

# Taking a SaaS Security LifeCycle Approach for the Largest Enterprises Globally



## APPOMNI'S IMPACT



**Deep visibility into business-critical SaaS apps**, providing the full picture of SaaS security posture.



A single, **easy-to-use platform** designed for any role in security.



**Clear visualization of the entire SaaS estate**, including what specific data is shared by which apps.



A programmatic approach to SaaS security with a **full lifecycle system built by the industry leader in SaaS cybersecurity**.



**Productivity gains are achieved without sacrificing security posture** by addressing the concerns and needs of business and IT stakeholders.

## TRACE3

### INDUSTRY

IT Value Added Reseller & Services Provider

### EMPLOYEES

1,300+

### HQ

Irvine, CA

### DEPLOYMENT

AppOmni SSPM Platform

### USE CASES

SaaS Data Protection  
SaaS Security Posture Management  
SaaS Data Security  
SaaS-to-SaaS Cyber Risk

### ABOUT TRACE3

Trace3 is a pioneer in the technology consulting space. Its mission is to empower IT executives and their organizations through a combination of leading technology solutions and elite consulting services.



If we didn't have AppOmni, we would be struggling to address SaaS cyber risk comprehensively for our customers. It's been a long-standing security challenge to ensure that the right permissions, identities, entitlements, data access monitoring, and governance for all SaaS apps are delivered within a full-life cycle methodology, regardless of scale or SaaS app complexity.

**Mark Butler**  
Advisory CISO, Trace3

## The Challenge

Trace3 is a leading transformative IT authority, providing unique technology solutions and consulting services to clients in healthcare, finance, technology, and a variety of industries.

Trace3 Advisory CISO Mark Butler is a veteran in the security space. He applies his expertise to help the leading enterprises address cyber risk across data, cloud, and security disciplines, positioning him to observe the trends in cybersecurity and how security teams must pivot to effectively manage emerging cyber risks.

Butler has noticed with increasing frequency that many organizations are struggling to adequately assess, prioritize, and remediate their SaaS cyber risks and vulnerabilities. This challenge stems from how quickly SaaS applications have become not only ubiquitous but also essential for any enterprise.

Take, for example, applications such as Salesforce, ServiceNow, Workday, and GitHub. These enterprise SaaS solutions typically have hundreds of integrated applications that touch sensitive company and customer data. Ensuring permissions are correctly granted for external users is essential, but applying correct permissions to internal users is vital as this group poses as much — if not more — risk than external users.

Butler is finding more and more organizations are realizing their legacy security tools only provide surface-level [SaaS security capabilities](#) and cannot offer the depth needed to offer complete visibility into their SaaS estate. Butler states:

“Data Loss Prevention (DLP) solutions, Cloud Access Security Brokers (CASB), and Security Web Gateways (SWG) are all trying to get at the issue. But they don’t really have the inspection capabilities or the permissions intelligence to understand what’s been provisioned and how that can cascade, or result in a set of permissions that ultimately leads to issues with data access, over exposure, and data sharing that needs to be addressed.”

To keep these business-critical applications running smoothly and securely, security teams are essentially trying to recruit security SMEs for each business-critical app. A team of experts is required to run the apps, and an additional team of experts is needed to configure the correct permissions and ensure only the right users are granted access to the sensitive data in these



AppOmni has surprised me in how quickly proof of value is shown from the initial conversation through purchase. AppOmni is one of our top cloud security partners. And there’s really nobody else in this space that’s leading the SaaS security conversations like AppOmni.

**Mark Butler**

Advisory CISO, Trace3

apps. This burdensome process for SaaS security and oversight is financially infeasible and unsustainable.

Between the lack of depth offered by legacy security products and the vast differences in complexities between each SaaS app, knowing what data security risk is contained in each SaaS app becomes nearly impossible. Butler also notes that stakeholder ownership over SaaS security is often unclear due to the decentralized nature of SaaS adoption, opening organizations up to further cyber risk.

