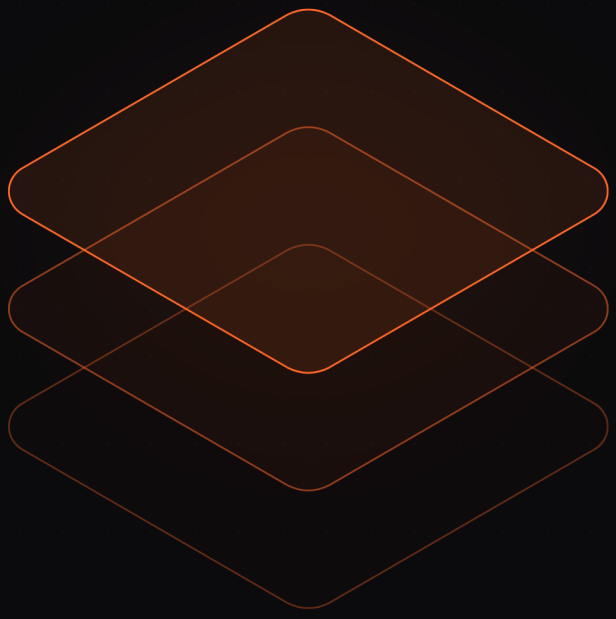
8Layers

PLATFORM SOLUTION BRIEF

8Layers.

Unified Identity Security & Continuous Compliance



September 2026

01

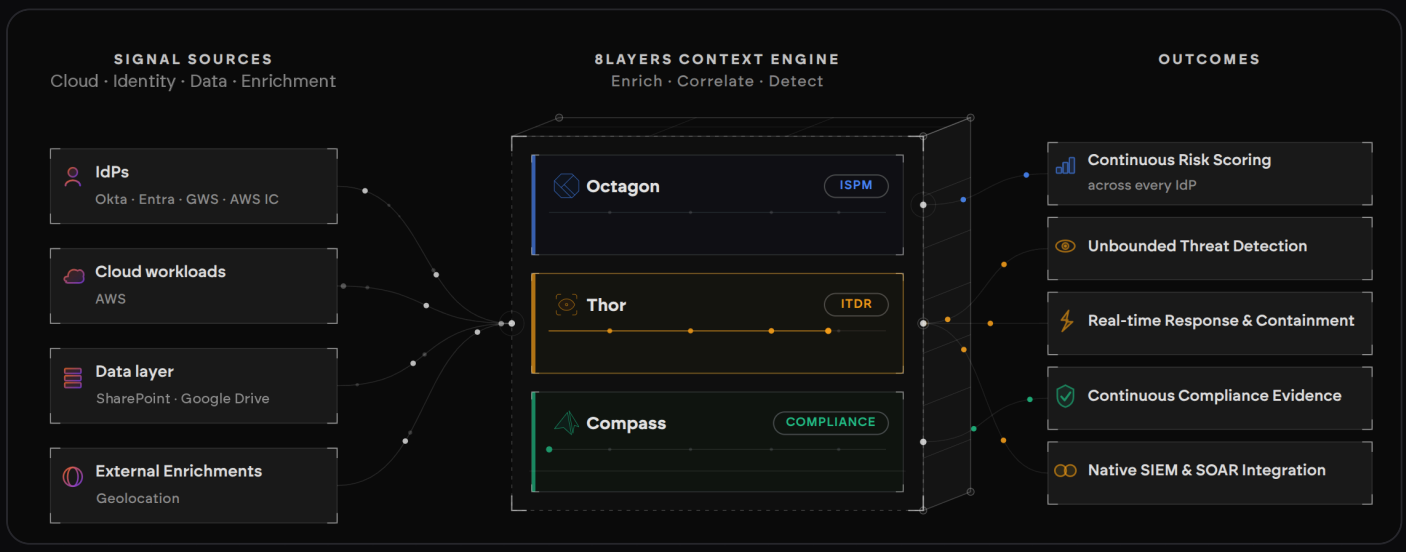
What is 8Layers?

