AXONIUS FEDERAL
SaaS MANAGEMENT

SaaS MANAGEMENT

SaaS applications like Slack, Zoom, Google Workspace, Workday, and others have become mainstays in the federal world. Employees appreciate the increased productivity, accessibility, and flexibility these tools offer.

Unfortunately, these applications also pose challenges for IT and security professionals, particularly when it comes to data sprawl and cybersecurity. That's why the Cybersecurity and Infrastructure Agency published its Secure Cloud Business Applications (SCuBA) project – to provide clarification on how to manage SaaS risk. The project is part of an effort to implement Executive Order 14028, Improving the Nation's Cybersecurity.

Axonius SaaS Management can help your agency adhere to this and similar guidelines by addressing existing SaaS challenges across multiple layers. It can help you discover all your known and unknown SaaS applications, identify misconfigurations and data security risks, and deliver insights for better IT management and cost optimization.

KEY BENEFITS FOR IT AND SECURITY PROFESSIONALS

Identify Shadow SaaS and Risky Accounts

Identify your unsanctioned, shadow, and unmanaged SaaS Applications, 3rd/4th party extensions, and Oauth tokens. Uncover users with excessive permissions, or who access apps outside of sanctioned SSO and authentication protocols.

Discover and Close Configuration Gaps

Quickly assess security risks that put sensitive data at risk, including misconfigured SaaS app settings, SaaS provider compliance gaps, and risky access and behavior.

> SOFTWARE-AS-A-SERVICE (SAAS) WILL LIKELY BECOME THE MORE PREVALENT WAY OF USING SOFTWARE. THIS MEANS LESS DOWNLOADING AND INSTALLING ON ENDPOINT DEVICES LIKE LAPTOPS OR PHONES AND MORE ACCESS THROUGH API OR DIRECT CONNECTION THROUGH THE INTERNET.
>
> *DIRECTOR OF SECURITY AND PRIVACY COMPLIANCE AT A MAJOR FEDERAL HEALTHCARE AGENCY*

Control Costs and Optimize SaaS Licensing

Optimize SaaS spend with data insights into licensing and utilization, redundant SaaS apps, and shadow apps and users.

Understand SaaS App Utilization

Gain a credible SaaS inventory and understand the full scope of SaaS applications and their utilization within the organization, including app usage, exact user counts, and asset ownership.

Gain Visibility and Address Existing Security Risks

View an extensive breakdown of existing app settings, misconfigurations, and vulnerabilities combined with extensive guidance on mitigation steps, and built-in remediation options.

Mitigate Identity and Access Issues

Identify SaaS users that access apps outside of sanctioned SSO and authentication mechanisms to improve your organization's security.

Detect and Investigate Suspicious Behavior

Axonius offers granular visibility into user behavior within SaaS apps and uncovers any suspicious activity, events, and complex behavioral patterns.

Assess Compliance Levels

Understand how various apps adhere to existing frameworks and certifications, facilitating reporting on business unit compliance and vendor risk.

Axonius gives customers the confidence to control complexity by mitigating threats, navigating risk, automating response actions, and informing business-level strategy. With solutions for both cyber asset attack surface management (CAASM) and SaaS management, Axonius is deployed in minutes and integrates with hundreds of data sources to provide a comprehensive asset inventory, uncover gaps, and automatically validate and enforce policies.

AXONIUS FEDERAL

Interested in what Axonius can do for you?

LET'S TALK