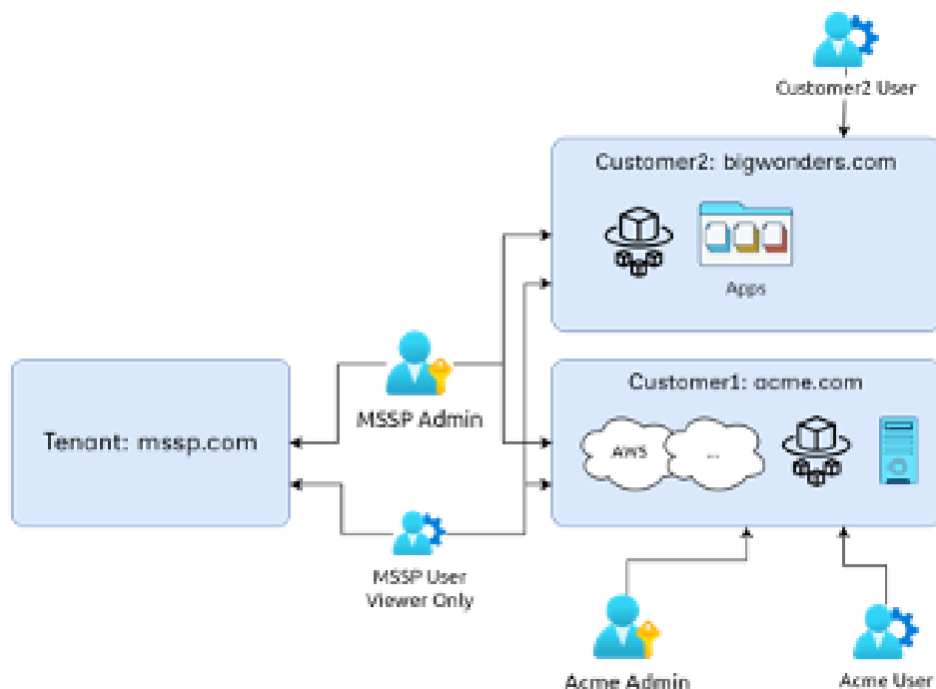
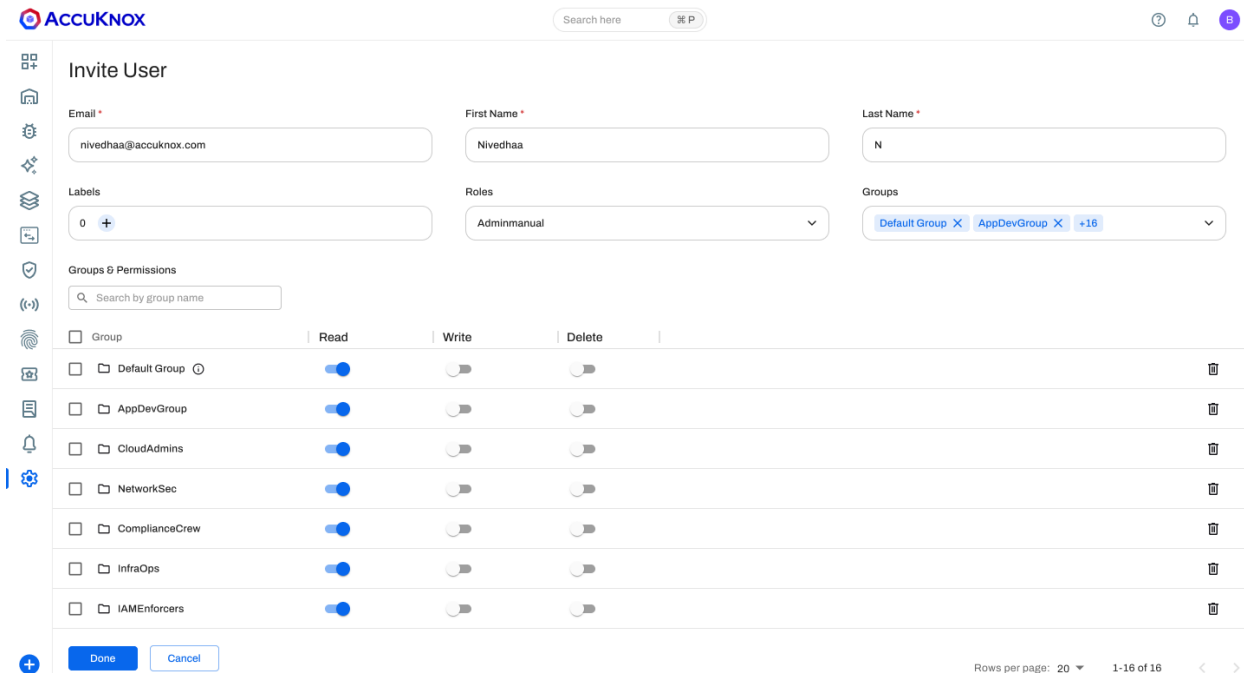


Figure — A user can hold different RBAC roles across multiple tenants.