8Layers is the integrated platform for securing the modern identity lifecycle and automating regulatory compliance.

By unifying **Identity Security Posture Management (ISPM)** and **Identity Threat Detection and Response (ITDR)** with **Continuous Compliance Validation**, 8Layers allows organizations to proactively reduce their attack surface, detect and respond to identity threats, and maintain a state of constant audit readiness.

The objective is simple:

Secure your identities, detect threats, and prove it 24/7.



THE PROBLEM WE SOLVE

Identity is the new perimeter, and it's the least protected one. Endpoints have EDR. Networks have NDR. But the credentials, sessions, service accounts, and OAuth apps that hold the keys to everything remain a blind spot.

That blind spot is exactly where attackers operate. They don't break in; they log in, then move slowly: a credential stolen in January, an escalation in June. Traditional tools usually can't connect those dots. And while security teams chase fragments, compliance teams scramble to prove controls they can't continuously verify.

THE THREE-MODULE ARCHITECTURE

8Layers delivers value through three integrated modules that share a common data plane:

Octagon	Active Identity Security. The engine for security posture and remediation (ISPM).
Thor	Identity Threat Detection and Response. The engine for detection, investigation, and containment (ITDR).
Compass	Continuous Compliance. The engine for audit readiness and governance.

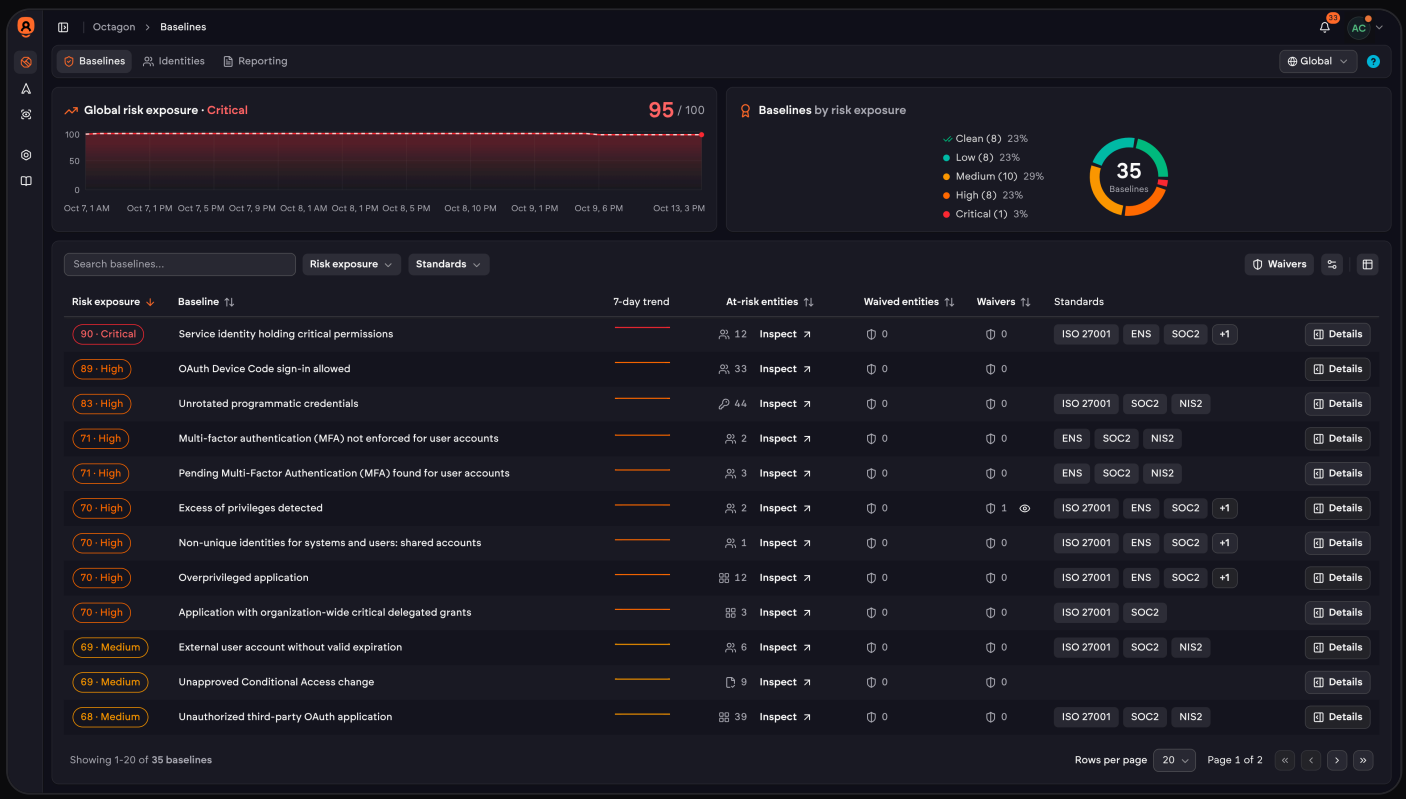
02

Octagon

Active Identity Security. The Engine for Security Posture & Remediation.

Octagon is an ISPM platform that inventories every human and non-human identity across all your IdPs, including AI agents. It continuously scores risk, prioritizes exposures, and remediates them directly from the console, with a full audit trail for every decision.

Octagon addresses the security incident response lifecycle from the standpoint of preparation. It unifies IASM (Attack Surface Management) and CAASM (Continuous Monitoring) to detect and fix risks before they can be exploited.



