black hat WEBINARS

No More Acronyms – Let’s Solve Problems: Putting CAASM and SSPM Aside to Talk Real Use Cases

Sean Blenkhorn, Vice President of Sales Engineering, Axonius

Moderator: Terry Sweeney, Contributing Editor, Black Hat

October 12, 2023

KEY TAKEAWAYS

- Rapid technology innovation and adoption drives the need for new security solution sets.
- CAASM and SSPM independently increase visibility for improved security.
- Axonius brings CAASM and SSPM together to secure complex environments.

in partnership with

AXONIUS

OVERVIEW

In increasingly complex IT environments, security practitioners need comprehensive visibility of assets to reduce risk and protect the attack surface. Rather than relying on isolated tools for separate teams that only create more silos, what's needed instead is a single solution that aggregates and contextualizes data from across the environment—including devices, users, software, SaaS apps, and other data sources—to provide real value for security practitioners. And two emerging security categories—Cyber Asset Attack Surface Management (CAASM) and SaaS Security Posture Management (SSPM)—do exactly that.

And while the security community doesn't need another acronym to define the very real-world problems they face on a day-to-day basis, CAASM and SSPM solutions have proven to be useful. Especially when combined within a unified platform.

Axonius, which combines industry-pioneering solutions in CAASM, SSPM, and SaaS Management Platforms (SMP), gives customers a comprehensive understanding of all assets, their relationships, and business-level context. By connecting to hundreds of data sources and aggregating, normalizing, deduplicating, and correlating data about devices, identities, cloud, software, SaaS applications, vulnerabilities, security controls, and their interrelationships, customers can ask questions, get answers, and automate action.

KEY TAKEAWAYS

Rapid technology innovation and adoption drives the need for new security solution sets.

Across industries, the technology stack has grown in complexity over time. The adoption of new technologies is driven from all sides—by innovation to solve various challenges, business interoperation requirements, the introduction of mobile devices into operations, environment configuration as businesses shift to the cloud, increase SaaS app adoption, and more.

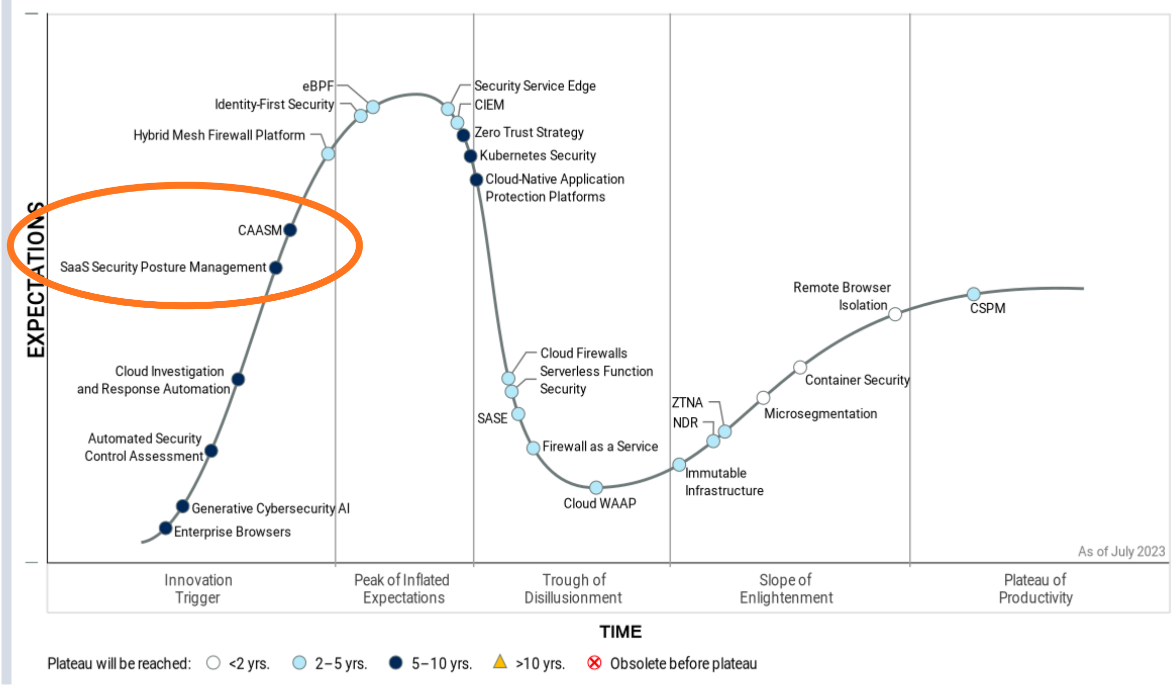
Yet, despite significant advancements in and adoption of new technology, security practitioners continue to struggle with fundamental questions such as,

