AppOmni

SOLUTION OVERVIEW

Secure Sensitive Legal Documents With Simplified SaaS Security for iManage

The Challenge

To prevent unauthorized access and protect sensitive documents, teams must establish constant oversight over the complex web of system settings, permissions, and role-based access controls (RBAC) in iManage. The intricate nature of iManage's global and library-specific resources — where users, roles, and groups exist both globally and within individual libraries — adds a layer of complexity that teams must navigate as they manage permissions. Properly established permission management helps organizations ensure that each of their users has the right level of access to only the documents that are necessary for each user's role.

To further complicate the process of maintaining iManage security, third-party app connections like Microsoft 365 and AI integrations introduce unique permission management challenges and expand the SaaS attack surface. In an integrated environment, a single oversight can lead to significant security issues such as data exposure and even non-compliance with security regulations. These challenges are further compounded by the lack of comprehensive monitoring tools and clear reporting, which make it difficult to apply security policies consistently.

The Solution

AppOmni integrates with iManage to provide a comprehensive SaaS security solution that is tailored to iManage's unique structure.

Simplify iManage security with AppOmni's clear view of all users — including both global and library-specific users — and any permissions they inherit.

Monitor your iManage posture with AppOmni's robust policy rules. These rules help teams track changes in permissions and can flag activity such as when a user assigns an admin-level permission like "Role Management." Policy rules cover a range of actions, including the creation of new groups, settings, libraries, roles, and specific permission assignments to roles or users.

THE CHALLENGE

- iManage settings are granular and complex
- Limited insights into dynamic permissions and policies
- Connections to other apps increase third-party risk
- Inadequate reporting results in inconsistent application of security policies

THE BENEFITS

- Continuously monitor your security posture, permission drift, and entity creation
- Gain a transparent view of user permissions
- Streamline access management and simplify configurations to reduce third-party risks
- Gain enhanced insights across user groups and permissions through reports

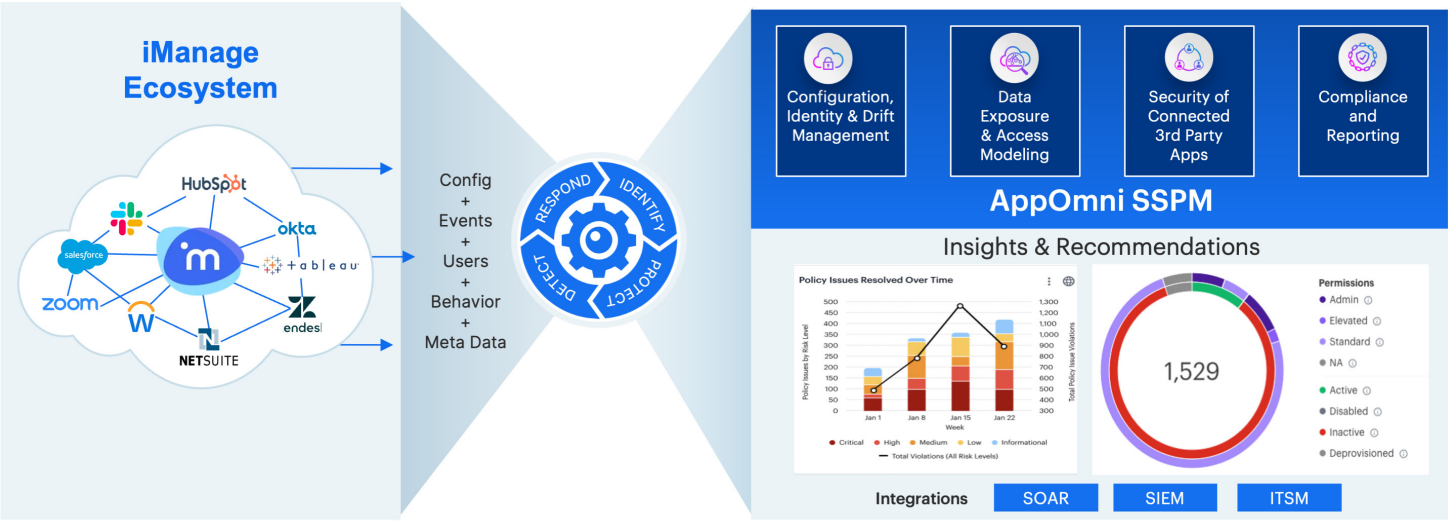
KEY CAPABILITIES

- Deep Visibility Into Permissions and Drift
- Continuous Monitoring and Alerting
- Critical Insights Through Reports
- Third-Party Connection Oversight
- SaaS Security Policy Management

AppOmni provides unprecedented transparency via four essential reports for iManage Monitored Services, which include details on users by group, library, role, and for those with elevated permissions. These reports collectively help maintain a secure and compliant document management environment because they help teams proactively manage the risk of data leaks or unauthorized access.

In addition to internal monitoring, AppOmni provides oversight of third-party applications that connect to your iManage environment. Visibility into third-party risks helps teams prevent unsanctioned SaaS-to-SaaS connections that could pose significant security risks.

Continuous Security Monitoring



Key Capabilities

Capability	Description	Use Case
Deep Visibility Into Permissions	Gain granular oversight of your iManage ecosystem at any scale. AppOmni provides deep insights into user permissions, which enable better management and security of sensitive documents and communications.	AppOmni provides a law firm with detailed insights into who has elevated or admin-level permissions to sensitive case files. This information helps the firm ensure that only authorized personnel can handle confidential client information.
Continuous Monitoring and Alerting	Continuous monitoring and advanced scanning capabilities detect risks early, allowing for a rapid response to potential security incidents in the iManage environment.	A financial institution uses AppOmni for continuous monitoring of iManage. AppOmni generates a policy violation alert when an employee is assigned an administrative level permission, and the organization deploys a rapid response to resolve the issue.

Capability	Description	Use Case
Critical Insights Through Reports	Report on users by group, library, role, or elevated permissions for a comprehensive overview of access control in iManage.	A mid-sized law firm utilizes AppOmni's reports to ensure that all Group members align with their organizational role to minimize the risk of insider threats.
Third-Party Connection Oversight	AppOmni offers comprehensive monitoring of third-party applications that interface with iManage to ensure that only authorized integrations are permitted. With third-party app oversight, organizations can reduce the risk of security breaches that occur through external connections.	A law firm safeguards its iManage environment by monitoring and controlling third-party SaaS apps with AppOmni. This approach to third-party app risks helps the firm restrict unauthorized integrations from gaining access to sensitive documents and data.
SaaS Security Policy Management	AppOmni acts as a central command center for security across your SaaS estate, translating and enforcing security policies across multiple SaaS applications.	A multinational bank with a complex SaaS stack applies consistent security policies across all apps. With AppOmni, the bank ensures that every user's access is subject to the same stringent security checks as in other financial systems.

About AppOmni

AppOmni is a leader in SaaS Security and enables customers to achieve secure productivity with their SaaS applications. With AppOmni, security teams and SaaS application owners quickly secure their mission-critical and sensitive data from attackers and insider threats. The AppOmni Platform continuously scans SaaS APIs, configurations, and ingested audit logs to deliver complete data access visibility, secure identities and SaaS-to-SaaS connections, detect threats, prioritize insights, and simplify compliance reporting. 25% of the Fortune 100 and global enterprises across industries trust AppOmni to secure their SaaS applications.

For more information, please visit appomni.com