Octagon: organizational risk exposure and baseline posture

FEATURES

- **360° Identity Visibility**: Consolidates all Human and Non-Human Identities (NHI) from IdPs including Okta, Google Workspace, Microsoft Entra ID, AWS IAM and AWS Identity Center. It enriches every profile with automatic tags, roles, and permissions context including third-party OAuth apps, tokens and scopes. Full Multi-IdP support aggregates identities across multiple tenants and subsidiaries into a single source of truth.

- **Continuous Risk Detection**: Calculates a dynamic Risk Score (0-100) for every identity and the organization as a whole. It automatically detects misconfigurations, dormant accounts, and excessive privileges using Out-of-the-Box (OOB) Baselines enriched by continuous baseline evaluation.

- **Active Remediation & Tracking**: Turn observation into immediate action. Eliminate security findings instantly with "One-Click" Remediations. For complex scenarios, the platform empowers response analysts with prescriptive, step-by-step guides, and every run is tracked with its own history and outcome, cross-linked to the finding and baseline it addressed.

- **Containment Actions**: Stop attacks in their tracks (blocking users, ending sessions, resetting credentials, revoking risky OAuth access and disabling Entra ID devices) without leaving the console. For Non-Human Identities, containment actions are tailored by subtype.

- **Expanded Risk Baselines**: Continuously growing baseline coverage for identity risk, including dangerous or declared app-only permissions and delegated consents to over-privileged applications, plus a risk score exposed directly on every credential so the riskiest ones surface first.

- **Posture Reporting**: Generate comprehensive, AI-assisted posture reports summarizing identity risk exposure, baseline compliance status, and remediation progress. A dedicated report viewer offers **Summary** and **Actions** reports with recent run history and PDF export; reports generate automatically, can be **scheduled per organization** (incremental or extensive), and are delivered straight to your notification channels (Email, Jira).