- *"How many Windows devices are in my environment?"*
- *"Are all my virtual machines being scanned?"*
- *"Do we have any critical misconfigurations in our top SaaS apps?"*

Every new technology generally drives a change in how security practitioners protect the business; however, the constantly changing complexity and an always-expanding sprawl of devices, users, software, SaaS applications, cloud services, and the tools used to manage and secure them has shifted the priorities of security practitioners, creating the need for full context of assets in the environment. Having a fundamental understanding of all assets is critical to securing the organization—this is the driver behind the emergence of CAASM and SSPM.

CAASM and SSPM were first recognized in 2021 as separate categories and are currently listed within the innovation trigger phase of the Gartner Hype Cycle™ for Workload and Network Security; meaning that although in the early stages of adoption, these will become critical tools for organizations to leverage to help manage security within their environment. Understanding what these solutions are and the value each provides can help security providers use these two tools together to solve real-world problems for their organization.

Figure 1: The Gartner Hype Cycle for Network Security, 2023

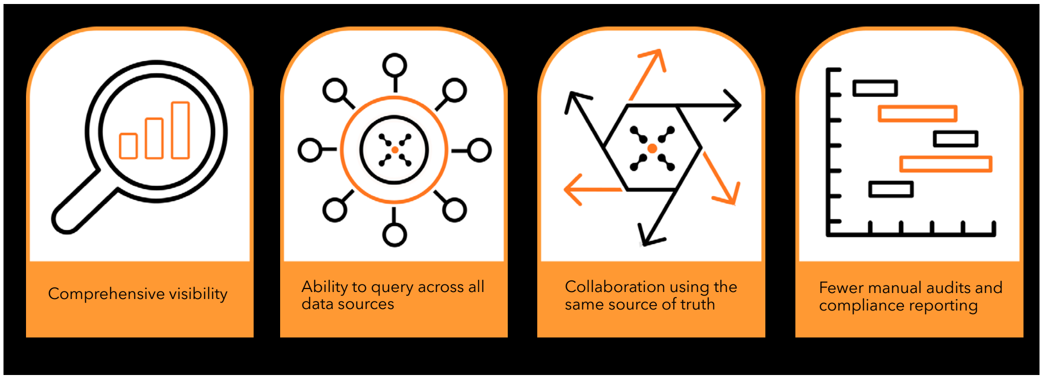


CAASM and SSPM independently increase visibility for improved security.

CAASM is a group of solutions that help organizations detect and identify all software, hardware, cloud assets, network assets, and network infrastructure, as well as vulnerabilities within those assets. It helps security teams solve their asset visibility and vulnerability challenges by providing a consolidated view of all assets. To gain this **comprehensive visibility**, CAASM solutions rely on API integrations with existing tools to aggregate and correlate information across all different technologies (e.g., network infrastructure, cloud infrastructure, endpoint technology solutions, software delivery solutions, mobile device management solutions).

Once information is pulled together, a key capability of CAASM is **the ability to ask questions of that information**, from basic inventory count of specific device types to more complex queries such as which devices are running vulnerable versions of a browser and do not have a functioning EDR agent. Using aggregated data in a single source of truth to answer questions helps **identify and remediate vulnerabilities** and enables collaboration between teams—whether IT or security—across the environment. And removing the manual processes from data collection and correlation **streamlines and automates audits and reporting**, whether for regulatory compliance or executive briefing.

Figure 2: Benefits of CAASM


Comprehensive visibility
Ability to query across all data sources
Collaboration using the same source of truth
Fewer manual audits and compliance reporting

