AppOmni

SOLUTIONS OVERVIEW

Secure Your Github Platform with AppOmni

Github boasts a community of 50MM developers and hosts over a million software repositories. It is relied on daily by Fortune 500 companies to build amazing things together.

Github is a core component to how companies work together to build software. For many, source code is a part of their 'secret sauce' and security teams are chartered with, and strive to, protect this intellectual property. They are often met with challenges around determining access, understanding integration sprawl, and determining the overarching risks that could lead to an issue.

SURFACE INFORMATION QUICKLY

Github org administration requires depth of knowledge and familiarity to properly navigate settings and administrative actions. This level of expertise creates a large learning gap for peripheral service users such as Security and IT teams.

Timely Access and Setting Discovery

AppOmni helps you uncover and answer key questions about your Github environment that have been inherently challenging to accomplish with existing functionality. Getting started is as straight-forward as installing the AppOmni app from the Github marketplace.

Once connected, a scan of your Github environment will be conducted. You will be provided with visibility across a wide array of settings and configurations. These include org settings, repo settings, users and teams information and repository access. You can now definitively answer key questions such as; does my organization have safe defaults for new repositories and new users as well as how many of my repositories are public.

DISCOVER
Make informed decisions with a comprehensive view of misconfigurations and data exposures.

PROTECT
Create and apply flexible and proactive enforcement policies and workflows.

MONITOR
Receive high-fidelity detection alerts and ensure protection with continuous monitoring.

ENSURE ACCIDENTS DON'T HAPPEN

Github is one of the best and most secure places to store your code. However, it can be all too easy to accidentally add the wrong user to an organization, or to a repository.

Ptotect with Proactive Policies

Unfortunately, companies are made aware of an issue only after it has become a problem. Staying ahead of these issues requires a proactive approach to ensuring requirements, both business and regulatory, are adhered to and upheld.

With AppOmni, teams can create policies to ensure they are timely notified of deviations from their intended secure behavior. This could include notification of a repository access grant to an external domain user or if any repositories are switched from private to public.

Our focus is to provide both a broad and deep set of rule and policy capabilities. At the org level, policies range from installed apps to default repository permissions. To complement org level capabilities, AppOmni also provides granular rule and policy options at the user, team, and repository level.

Our intention is to provide you an approachable and intuitive set of policy functionality to alleviate administrative overhead and proactively protect your Github environment.

WHO HAS ACCESS TO CODE

Being able to quickly determine user and team access to repositories is not very convenient. It requires traversing repositories and then manually linking users and teams to those repositories.

MONITOR EACH REPOSITORY

Hopefully we can agree that not all repositories are created equal. Most companies have a set of baseline repositories that any developer or engineer would need in order to build software. There are also likely business unit repositories that would require limited team access. And at the most granular level, repository access that needs to provisioned at the individual level. With constant change, this level of management is highly complex.

Fear not, with AppOmni you can easily monitor user and team level repository access. Quickly determine what access a user will be provided if they are added to a team and what repository access teams are provisioned. Looking for better ways to curb one-off access or snowflake environments. Monitor for deviations from your established user and team access model.

Another powerful monitoring option is timely notification of access grants to restricted or confidential repositories. Receive alerts any time a new user is added and create custom workflows to the teams in charge of managing access.

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.

AppOmni