

SOLUTION OVERVIEW

Manage Security and Optimize Access in Microsoft 365

Microsoft 365 continues to grow in popularity and organizations worldwide consider Microsoft 365 to be a critical business application. However, with this rise in usage, unauthorized access to Microsoft 365 environments has become increasingly lucrative to motivated attackers.

Microsoft 365 appears to be a cohesive set of services neatly bundled together. But once you dig deeper, it becomes apparent that each service is unique, with a multitude of different security configurations and capabilities. Understanding the complexities and how to properly configure these settings is no small task.

Although Microsoft 365 provides several security features in its E3 and E5 products, security teams still lack centralized visibility. And most teams don't have the necessary expertise and time required to take full advantage of native security features. Companies must take a proactive approach to ensure their M365 environments, users, and data are protected.

AppOmni helps enterprises gain deep, centralized visibility to cybersecurity risk across their SaaS ecosystems, including Microsoft 365.

This enables security teams to discover misconfigurations and data access risk throughout their systems. With AppOmni, security and admin teams can quickly and efficiently discover, protect, monitor, and verify security and compliance in Microsoft 365.



for



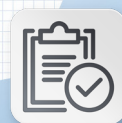
CENTRALIZED
RISK VISIBILITY



PROTECTION AND
REMEDiation



CONTINUOUS
MONITORING



VERIFY
COMPLIANCE

AppOmni enables organizations to quickly and easily improve the security of their Microsoft 365 environment while decreasing the workload of IT and security teams.



SOLUTION BENEFITS

- Increase awareness with centralized visibility of Microsoft 365 security posture using AppOmni Posture Explorer to see System Settings, Roles, Groups, and Users
- Gain visibility into which SharePoint sites and data are shared internally (all company) and publicly
- Detect data theft and manage Posture Policies for major Microsoft 365 modules including Exchange, SharePoint, Intune, Azure AD User settings, Mail transport rules, Conditional Access Policies, Identity settings, Defender for O365 settings
- See data access trends over time through tools like Persona and Historic Analysis
- Implement 21 in-product M365 specific security settings
- Go in-depth on Data Access for SharePoint sites, including new Policies, Access Explorer, and Role and Time-based comparisons
- Use AppOmni Insights to identify potential security risks. Insights are defined by AppOmni SaaS security experts and designed to make Microsoft 365 administrators experts in Microsoft 365 security
- Implement continuous monitoring to maintain Microsoft 365 security posture and hygiene
- Prevent data leaks through misconfiguration and oversharing of data from default sharing rules
- Continuous monitoring for configuration drift
- Convert a specific access scan result into a policy for continuous evaluation and maintenance of data access posture
- Review and triage policy violations
- Receive high-fidelity detection alerts in existing SIEM and collaboration tools to prioritize response
- Prove compliance with regulatory standards - CIS benchmarks, SOX, SOC 2, ISO 27001, NIST

SUPPORTED MICROSOFT 365 APPLICATIONS



Contact us to request a demo at <https://appomni.com/demo-request>

To learn more, email us at info@appomni.com or visit appomni.com.

AppOmni is a leading provider of SaaS Security Management software. Its patented technology scans APIs, security controls, and configuration settings to compare the current state of enterprise SaaS deployments against best practices and business intent. AppOmni makes it easy for security and IT teams to protect and monitor their entire SaaS environment from each vendor to every end-user.