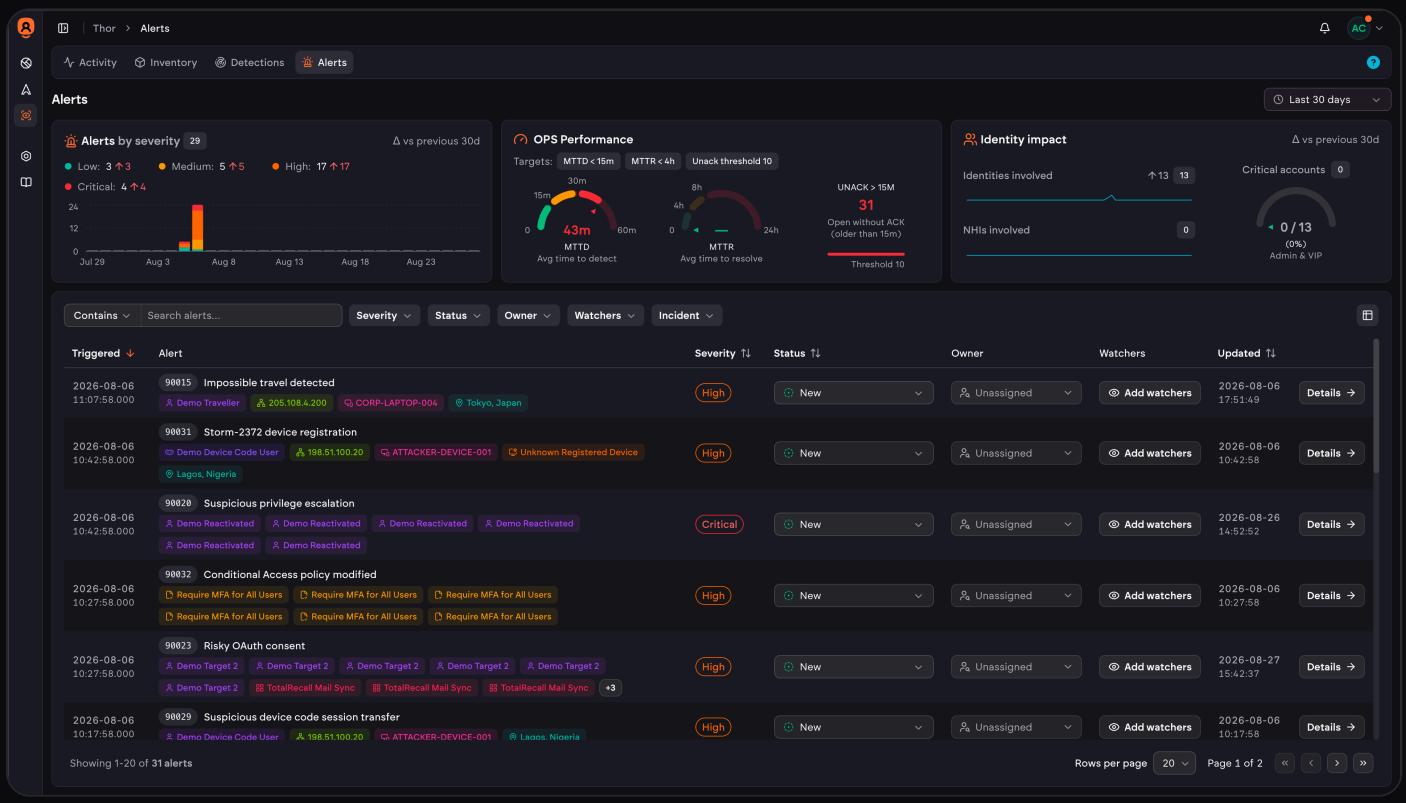
03

Thor

Identity Threat Detection and Response. The Engine for Detection, Investigation & Containment.

Thor is a real-time ITDR platform that detects identity threats across your full activity history. When a threat fires, it delivers a full timeline, a causality graph (Beta), and direct response actions.

Thor addresses the security incident response lifecycle from the standpoint of detection and response. It equips analysts with a unified workspace to hunt, detect, investigate, and contain identity-based threats.



Thor: alert overview with severity trend and OPS performance (MTTD/MTTR)