All of these issues are subsets of the greatest challenge Butler has found: neglecting a complete lifecycle approach to SaaS security. He explains that:

“Whether you’re a startup using Google Suite or an organization that has migrated from on-premise Exchange to the cloud, all organizations are really starting to feel the heat. Not only from an auditor perspective, but from a governance program or SaaS security lifecycle approach. We are finding that most clients just don’t have a program in place – and it’s pretty obvious. They may have some limited visibility into what apps are in use, but they don’t necessarily have those apps integrated into entitlement reviews, recurring security approval, real-time monitoring, or permission reapproval processes.”

Butler continues that the absence of a lifecycle approach to SaaS security will result in an incomplete and piecemeal view of SaaS cyber risk. A lifecycle approach to SaaS cybersecurity provides a comprehensive, risk-based view of an organization’s SaaS estate that can be measured in real-time and historically.

## Requirements

Trace3 selected AppOmni as a strategic technology partner based on AppOmni's enterprise readiness. Butler states, "AppOmni's respect for the complexity of what it takes to get things done within an organization makes them one of our top partners. One of the biggest challenges of SaaS security is determining who owns it, and AppOmni is able to navigate multiple stakeholders by telling a story that makes sense across the entire organization – resulting in a positive relationship-building experience and obtaining the appropriate funding required to solve the problem."

Must-have capabilities for Trace3 include:

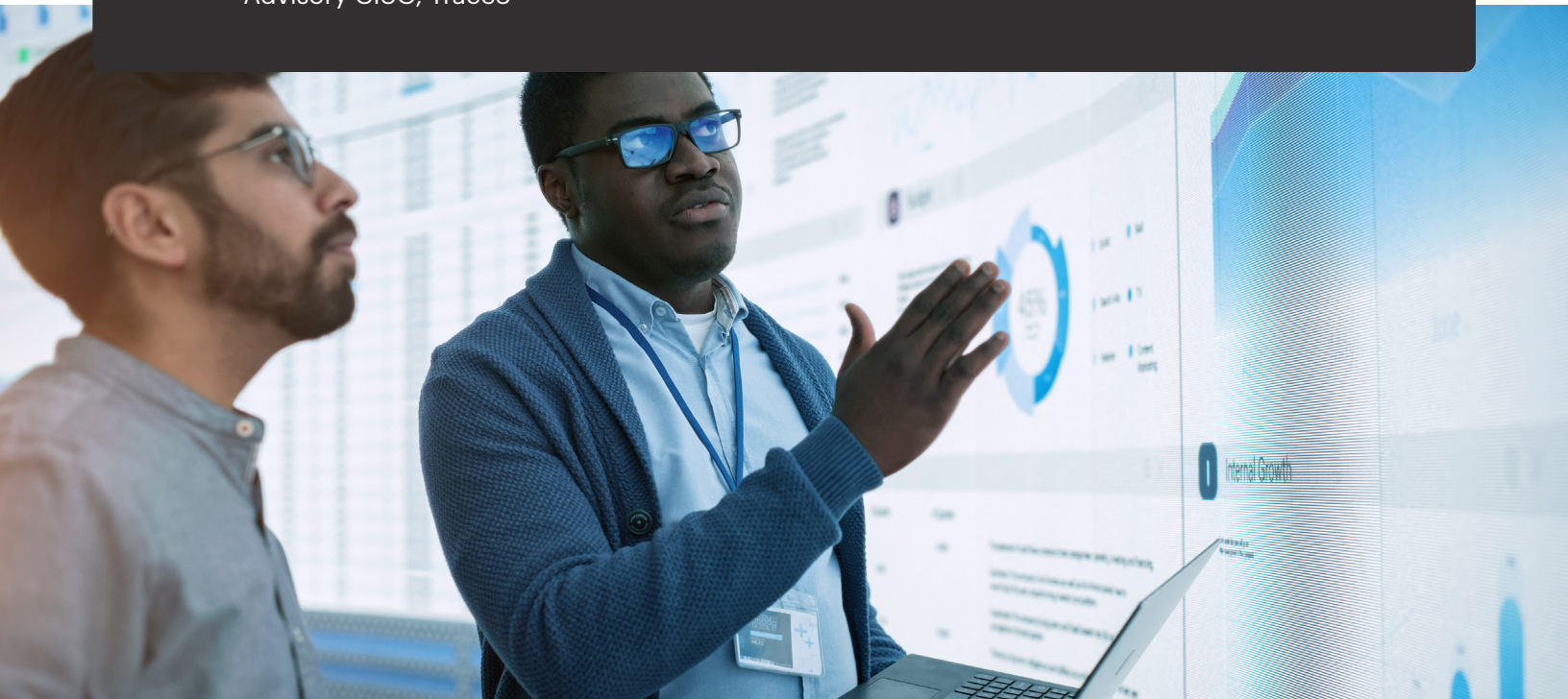
- SaaS security lifecycle with a programmatic approach
- Depth of SaaS Security Posture Management (SSPM) coverage for core SaaS apps
- Highly experienced partner, technology, and management teams