Invite User

Email *

First Name *

Last Name *

Labels

Roles

Groups

Groups & Permissions

Group	Read	Write	Delete
☐ Default Group	☒	☐	☐
☐ AppDevGroup	☒	☐	☐
☐ CloudAdmins	☒	☐	☐
☐ NetworkSec	☒	☐	☐
☐ ComplianceCrew	☒	☐	☐
☐ InfraOps	☒	☐	☐
☐ IAMEnforcers	☒	☐	☐

Rows per page: 20 1-16 of 16

Figure — Inviting a user and assigning group-level read/write/delete permissions in the AccuKnox UI.

Resource allocation and the noisy-neighbor problem

AccuKnox uses a hybrid allocation model: customers requiring hard isolation get a dedicated control plane, while multiple small or mid-size tenants share compute through Kubernetes-native soft isolation. To prevent one tenant's workload from starving another's — the classic "noisy neighbor" problem — AccuKnox uses Kueue for cluster-wide job scheduling and isolated, namespace-based replica sets for parser tasks.

Data isolation

Tenant data is isolated at the storage layer without spinning up a separate database instance per customer: each tenant gets its own PostgreSQL tables and its own MongoDB collections, each with independent access control, which keeps the blast radius contained if one tenant's access is compromised.

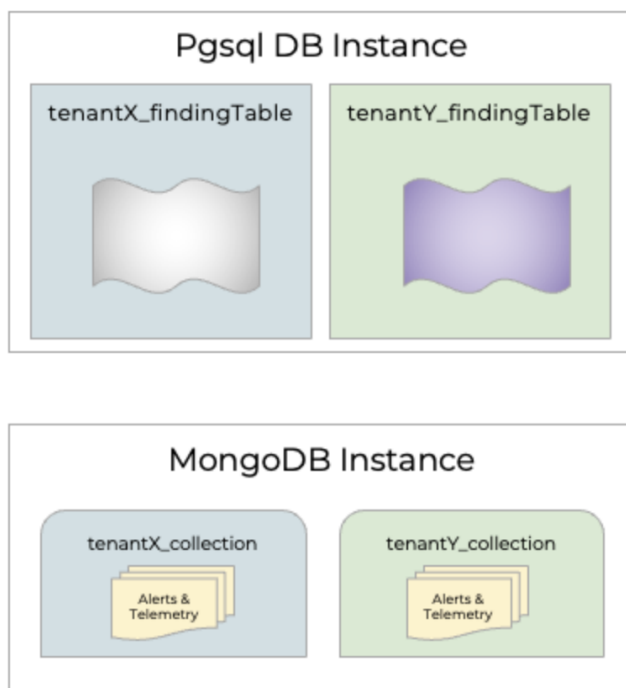


Figure — Per-tenant data isolation at the storage layer.

Deployment models

- SaaS
- Customer cloud (AccuKnox control plane deployed in the customer's AWS/Azure/GCP)
- On-premises / air-gapped

The same multi-tenancy architecture applies across all three models, and AccuKnox's control plane is already battle-tested at MSSP scale — one OEM partner alone onboards hundreds of tenants on a shared control plane.

Appendix B: Integration Ecosystem

AccuKnox integrates with 80+ ecosystem tools and frameworks across cloud, SIEM, CI/CD, and container platforms. The latest full list is available at accuknox.com/integrations.

- **Identity:** AD/LDAP, Okta, Microsoft O365, GitHub, and AccuKnox CNAPP cloud findings.
- **Firewalls & network appliances:** FortiGate, Palo Alto, and any syslog-capable firewall; routers and managed switches.
- **Cloud service providers:** AWS CloudTrail, Azure Logs (Activity Logs via Event Hub, with Entra ID sign-in/audit logs, Microsoft Defender for Cloud alerts, and NSG flow logs available as extensions), GCP Logs.
- **Endpoints:** Syslog, KubeArmor, Microsoft Defender, Microsoft Windows.
- **Kubernetes:** KubeArmor and Kubernetes API server logs.



Figure — AccuKnox platform integration ecosystem.

Appendix C: Evaluation (POC) Methodology

A proof-of-concept validates AccuKnox SIEM against a prospective customer's own log sources and retention requirements in a structured, milestone-driven approach — typically SIEM ingestion and detection only, with automated remediation out of scope unless separately agreed.