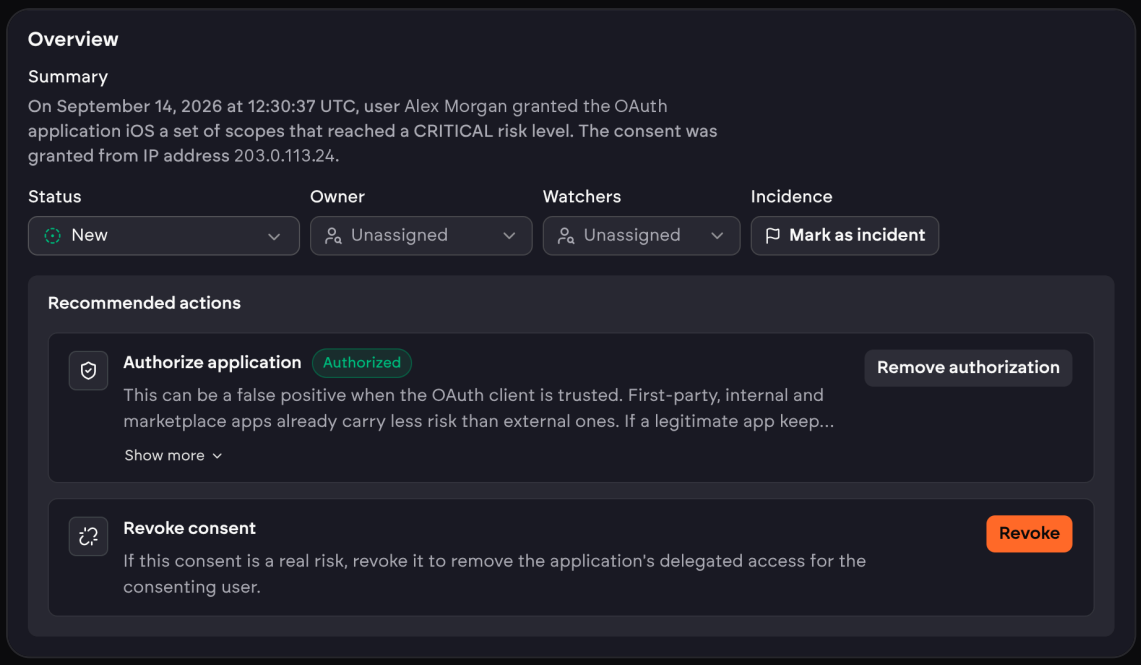
FEATURES

- **Detection Engine**: A growing library of OOB detections, each mapped to MITRE ATT&CK, covering the full identity kill chain: brute force, credential abuse, impossible travel, device-code phishing, privilege escalation, publicly exposed files, and protocol anomalies. Grouped detections automatically cluster correlated signals into consolidated alerts, while WatchLists and exclusion lists let analysts tune what each detection watches and what it ignores.

- **OAuth Consent Risk Detection**: Hardened detection for risky OAuth consent grants across Entra ID and Google Workspace, surfacing the underlying consent event, the scopes actually granted, and a clear risk rationale, with admin-level IdP consent kept distinct from the organization's own authorization.

- **Conditional Access Change Detection**: Detects and alerts on Conditional Access policy changes, with a drift baseline that links a modified policy back to the applications it governs.

- **Alert Triage & Lifecycle**: Structured alert workflows (assign, investigate, escalate, and close) with full audit trails, alert activity feeds, watchers, inline commenting, AI-powered alert enrichment, and ticketing to Jira / ServiceNow.

