aembit

Auditing and Governance in Modern Identity

How Aembit provides visibility and insights into workload identity, agents, and access.

The Audit Challenge in AI-First Infrastructure

Traditional identity audit frameworks assume humans make decisions at defined checkpoints. But modern infrastructure operates differently: workloads authenticate constantly with blended identities, mixing user context and system permissions, at scale and millisecond speed across systems not built to log them together. Organizations need visibility into what's happening: who or what is authenticating, what they're attempting, authorization status, and outcomes. This data must be granular enough to investigate anomalies, comprehensive for compliance audits, and integrated into existing security operations.

> **Aembit sits at the center of agent and workload identity and access enforcement, making it the natural place to capture and act on this audit and governance data.**

1. What We Log

Administrative Activity

- Policy changes
- Credential providers
- MCP configuration
- Team administration
- Integrations & settings

Workload & Agent Activity

- Workload authentication
- Agent requests
- Authorization decisions
- Credential issuance
- Access success / failure

aembit

Identity Control Plane

Authenticate

Authorize
Enforce Policy

Issue Just-in-Time
Credentials

Audit Event Generated
Every action. Every decision. Full context.

2. Rich Context Captured

Identity Context
User, workload, agent, roles, attributes

Resource Details
Target system, resource, environment

Authorization Outcome
Allow / Deny, policy ID, decision reason

Request & Response Metadata
Headers, parameters, status, direction, timestamps, more

3. Analyze & Report

Aembit Dashboard

- Real-time activity overview
- Authorization insights
- Policy enforcement visibility
- Troubleshooting & investigation

4. Export & Integrate

Amazon S3

Splunk

SIEM
Platforms

Stream all logs and audit data for long-term retention, correlation, alerting, and reporting.

5. Complementary Governance

Pair Aembit's enforcement and visibility with broader identity governance capabilities to:

- Define access policies
- Manage identity lifecycle
- Review and certify access
- Maintain compliance

Aembit enforces secure access and captures the complete audit trail.
Use your existing tools and processes to govern, analyze, and act on that data.

Comprehensive Logging of *Administrative and Operational Activity*

Admin Actions

Every administrative action in Aembit is logged with full context. Policy changes, credential provider configurations, MCP server integrations, authorization rules, and team management generate detailed audit trails. Each entry captures who made the change, when, what changed, and why—providing the record of intent and configuration for compliance audits and forensic investigation.

Workload and Agent Activity

Beyond administrative actions, Aembit logs every access request from workloads and agents with blended identity. This includes the identity attempting access, the resource requested, the authorization decision, and whether access succeeded. When agents operate with combined user and system contexts, logging captures both dimensions for visibility into agent-driven access patterns.

Rich Metadata and Transaction Headers

For every transaction, Aembit captures extensive metadata and headers in both directions. This includes the originating workload or user, target system, request and response metadata, authentication attributes, and contextual information. This depth of data enables tracing specific access patterns, correlating activity across systems, and understanding operational context for each request.

Visibility Through Dashboards and *Real-Time Insights*

Dashboard Analysis

Aembit's dashboard provides immediate visibility into access patterns, authorization decisions, and administrative changes. You can quickly identify access trends, spot authorization failures that may indicate misconfigurations, and track policy enforcement in real time. The dashboard is built to answer the questions auditors and security teams ask most often: What's being accessed? Who or what is accessing it? Are policies being enforced correctly?

MCP Authorization Tracing

For deeper agent access investigation, Aembit's MCP Authorization Tracing tool provides real-time insights into MCP transactions flowing through the Aembit MCP Authorization Service and MCP Gateway. This allows you to inspect individual MCP calls, understand authorization decisions at the transaction level, and debug access issues without waiting for log exports.

Practical *Applications*

1 ### Compliance Audits

Audit teams can pull comprehensive logs of who accessed what, when, and under what authorization policy. Admin logs show policy history. Transaction logs show enforcement.

2 ### Incident Response

When an incident involves workload or agent activity, Aembit's full transaction logs and metadata provide the complete context needed to understand what happened and what was accessed.

3 ### Access Reviews

Organizations often need to validate that access is still appropriate. Aembit's logs show exactly which agents and workloads have been active, what they accessed, and whether those patterns align with their intended purpose.

4 ### Policy Effectiveness

By analyzing the decisions Aembit made under your authorization policies, you can identify policies that are blocking legitimate access, policies that are too permissive, or patterns you hadn't anticipated.

Integration With Your Audit and SIEM Infrastructure

Aembit exports logs and audit data to data buckets and SIEM platforms, ensuring your identity access logs are available in the same systems you use for security analysis, incident response, and compliance reporting. This integration separates concerns cleanly: Aembit enforces workload identity and access in real time, captures the complete audit trail, and makes that data available to your security operations tools. Your SIEM and governance tools handle correlation, alerting, and retention.

Complementary to Identity Governance Programs

Aembit's strength is enforcement with detailed logging at the point of access. Organizations with broader identity governance programs will find that Aembit provides the operational detail and real-time insights necessary to understand what's actually happening with workload access, complementing policy definition and lifecycle management tools. By pairing Aembit with a comprehensive governance approach, you ensure that access policies are not only defined but enforced, audited, and understood.

Operational *Visibility*

Application Teams

Understand exactly how their services authenticate to every dependency.

Platform Teams

Validate that workload identity policies are being applied as designed.

DevOps

Catch authentication issues early, before they become operational incidents.

Next *Steps*

Aembit's audit and governance capabilities, including logging configuration, dashboard usage, data export to data stores and SIEM platforms, and MCP Authorization Tracing, are documented in detail at **docs.aembit.io**