Representative checklist

Checklist Item	Validation Criteria
Log Ingestion	Validate ingestion from the agreed cloud, SaaS/API, and syslog-middleware sources.
Threat Detection	Confirm out-of-the-box and custom detectors trigger correctly against sample and live events.
Threat Intelligence	Validate IP/domain reputation enrichment against known indicators.
Dashboards	Build and validate a sample custom dashboard and saved search.
Alerting	Validate notification delivery to Slack, email, and/or Jira.
Retention & Search	Confirm the agreed retention configuration, searchable window, and audit log export in JSON/CSV.
RBAC & Multi-tenancy	Validate tenant isolation and role-based access for the customer's teams.

Representative timeline

Phase	Activities	Duration
Phase 1	Log source onboarding across cloud, SaaS/API sources, and syslog VM setup for network appliances.	2 business days
Phase 2	Threat detection and threat-intelligence validation across onboarded sources.	1 business day
Phase 3	Dashboards, alerting, and audit log export validation.	1 business day
Wrap-up	End-to-end validation, fine-tuning, knowledge transfer, and next-steps planning.	1 business day

Appendix D: Syslog Integration Approach for Firewalls

AccuKnox SIEM does not parse the Syslog protocol directly. For syslog-only sources such as Palo Alto Firewall and Cisco Meraki, AccuKnox uses a lightweight middleware VM to convert Syslog to JSON before ingestion.



Figure — Syslog-to-JSON middleware pipeline.

Step by step

- **1. Source configuration** — point the firewall or appliance’s dashboard to forward Syslog to the Syslog VM’s IP and port (default UDP/TCP 514).
- **2. Syslog VM setup** — deploy an Ubuntu VM in the same network segment or VPC as the source devices, and install Rsyslog to receive messages from all configured sources.
- **3. JSON conversion** — a script on the Syslog VM parses each incoming line and converts it to a JSON object (source IP, timestamp, event type, message body, device name).
- **4. Forward to AccuKnox SIEM** — the JSON payload is sent to AccuKnox SIEM’s ingestion endpoint via Bulk API or LogStash HTTP output.
- **5. Indexing & detection** — AccuKnox SIEM indexes events under the tenant namespace and applies detection rules — for example, port-scan and policy-violation detectors for Palo Alto, or client-association and unauthorized-SSID detectors for Meraki.

The Syslog VM is a small piece of onboarding infrastructure that lives in the customer’s environment; AccuKnox does not require inbound access to the customer’s network to operate it.

Appendix E: Azure Integration Detail

AccuKnox SIEM ingests Microsoft Azure telemetry natively, using an event-driven architecture built around Azure's own Diagnostic Settings and Event Hub services — no agent runs inside the customer's Azure environment.

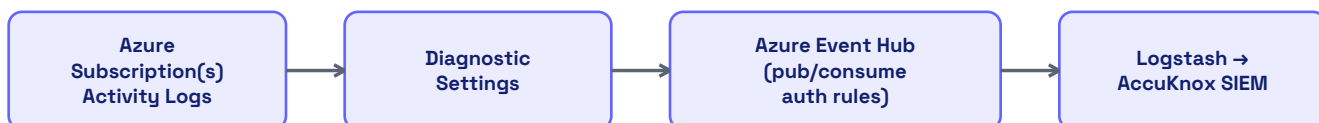


Figure — Azure Activity Logs ingestion pipeline.

Supported log categories

Azure Activity Logs are ingested across the following categories:

- Administrative
- Security
- ServiceHealth
- Alert
- Recommendation
- Policy
- Autoscale
- ResourceHealth

Ingestion architecture

- **Activity Logs → Diagnostic Settings:** Azure Activity Logs are configured via diagnostic settings to forward events for the log categories above.
- **Event Hub as message broker:** events route through an Azure Event Hub, which serves as the central collection point.
- **Authorization rules:** separate rules manage publishing (activity logs) and consuming (Logstash/AccuKnox) permissions, so Azure's publish path and AccuKnox's consume path are cleanly separated.

Core components deployed

Onboarding is Terraform-driven and deploys:

- An Event Hub Namespace
- An Event Hub instance
- Authorization Rule **"activity_logs"** — enables Azure services to publish messages
- Authorization Rule **"logstash"** — enables subscriber access for log processing

Multi-subscription support

The same pattern extends to additional subscriptions in an organization: diagnostic settings are configured across multiple subscription IDs, all routing into a single Event Hub for centralized collection — so a multi-subscription Azure estate onboards to one AccuKnox SIEM ingestion pipeline rather than one per subscription.

Detection coverage

The breadth of Activity Log categories spans identity, security events, resource changes, and alerts, giving out-of-the-box detectors visibility into administrative actions, security-relevant events, service and resource health, and policy/autoscale changes across an Azure tenant. As with AWS, GCP, and OCI, this can be extended with custom detectors tuned to an organization's specific Azure usage patterns (for example, Entra ID sign-in anomalies or Defender for Cloud alert correlation) as those sources are onboarded.