WHITE PAPER

7 REASONS Why your Organization Needs to Focus on Cyber Asset Attack Surface Management

LUCIDUM

NOW PART OF cyderes

TABLE OF CONTENTS

Introduction

This whitepaper outlines the cybersecurity risks all organizations face and how a comprehensive Cyber Asset Attack Surface Management (CAASM) program can help address them. A CAASM platform empowers your organizational leaders to be more aware, more proactive, and more targeted when it comes to assessing risk, mitigating threats, and protecting the things you care about most.

LUCIDUM

YOUR DIGITAL ECOSYSTEM

Is Even More At Risk Than You Realize

Every organization is connected to the world via the internet, which makes them vulnerable to attack. Even those organizations that do not rely on cloud technology increasingly use cloud-based Software as a Service (SaaS) tools, providing a vector to infiltrate their broader informational network. Being 100% offline is no longer a viable option; additionally, there are internal risks that can come from employee errors, configuration item (CI) issues, intentional theft, and other vulnerabilities.

Combined, these risks mean that cybersecurity threats have become an everyday aspect of doing business.

45%

2021 DATA REPORT
Found that nearly half of US Companies suffered a data breach in the previous year.

4.35M

2022 IBM ESTIMATES
That a single data breach incident cost, a 12.7% increase from 2020.

Those costs are just the immediate impact. Research from FTI Consulting showed that a company can expect a 9% hit to their overall financial position year-over-year after a data breach or a similar cybersecurity incident.

Overall, the message is clear: Cybersecurity risks are ever-present, and the financial incentive to avoid them is high.

PROLIFERATING DIGITAL FOOTPRINTS

Means More Vulnerabilities Than Ever

At the same time that cybersecurity risks proliferate, technology has become embedded into the way organizations operate. Companies use more digital technologies than ever to bring their services to life, and those technologies represent increasingly complex digital ecosystems.

LUCIDUM

82%

ACCORDING TO CISCO
company IT leaders say theyare operating on a hybrid cloud model

47%

REPORTED USING
2-3 public clouds for an Infrastructure as a Service (IaaS) platform

37%

CISCO'S REPORTS
IT leaders consider security as a primary challenge when deploying through multiple cloud platforms

With technology proliferation comes a lack of clarity. Organizational leaders lose sight of what is in their tech stack and what is coursing through their larger digital ecosystem. What they need is a way to make every asset and every connection visible. **This practice is called Cyber Asset Attack Surface Management.**

> Risks associated with the use of cyberphysical systems and IoT, open-source code, cloud applications, complex digital supply chains, social media and more have brought organizations' exposed surfaces outside of a set of controllable assets. Organizations must look beyond traditional approaches to security monitoring, detection and response to manage a wider set of security exposures.

PETER FIRSTBROOK
VP OF RESEARCH, GARTNER

LUCIDUM

MOST MODERN ENTERPRISES CAST A DIGITAL FOOTPRINT SO WIDE, YOU CAN'T EVEN SEE ITS EDGES.