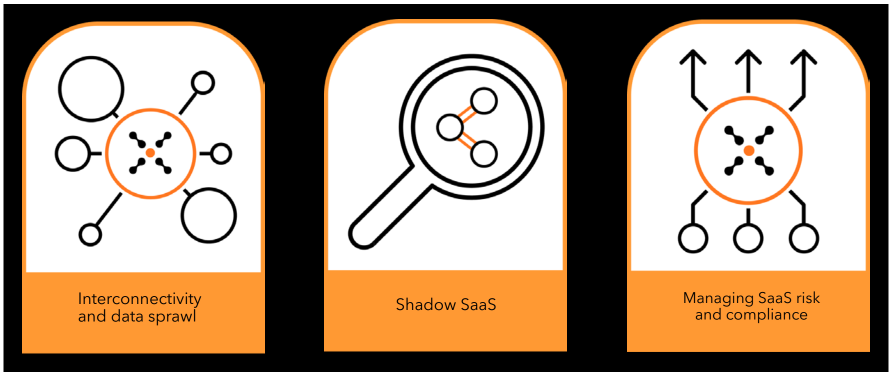
The proliferation of SaaS applications within organizations has introduced several challenges for IT and security teams due to lack of understanding around the interconnectivity of SaaS tools and capabilities. To address these challenges, security practitioners need a solution for identifying and managing data that exist outside of an organization's boundaries, such as when it is stored within SaaS applications.

SSPMs and **SMPs** provide some much-needed visibility into the interconnectivities created by SaaS applications.

- Like CAASM, **SSPMs** connect to assets via APIs; however, SSPMs are specific to SaaS applications. SSPMs leverage APIs to monitor the various risks (e.g., misconfigurations, unnecessary user accounts, excessive permissions, standards compliance) within SaaS applications.
- **SMPs** (SaaS Management Platforms) are platforms built to discover, manage, and automate the governance of SaaS applications, such as SaaS licensing and user on- and off-boarding. The increased visibility also helps identify shadow SaaS applications. With SSPMs and SMPs, overall risk is decreased, and overall compliance increased through identification and automated remediation of vulnerability and gaps.

> "If we want to be able to prioritize risk reduction, we first have to understand what we're trying to protect. We can't protect what we don't see."
>
> *Sean Blenkhorn, Axonius*

Figure 3: The problems that SSPMs and SMPs solve


Interconnectivity and data sprawl
Shadow SaaS
Managing SaaS risk and compliance

Axonius brings CAASM and SSPM together to secure complex environments.

When used together, CAASM and SSPM provide operational improvements to IT and security teams. While there are other categories that security practitioners might consider applying in the business environment, CAASM and SSPM play particularly well together because both drive the establishment and maintenance of complete visibility into all assets.

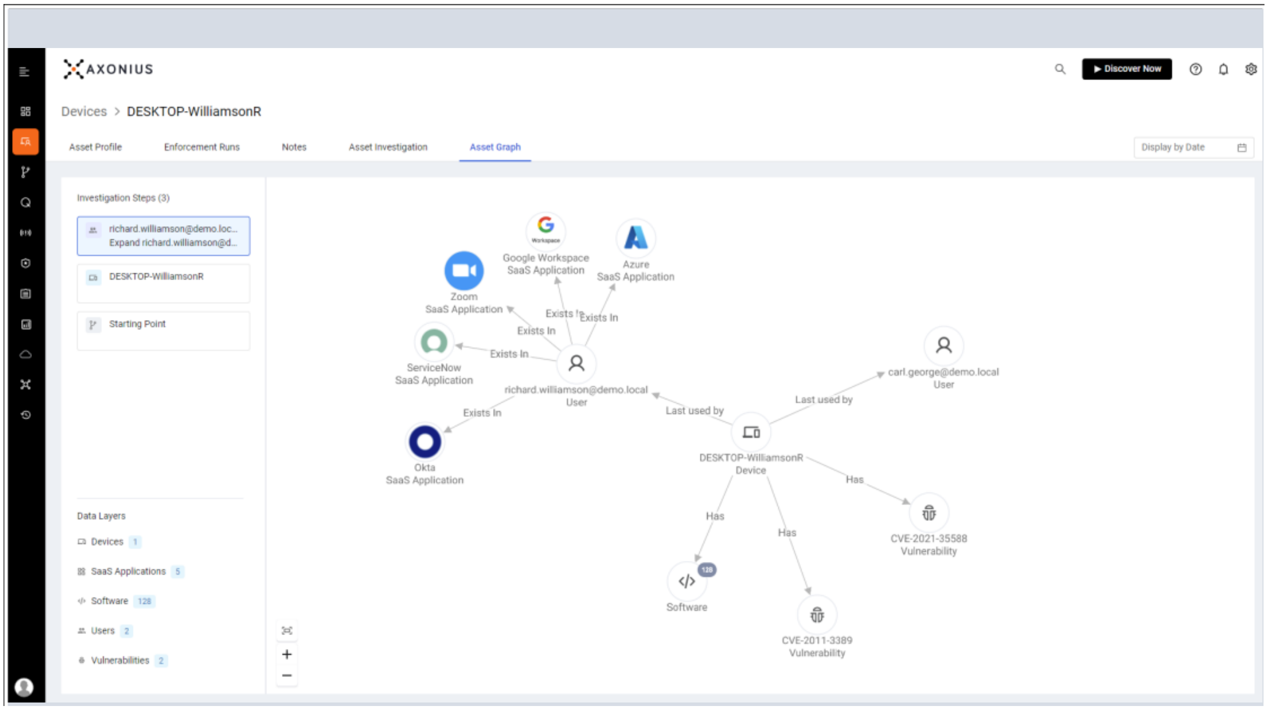
Axonius gives IT and security teams the confidence to control complexity by providing a system of record for all digital infrastructure. With a comprehensive understanding of all assets including devices, identities, software, SaaS applications, vulnerabilities, security controls, and the context between them, customers are able to mitigate threats, navigate risk, decrease incident response time, automate action, and inform business-level strategy—all while eliminating manual, repetitive tasks.