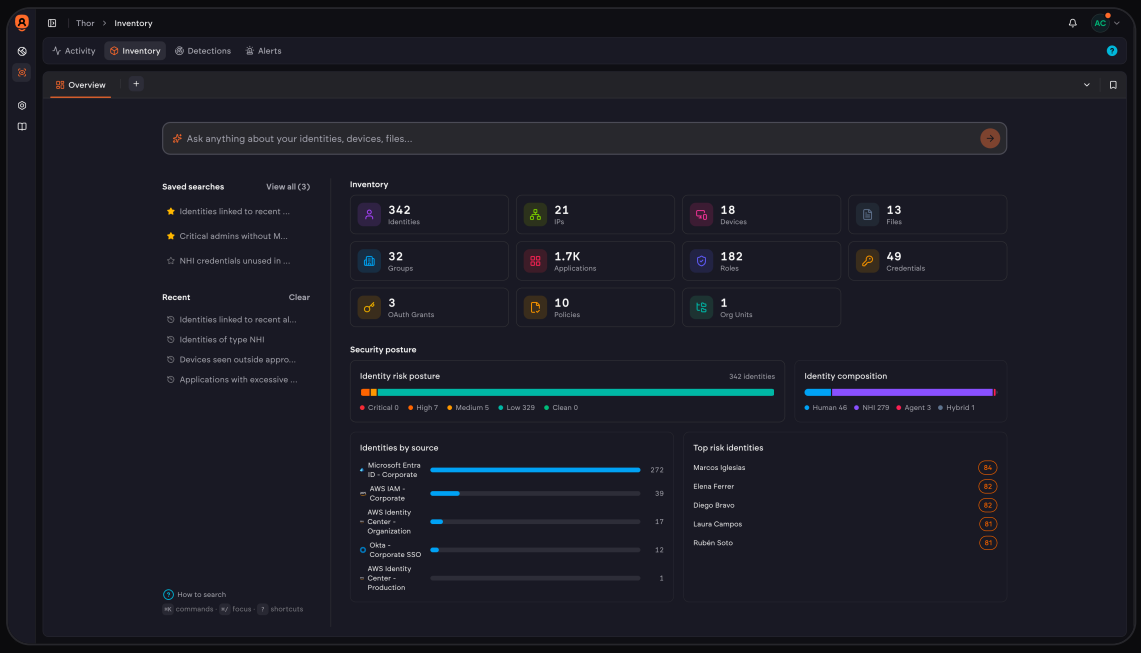


Alert detail: recommended actions next to the summary

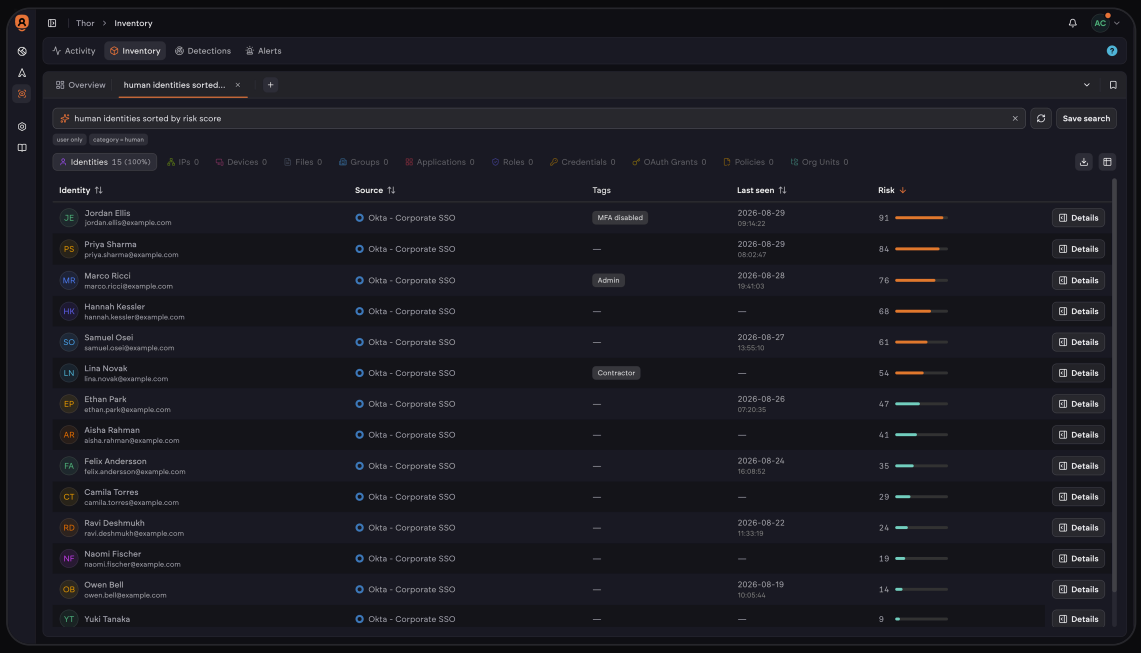
- **Automated Response**: Detection rules can trigger immediate containment actions: suspend user, revoke sessions, reset credentials, revoke a risky OAuth consent, or full containment.