It's been refreshing to work with AppOmni. There's a SaaS security lifecycle strategy that includes tooling along with processes to inventory, define, and monitor data access permissions; perform identity risk analysis; and properly govern them over time. All of these categories need continual focus so that SaaS can be delivered, operated, and securely maintained. AppOmni understands the enterprise complexities and delivers a holistic lifecycle approach for our customers, which has been the best partner experience.

### Mark Butler

Advisory CISO, Trace3





## The Results

By working closely with the AppOmni team, Trace3 is providing its largest customers with end-to-end SaaS Security Lifecycle Management programs, operationalization success, and the intended value of their SSPM investments. Trace3 customers are building sustainable SaaS security programs that incorporate full visibility, continuous drift monitoring, identity correlation, data access reviews, and remediation integration with existing forensics, threat intelligence, and incident response (IR) processes.

Internal or external auditors alike are no longer satisfied knowing just what SaaS apps are in use, according to Butler. They are expecting organizations to continuously monitor usage to reduce licensing spend where possible, refine permissions to only what is needed for business purposes, and establish repeatable processes for continuous cyber risk reduction. AppOmni understands the bigger picture and helps its partners achieve the continually raising bar for SaaS security standards.

Butler recognizes AppOmni for defining the SSPM market and what's possible for SaaS security. Unlike other SSPM vendors, Butler notes that AppOmni possesses the requisite leadership expertise and product engineering discipline to be successful in large, complex matrixed organizations where stakeholder ownership and accountability is ambiguous for SaaS applications.

When considering the value AppOmni brings to SaaS data security, Butler states, "AppOmni will help you solve the risks you never knew about that could result in a breach or data exposure. The AppOmni platform solves this in a painless and efficient way." He concludes, "AppOmni as a partner helps to shift the entire paradigm of the conversation with multiple stakeholders by showing risk analysis data upfront. This allows us to go to our clients and share the results of analyzed permissions from a risk-based perspective. We are then able to put a plan into place to programmatically improve the SaaS security posture of the organization."



The biggest shortcomings of legacy security tools applied to SaaS are the lack of deep permissions, deep identity analysis, and awareness of real user access from a data perspective. AppOmni understands the intricacies of business-critical apps like Salesforce, Workday, and GitHub — and offers coverage for all of them in a single platform.

**Mark Butler**  
Advisory CISO, Trace3

### About AppOmni

AppOmni is the pioneer of SaaS Security Posture Management enabling 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 constantly 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. Over 25% of the Fortune 100 and global enterprises across industries trust AppOmni to secure their SaaS applications. For more information, please visit <https://appomni.com>.