Even in highly complex environments, Axonius addresses key use cases critical to business operations, including:

- **Visibility.** Without visibility into everything that is considered part of the organization's domain—whether on-premise, in the cloud, or in a third-party application—solving security risks and issues is exceptionally challenging. The single source of truth made possible by CAASM and SSPM provides the comprehensive visibility required to maintain security in today's complex environments.
- **Inventory of software.** Software today falls into one of two main categories: installed software and cloud (SaaS) applications. To manage software effectively and securely depends on understanding application in use within the organization, as well as who is using those applications (if anyone) and how often. This supports optimized cost management, including license reclamation and pricing negotiations, and streamlines operations such as user on- and off-boarding.
- **Device-to-SaaS correlation.** Mapping relationships between entities is critical to security. Knowing which devices in an environment are accessing SaaS applications helps security practitioners protect sensitive data such as PII or PHI by limiting unauthorized user and device access.
- **Incident impact.** Incident response is a situation in which CAASM and SSPM can come together to provide a powerful benefit through better clarity and contextual awareness for organizations that are experiencing an incident. Comprehensive visibility of assets and relationships between them can speed incident response and lessen the overall impact.

> "Being able to connect the dots and understand how all these entities relate to one another is really, really important to the expediency, effectiveness, and efficacy of the incident response."
>
> *- Sean Blenkhorn, Axonius*

Figure 4: CAASM and SSPM together can clearly define the blast radius of an incident



- **Zero trust reconciliation.** A core practice of zero trust is to verify every request for access to data or resources. In today's sprawling and complex environments, visibility is key to understanding how access should be configured and structured, both in initial implementation of, as well as ongoing maintenance of and adherence to, zero trust architecture and practices.
- **Policy management and enforcement.** The responsibility of security teams is to ensure all assets are adhering to policies and standards. CAASM and SSPM effectively identify the gaps in policy application across the entire spectrum of assets and configurations.
- **Determine ownership.** In a security event, whether a configuration error or a breach, knowing the ownership of a particular device or SaaS application within the context of the organization will speed the response.

In a world where the rate of change makes the manual work of finding, managing, and securing assets tedious, error-prone, and a waste of scarce, valuable resources, a solution like Axonius is needed to help organizations understand the full context of all assets in the environment at any given time. By leveraging existing data and combining the power of CAASM, SSPM, and SMPs within one platform, Axonius provides organizations with a comprehensive, up-to-date inventory, helps uncover gaps, and automates response actions.

ADDITIONAL INFORMATION

To learn more about Axonius, visit axonius.com

BIOGRAPHIES

Sean Blenkhorn

Vice President of Sales Engineering, Axonius

Sean is the Vice President of Sales Engineering at Axonius. As a 20 year cybersecurity expert, Sean has worked with some of the world's largest companies in architecting and deploying security and compliance solutions including DLP, endpoint security, SIEM, encryption, and more. Sean has extensive experience leading and building both sales engineering and consulting services organizations in rapid growth companies.

Terry Sweeney

Editor, Dark Reading (Moderator)

Terry Sweeney is a Los Angeles-based writer and editor who has covered technology, networking, and security for more than 20 years. He was part of the team that started Dark Reading and has been a contributor to The Washington Post, Crain's New York Business, Red Herring, Network World, InformationWeek and Mobile Sports Report. In addition to information security, Sweeney has written extensively about cloud computing, wireless technologies, storage networking, and analytics. After watching successive waves of technological advancement, he still prefers to chronicle the actual application of these breakthroughs by businesses and public sector organizations.