- **Activity, Investigation & Hunt**: An activity workspace where alerts pivot into investigations, an identity graph on each alert (Beta) with nodes, edges, events, remediation and role/group/token context for reconstructing attack paths, plus Threat Hunting (Beta) with the IQL query language (filter by integration, actor, geolocation) and aggregation.

- **Identity Inventory & Search**: A unified inventory of every identity and entity (including applications, roles, groups, devices, files and IPs) queryable with **natural-language search** and saved searches for fast investigation and reporting.



Identity Inventory: natural-language search across identities, devices, files and more



Natural-language query resolved into a filtered inventory view

---

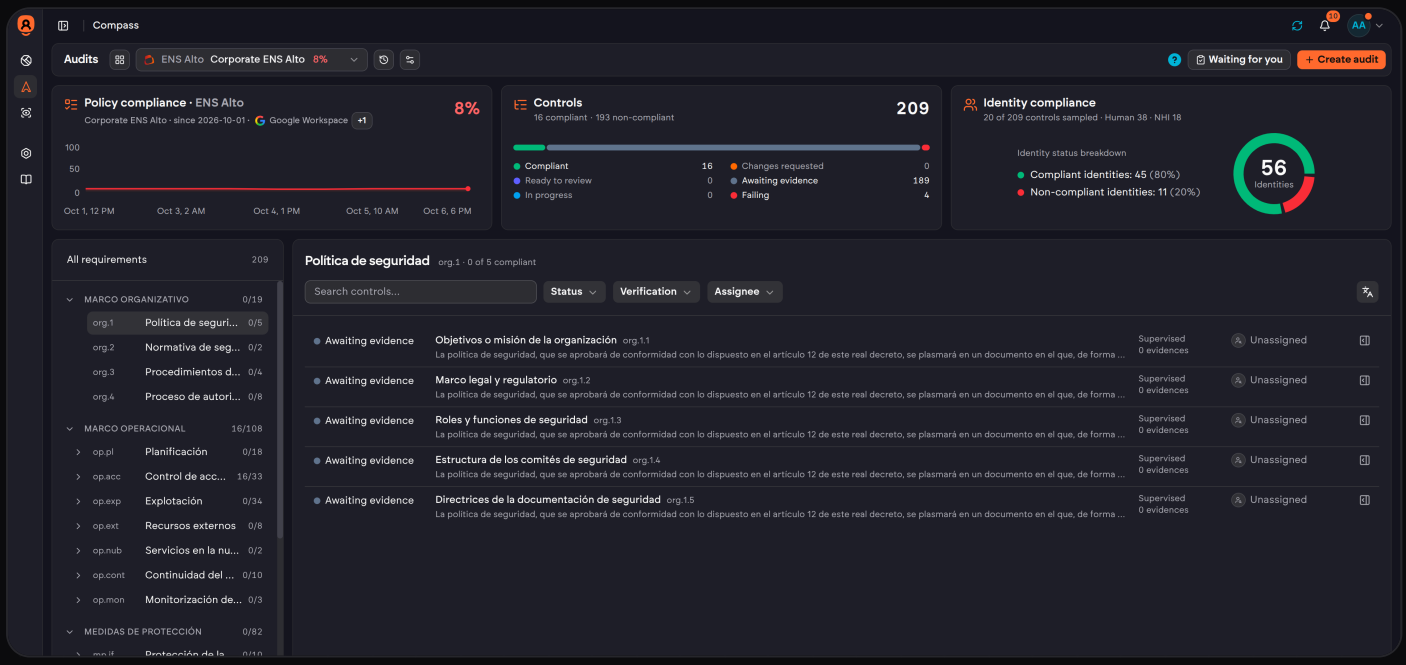
- **SIEM Integration**: Native alert forwarding to Splunk through HTTP Event Collector, and to other platforms through generic HTTP collectors.

04

Compass

Continuous Compliance. The Engine for Audit Readiness & Governance.

Compass maps your controls once against ENS, NIS2, ISO 27001, SOC 2 and CISA SCuBA, validates them continuously, and generates audit-ready evidence automatically. When an auditor arrives, the work is already done.



