AppOmni

SOLUTION BRIEF

HELPING YOU MANAGE SECURITY POSTURE AND RISK FOR Microsoft 365

DISCOVER

Empowering you to make informed decisions by providing a comprehensive and complete view of potential misconfigurations and data exposures for Microsoft O365

PROTECT

Providing you flexible and proactive enforcement policies and workflows for securing Microsoft O365

MONITOR

Helping you prevent posture and data access issues via consolidated monitoring and detection alerts and events for Microsoft O365

Microsoft is integral to your company. Their suite of services provide your users with communication and collaboration tools to help them effectively do their jobs. Luckily, they have you behind the curtains administering and protecting this environment.

And while you don't take these responsibilities lightly, balancing administration across all of these services requires a good deal of your time and effort. At times, it is challenging to keep up with the nuances and potential risks of all the services and configurations. You find yourself trying to balance business use cases, risk mitigation, and compliance requirements. We feel for you, it can be overwhelming.

EMBED AN EXPERT

From a macro view, Microsoft 365 appears to be a cohesive set of services neatly bundled together. However, once you start digging under the covers, it quickly becomes apparent that each service is unique with a multitude of configurations and capabilities. Understanding these complexities and how to properly configure these settings is not a trivial task.

DISCOVER GAPS AND PRIORITIZE EFFORT

We know that IT and Security teams have a limited amount of time but a limitless amount of priorities. As you continue to expand your usage of Microsoft 365, you will inherently be met with trade-offs between prioritizing business use cases and system administration.

AppOmni allows you to discover where these trade-offs may occur. By connecting via an account-wide OAuth grant, which only requires read-only scopes, we have the ability to read directory data, groups, organizational policies, and usage reports. No installation package needed, it's that easy!

From there, you can easily determine what configurations pose a risk to your company based on regulatory requirements — SOX, SOC2, ISO 27001 and NIST security frameworks. You can also quickly gain visibility into 50+ systems configuration settings, group/team settings, and installed third-party apps with our recommended best practice settings.

By arming yourself with these data points, you will have increased visibility of the risks to your company as well as being empowered to make more informed prioritization decisions.

CONSISTENTLY APPLY SECURITY FUNDAMENTALS

With all the services that are rolled under the Microsoft 365 banner, having consistency when applying security best practices becomes rigorous and time-consuming. This often leads to either overly permissive access or a locked down environment which decreases employee productivity. To compound this, Role-Based Access Controls (RBAC) across Microsoft 365 services can be independent and varied. Simply meaning, you could have unique admin accounts floating around.

PROTECT YOUR INVESTMENT, GAIN PEACE OF MIND

Microsoft 365 provides a ton of functionality and with that comes additional administration complexity. We know that it is challenging to track and manage users permissions and their data access capabilities.

Our approach starts with giving you a high-level view of your Microsoft 365 environment. This allows you to quickly detect misconfigurations and inadvertent or malicious disclosure of data. We focus on abstracting away the noise and complexity and provide you guidance based on our SaaS security expertise. Our Risk Dashboard provides a birds-eye view that highlights these configuration issues so you know exactly where to focus your efforts.

Your team can then leverage our Security Posture Policies, like ensuring all users have MFA and lockout thresholds, to enforce configuration settings that strengthen your security posture. You also have the ability to decrease administrative overhead by enacting policies that allow decentralization of configurations while aligning to your organization's risk tolerance.

UNIFY MONITORING AND DETECTION

Reading over the Office 365 Management Activity API schema it quickly becomes apparent that each Microsoft 365 service has a different way of providing event and log information. Obtaining holistic visibility in a standardized format is not a minor undertaking and takes teams a lot of time to configure. While there are a couple of recommended approaches, they can be error prone and largely fall short of being able to deliver much value. Unfortunately this dissuades teams from capturing these logs, which invariably creates a general lack of visibility for Security and IT teams.

MICROSOFT OFFICE 365 MONITORING MADE EASY

The AppOmni team is composed of security practitioners who deeply understand the power of high fidelity alerting. We focus on providing you with actionable Microsoft 365 alert data so you can focus your response efforts accordingly.

We do this by consuming event logs from your Microsoft 365 environment, which include 40+ event categories ranging from Advanced eDiscovery to Workplace Analytics. We then take the time to normalize these events to Elastic Common Schema (ECS) format which allows you to build detection rules based on your existing security monitoring technologies.

Our intention is to save you a ton of time by providing you the right information in the right format. You can act on this information either through AppOmni's automated workflows and policy enforcement capabilities or through leveraging the extensibility of AppOmni to tie into your existing processes. This will allow you to quickly understand issues in your environment and drive resolution.