

Omada Identity Cloud: Access Intelligence

Visibility and Control for Identity Access Governance



Identity-related breaches now account for the majority of security incidents (Verizon, 2025). Yet most organizations only discover excessive privileges after an audit finding or worse, after a breach. The problem accelerates as users change roles, cloud platforms multiply, and entitlements accumulate faster than governance teams can validate them. Every orphaned account and unreviewed privilege expands your attack surface.

Traditional role-based access control (RBAC) was designed to prevent this. But manual processes for defining and maintaining roles can't keep pace with organizational change. Roles become outdated, environments remain overentitled, certifications approve access that auditors cannot verify and compliance teams spend more time explaining exceptions than preventing them. The cycle repeats because visibility is static, analysis is periodic, and action is disconnected from insight.

Omada Access Intelligence breaks this cycle with a continuous, intelligence-driven model where visibility, analytics, and action reinforce each other. Built on Omada Identity Cloud, it unifies identity data across the enterprise, exposes where risk resides, and connects analytical insight directly to governed workflows. Each phase informs the next in a self-reinforcing loop: discovery provides the visibility to understand how access is used, analysis reveals where risk or inefficiency exists, and governance decisions drive actions that continuously improve access hygiene.

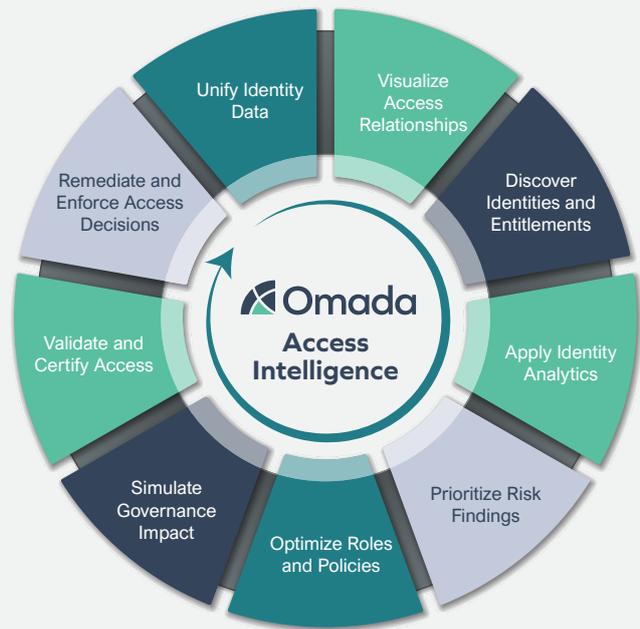
Introducing Omada's Access Intelligence

Omada Access Intelligence extends Omada Identity Cloud with an iterative loop of discovery, analysis, and action that connects visibility, intelligence, and governance into one repeatable process. Discovery consolidates identity data across your environment. This establishes clear visibility into how access is distributed and used. Analysis applies intelligence to reveal where risk or inefficiency exists. Action converts findings into governed remediation that feeds back into the loop, creating a sustainable rhythm of improvement where access data stays accurate and identity risk remains under control.

What makes this approach different from traditional role-based access control models is how the phases reinforce each other. Visibility improves with each cycle as dormant accounts are removed, and roles are refined. Intelligence becomes sharper as cleaner data reveals more meaningful patterns. Actions become faster and more confident as governance teams learn which insights drive the greatest risk reduction. Organizations move from discovering overentitlement after the fact to preventing it before it creates risk.

Omada Access Intelligence

Access Intelligence unifies visibility, analytics, and governance into one continuous cycle. Built on Omada Identity Cloud, it reveals how access is used, where risk exists, and what actions deliver the greatest impact. Access Intelligence helps organizations maintain a clean, governed state while continuously improving access accuracy, reducing exposure, and accelerating compliance with confidence.



Gain Visibility Across Identities and Entitlements

Access Intelligence consolidates accounts, entitlements, and roles from connected systems into a single, unified view of identity data. This eliminates the fragmented perspective that forces security teams to piece together access information from multiple sources. With all identity information connected, governance teams can answer the question of who has access to what and why with confidence rather than approximation.

Visual analytics reveal how entitlements align with business functions, where they diverge, and what the implications are for risk and compliance. Inconsistencies become visible: orphaned accounts, unused privileges, and access patterns that signal process gaps or policy violations.

This foundation of complete visibility enables governance teams to direct their attention strategically rather than reacting to whatever surfaces during the next audit. When every identity, account, and entitlement is visible in context, governance becomes proactive.

Apply Intelligence to Reveal Risk and Opportunity

Access Intelligence applies analytical insight to expose risk patterns that would remain hidden in the volume of entitlements. It highlights outliers such as dormant accounts, excessive privileges, and unusual access combinations, prioritizing findings that connect directly to measurable risk. For organizations managing RBAC, Access Intelligence evaluates role models to identify redundant, overly broad, or misaligned roles. Role simulations make it possible to test changes before deployment, validating that adjustments improve security without disrupting users.

This intelligence transforms governance into a continuous process of optimization rather than periodic remediation. Security teams identify and address problems as conditions change, aligning security outcomes with operational realities.

Act With Confidence Through Governance Workflows

Access Intelligence connects analytical results directly to Omada's governance workflows, enabling organizations to remediate issues efficiently and consistently. Teams can initiate targeted or bulk access requests and revocations based on verified findings, with every change following the appropriate policy path and maintaining a full audit trail.

Routine tasks can be automated to reduce manual workload while governance oversight ensures control remains where it matters most. High-risk scenarios stay within appropriate approval chains while low-risk changes that meet policy criteria move forward automatically.

For faster response, Omada's AI assistant, Javi, brings insights directly into Microsoft Teams or Slack so managers can review and approve actions within their everyday workspace. Every step remains transparent, traceable, and compliant.

Benefits of Omada Access Intelligence

Omada Access Intelligence delivers measurable improvement across the metrics that matter most to security leadership: reduced security incidents, fewer audit remarks, and demonstrable compliance readiness. Access landscapes become cleaner as dormant, and redundant accounts are systematically eliminated. Access reviews move faster because reviewers work from accurate, contextualized data. Audit findings decrease as governance controls tighten, and policy violations are addressed before they compound.

With Access Intelligence you will gain:

- **Unified Visibility:** Consolidates identity data into one authoritative view for faster, evidence-based decisions
- **Data-Driven Intelligence:** Detects anomalies, highlights risk, and pinpoints where access can be streamlined
- **Directed Remediation:** Converts insight into governed workflows that resolve issues quickly and visibly
- **AI-Enabled Automation:** Speeds reviews and approvals through Javi, reducing manual effort and human error
- **Continuous Optimization:** Keeps access clean and compliant as business and security needs evolve

Accelerate Your Path to a Clean, Governed State

Access Intelligence transforms identity governance from a periodic project into a living process that strengthens with each cycle. Built on Omada Identity Cloud, it continuously connects visibility, intelligence, and action, giving security organizations the clarity to see risk, the confidence to act decisively, and the control to sustain compliance as business needs evolve. Designed for both new and maturing programs, Access Intelligence provides the fastest, lowest-friction path to modernize IGA and achieve a clean, governed state with confidence.

Ready to take control of your identity landscape?

Schedule a demo today to see how Access Intelligence helps you gain visibility, reveal risk, and act with confidence.