Compass: an audit with its control status, identity sampling and requirements

FEATURES

- **Multi-Framework Mapping**: "Test once, comply many." Compass maps technical controls to multiple standards simultaneously (ENS, ISO 27001, NIS2, SOC 2, CISA SCuBA). A single check automatically satisfies requirements across distinct regulations.

- **Automated Evidence Collection & Audits**: Replaces manual screenshots with automated, timestamped evidence logs. Compass validates technical controls 24/7 and runs audits that are reviewed control by control and handed over to the auditor as a snapshot with its report and workbook. External auditors get their own role to review the audit and decide on its controls.

- **Hybrid Governance**: Supports both automated checks and Manual Validation Workflows for non-technical requirements (policies, HR reviews), so they are covered in the same audit.

05

Why Unified? The Platform Advantage.

By running Octagon, Thor, and Compass on a single platform, 8Layers bridges the gap between Security Operations (SecOps) and Governance (GRC):

- **Unified Source of Truth**: No data discrepancies. The same inventory data used to identify vulnerable identities in Octagon and detect threats in Thor is used to prove compliance in Compass.

- **Smart Risk Acceptance (Waivers)**: A centralized waiver system applies across all modules. If you accept a risk in Octagon, Compass shows the exception beside the control it affects, so the auditor can tell a documented, accepted risk from a failure nobody has reviewed. The control's result is left as measured: weighing the accepted risk is the auditor's call. A waiver can cover named entities or a whole integration, stays current as new entities appear, and expires at an exact time.

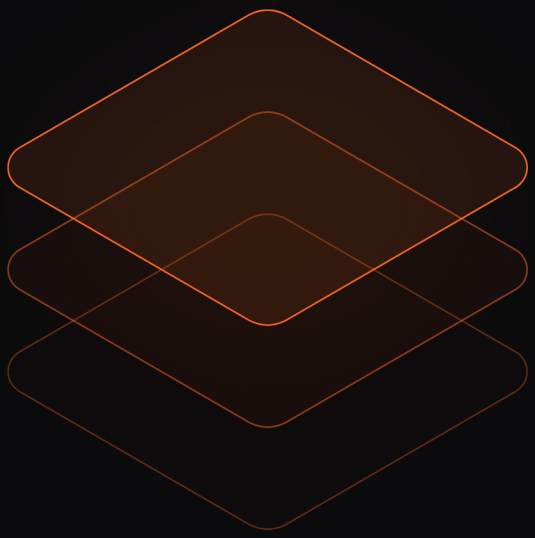
- **Real-Time Context**: Compliance drifts (e.g., "MFA disabled for Admin") surface continuously as actionable findings, allowing teams to fix the root cause rather than just reporting the failure.

Technical Specifications

Architecture	100% SaaS, Agentless.
Deployment	Connects via API in minutes.
Integrations	Native support for Okta, Google Workspace, Microsoft Entra ID, AWS IAM and AWS Identity Center. Okta, Google Workspace and Entra ID are read/write (one-click remediation and containment); AWS is read-only, with guided remediation.
Multi-Tenancy (MSSP)	Dedicated MSSP portal with per-tenant context and metrics, role-based access control (RBAC), a provider view over the tenants' Compass audits, and a management API: operate Octagon, Thor and Compass across multiple tenants.
Data API	Read-only access to identities, roles/groups, signals, events, enrichments, tags, containment history, alerts and Compass audits, with bulk export and natural-language-to-query. Enabled per organization.
SIEM Integration	Native alert forwarding to Splunk through HTTP Event Collector, and to other platforms through generic HTTP collectors.
Notification Channels	A single place to configure how security alerts are delivered and routed: Email, Jira, Microsoft Teams, Slack, ServiceNow, Splunk HEC, Torq, and generic HTTP collectors (webhooks to SOAR platforms and custom endpoints), with a configurable default method.
Data Model	OCSF-based, ensuring interoperability with SIEMs, data lakes, and third-party platforms.

8Layers.

If you'd like to assess how it fits within your organization or explore its capabilities in more depth, the 8Layers team is available to support you.



8Layers