AppOmni

SOLUTION OVERVIEW

Achieve Unified SaaS Security Management for Microsoft 365

The Challenge

Although Microsoft 365 appears cohesive, it comprises multiple services—each with their own unique security configurations. The fragmented management of services makes it difficult for security teams to maintain centralized visibility and ensure proper configurations across all services. Misconfigurations, overprivileged access, and inconsistently applied policies lead to data leaks and configuration drift.

Even if organizations use Microsoft's Entra ID and advanced E3 and E5 features, traditional SaaS security approaches often fail to deliver the necessary depth and breadth of threat detection and security controls. This lack of granular policy and rule customization prevent the ability to tailor security measures to the unique requirements of each law firm.

And without specialized SaaS expertise—including actionable insights and remediation guidance—it's challenging to proactively identify and mitigate vulnerabilities, consistently apply security policies, track user identities, and streamline compliance reporting across various standards.

The Solution

AppOmni consolidates visibility and control across all Microsoft 365 services, simplifies the detection of toxic combinations and misconfigurations, monitors configuration drift, and enforces security policies. This holistic approach allows teams to proactively identify vulnerabilities that arise from the complex interplay of different configurations and access permissions. By integrating with Microsoft Entra ID, AppOmni streamlines identity and access management to reduce the risk of unauthorized access and potential data breaches.

The platform's advanced analytics and continuous monitoring capabilities surface critical vulnerabilities, which enable security teams to proactively address issues. AppOmni also continuously monitors audit logs, exports normalized logs to existing SIEMs or SOARs, and provides near real-time alerts for potential threats like unauthorized access or unusual data activity.

THE CHALLENGE

- Multiple services with unique security configurations
- Difficult to avoid issues such as data leaks and configuration drift
- Inconsistent configurations across disparate services
- Complex compliance requirements

THE BENEFITS

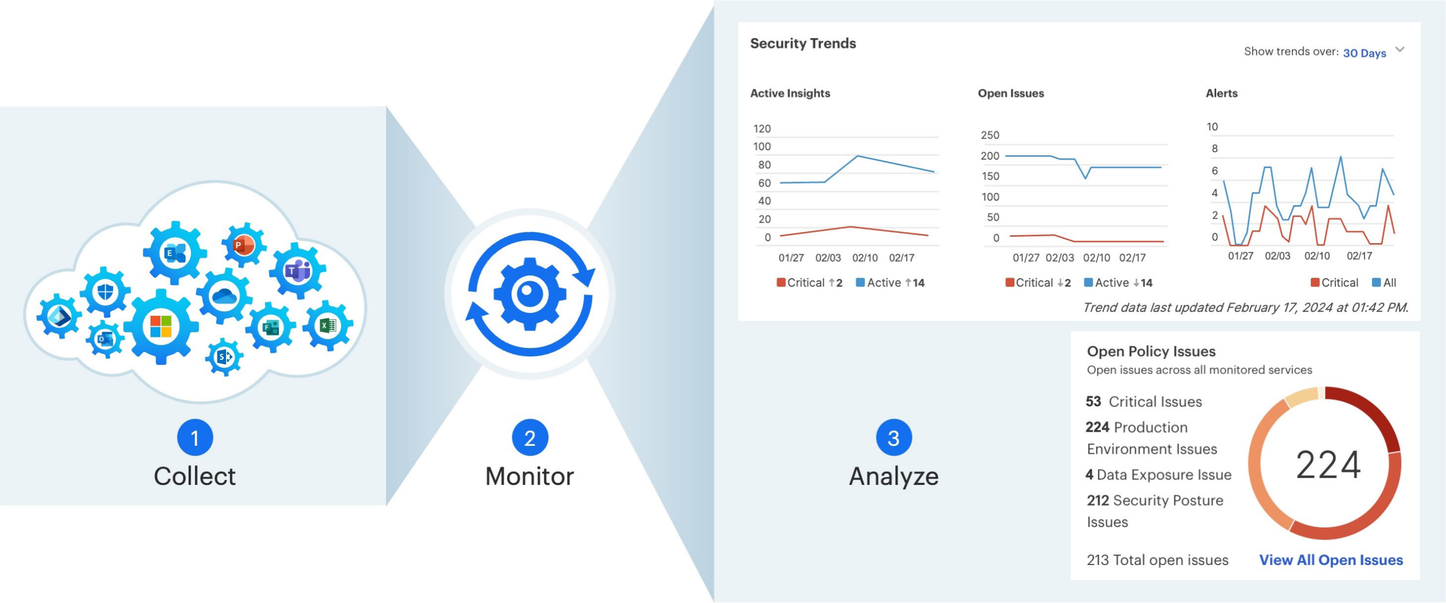
- Centralized visibility with a unified view of settings, roles, groups, users and identities
- Prevent drift and data leakage through policy configuration and continuous monitoring of security settings
- High-fidelity threat detection seamlessly integrates with existing SIEM
- Simplified compliance and ensure adherence to regulatory standards like SOX, ISO 27001, and NIST

KEY CAPABILITIES

- SharePoint Access Policies
- Identities Sync with Entra ID
- MFA Insights
- Automatically enforce CIS Benchmark 3.0

AppOmni's dual approach enhances overall security by combining proactive vulnerability identification with swift reactive threat detection and response. With the platform, organizations can get comprehensive protection for their Microsoft 365 environments.

Continuous Security Monitoring



Trend data last updated February 17, 2024 at 01:42 PM.

Open Policy Issues
Open issues across all monitored services

53 Critical Issues
224 Production Environment Issues
4 Data Exposure Issue
212 Security Posture Issues

213 Total open issues

Key Capabilities

Capability	Description	Use Case
SharePoint Access Policies	Monitor and control data access by creating block or allow access type policies to ensure that role groups adhere to your organization's data security policy.	A university prevents unauthorized sharing of research data by enforcing strict access controls. With these new access controls, there are zero data leaks that academic year.
Identities Sync With Entra ID	Make Entra ID SaaS-aware by synchronizing user identities with Entra ID for unified access control in Microsoft 365.	Through unified identity management, a hospital reduces the risk of unauthorized access due to inconsistent user identity data across platforms.

Capability	Description	Use Case
MFA Insights	Increase visibility into MFA configurations through Conditional Access Policies (CAPs) and detect admins and users with exclusions.	A healthcare provider uses MFA insights to audit Conditional Access Policies, which enable the organization to quickly identify and fix misconfigurations—thereby reducing the risk of a data breach.
Automatically Enforce CIS Benchmark 3.0	Automate the enforcement of CIS Benchmark 3.0 by continuously monitoring and evaluating policies to ensure that the organization follows Microsoft best practices at all times.	A retail company reduces security incidents by automating CIS Benchmark 3.0 compliance, which leads to a significant decrease in security incidents.

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