WHITE PAPER

# Not All CAASM Initiatives Are Made The Same Learn How Lucidum Differs

LUCIDUM

NOW PART OF cyderes

# Introduction

As organizations continue to rely heavily on technology to store, process, and transmit information, cybersecurity has become more important than ever. However, the constant evolution of technology and the increasing number of cyber threats make it difficult for organizations to keep their technology infrastructure secure.

Cyber Asset Attack Surface Management (CAASM) is a proactive approach that identifies and mitigates vulnerabilities in an organization's technology infrastructure. CAASM is a critical component of a cybersecurity strategy and can help reduce the risk of cyber-attacks.

Not all CAASM solutions are created equal. In this whitepaper, we will compare Lucidum's approach to CAASM and that of our competitors, Axonius and JupiterOne. We will discuss the key features and benefits that differentiate Lucidum, and show why our solution is the best choice for organizations looking to proactively manage their attack surface.

**Proactive Risk Management**

One of the key benefits of Lucidum's CAASM solution is its proactive approach to risk management. Lucidum's solution identifies and mitigates vulnerabilities in an organization's technology infrastructure before those vulnerabilities can be exploited by cybercriminals. This proactive approach is crucial in today's threat landscape, where new vulnerabilities and attack methods are constantly emerging.

By identifying and mitigating vulnerabilities before they can be exploited, Lucidum's CAASM solution helps organizations reduce the risk of a successful cyber-attack.

See how the CASSM solutions compare in the following table on the next page:

| Feature | Lucidum | Axonius | JupiterOne |
|---|---|---|---|
| Ability to ingest on-premises and cloud data to bring assets and vulnerabilities into a single pane of glass | Yes | Yes | Yes |
| Machine-learning assisted enrichment of contextual information about assets and users. (In addition, Lucidum applies NLP and ML to further enrich asset data, creating an additional pillar of context and enabling risk ranking | Yes | Limited | No |
| Risk assessment of each asset, user, and data | Yes | No | No |
| Risk ranking of each asset for easy prioritization | Yes | No | No |
| Preconfigured dashboards that display risk factors, risk level, assets without endpoint protection, and assets affected by all active CVEs | Yes | No | Limited |

As the table above illustrates, while all three providers offer a proactive approach to risk management, Lucidum stands out with its machine-learning assisted asset, user, and data identification, correlation of assets, users, and data, risk assessment and rankings of all assets, users, and preconfigure dashboards that identify risk and vulnerabilities.

**Comprehensive Asset Identification**

Another key benefit of Lucidum's CAASM solution is its comprehensive asset identification capabilities. Our solution is designed to identify all assets that make up an organization's attack surface, including servers, network devices, cloud resources, mobile devices, and IoT devices. By identifying all assets, organizations can better understand their attack surface and take steps to mitigate the risk of a successful cyber-attack. When it comes to comprehensive asset identification, the following is a comparison of Lucidum, Axonius, and JupiterOne:

| Feature | Lucidum | Axonius | JupiterOne |
|---|---|---|---|
| Comprehensive Asset Identification | Yes | Yes | Yes |
| Comprehensive User Identificationons | Yes | Yes | Yes |
| Comprehensive Data Identification and Data Classification ((highly confidential, confidential, and public) | Yes | No | No |
| Correlation of Assets, Users, and Data | Yes | No | No |
| Data quality assessment, insights, and notification | Yes | Limited | No |
| Risk assessment of each asset, user, and data source | Yes | No | No |

As the table before illustrates, all three solutions offer comprehensive asset identification capabilities and user identification abilities. However, only Lucidum differentiates itself by correlating assets, users, and data, deduplicating records, and providing risk analysis of each asset, user, and data source. Lucidum provides a detailed, "single pane of glass" view of an organization's attack surface that includes assets, users, data, and their relationships and risk.

**Flexible and Scalable**

Lucidum's CAASM solution is also designed to be flexible and scalable, making it suitable for organizations of all sizes and industries. Our solution can be easily configured to meet the specific needs of each organization, and can be scaled to accommodate growth and changing requirements. This flexibility and scalability make Lucidum's CAASM solution the ideal choice for organizations looking

| Feature | Lucidum | Axonius | JupiterOne |
|---|---|---|---|
| SaaS (Software as a Service) platform that allows for easy upgrades and scalability | Yes | Yes | Yes |
| Dynamic fields that allow organizations to add and define their own business rules | Yes | No | No |
| Custom field that allow organizations to bring their custom data into the CMDB (congiration management database) | Yes | Limited | No |
| Allow organizations to upload files to attach to asset or user records | Yes | No | Limited |
| Role-based access control for fine-grained control of access within the solution | Yes | No | No |

It is clear that all three providers offer flexible and scalable solutions, but it's important to note that Lucidum is designed for easy customization and scalability to meet the exact need of each organization. Lucidum is a SaaS-native product that scales easily. Lucidum includes multiple features to allow customization, and Lucidum's RBAC features allow granular control of access to Lucidum's data.



LUCIDUM

**Competition Comparison**

While Axonius also offers a CAASM solution, it lacks the level of proactive risk management found in Lucidum. Axonius' solution identifies assets but does not provide the detailed, "single pane of glass" view of an organization's entire attack surface that includes assets, users, data, and their relationships. Axonius' solution lacks the ease-of-use and flexibility that Lucidum offers. Similarly, JupiterOne's CAASM solution is more focused on mapping and visualizing an organization's attack surface. While this can be useful for understanding an organization's attack surface, it does not offer the same level of proactive risk management and comprehensive asset identification as Lucidum's solution.

# Conclusion

In conclusion, we have compared Lucidum's CAASM solution to those of our competitors, Axonius and JupiterOne. We have highlighted the key features and benefits that set Lucidum apart, including its proactive approach to risk management, comprehensive asset identification capabilities, and flexibility and scalability.

By choosing Lucidum, organizations can be sure that they are getting a comprehensive and proactive CAASM solution designed to help reduce the risk of a successful cyber-attack. With Lucidum's solution, organizations can better understand their attack surface, easily and quickly take steps to mitigate vulnerabilities, and stay upto-date with the latest threats and vulnerabilities.

# About Lucidum

Lucidum was built by cybersecurity experts on a mission to gain full visibility into their tech ecosystem. We take pride in our innovative platform, and we're thrilled each time we offer our customers the ability to see and understand what was formerly lurking just off the radar.

We put everything in your sights, giving you the power to understand what it is and what it's doing. Understand the lay of your tech landscape, lock onto threats, and keep your perimeter secure – all empowering you to defend and dominate your space in an increasingly threatening world.

Learn more at **www.lucidum.io**



LUCIDUM