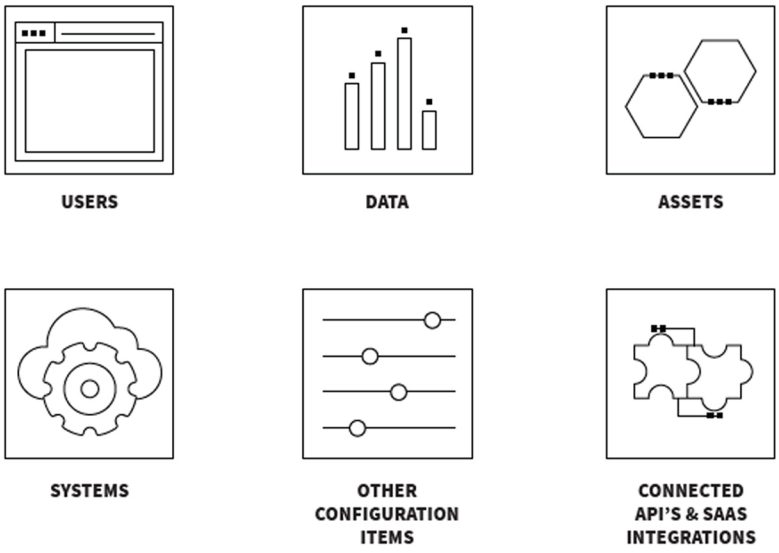
CAAS M IS N ECESSARY TO

PROTECT WHAT MATTERS MOST

As the number of assets and systems connected to digital ecosystems rises, there's more ground than ever for risk management leaders to cover.

In order to secure top priorities, organizations must have visibility. Cyber Asset Attack Surface Management (CAASM) gives you that visibility.

A COMPREHENSIVE ASM PLATFORM IS CAPABLE OF REVEALING ALL OF THE FOLLOWING CONNECTING TO YOUR GLOBAL NETWORK OF TECHNOLOGIES:



Unlike a scan, these items are revealed in specificity with all known meta-information and relevant parameters. Unlike an agent, there's no need for specific software to be installed on any of these items for them to be revealed. Unlike manual CI and asset lists, the information is complete and updated in real time.

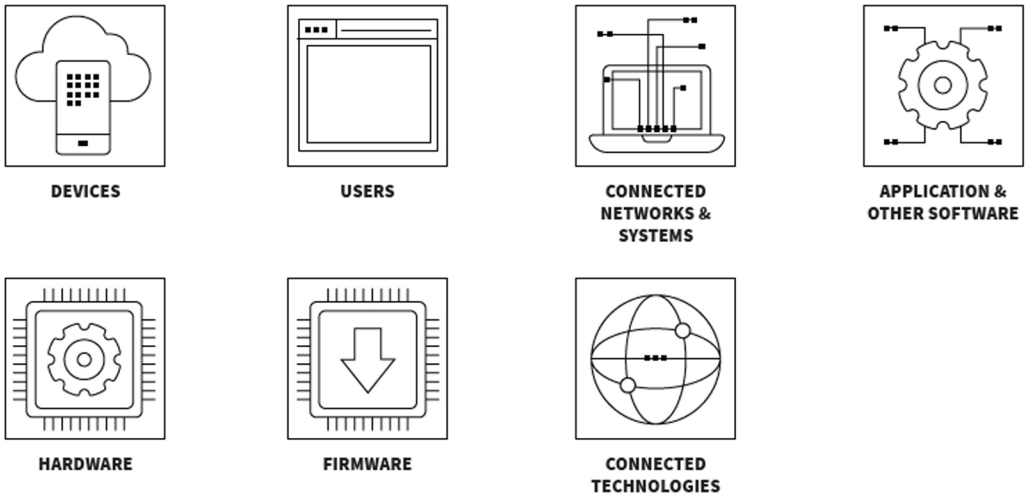
A best-of-breed CAASM platform provides more than mere visibility, too; it empowers cybersecurity leaders to quantify risks immediately. Through a single lens, they can see threats and asset statuses, enabling them to quickly respond and mitigate during emerging incidents.

LUCIDUM

WHAT IS CAASM?

An "attack surface" refers to the sum total of all technologies that pose a risk of becoming a cybersecurity attack vector. Since risks encompass internally-sourced incident causes as well as external threats, having a view of all possible vulnerable factors is critical.

A CAASM CAN CONSIST OF ANY OR ALL OF THE FOLLOWING:



Organizations that lack a CAASM strategy have an incomplete picture on their radar. They could be surprised by sudden threats – or even unexpected compromises potentially introduced by connected devices and applications or practices that aren't officially sanctioned by the organization.

In sum: having a CAASM platform you can rely upon is like having a copilot give you a constant readout of your full tech landscape, including things you didn't even know were inside of it. A Cyber Asset Attack Surface Management (CAASM) strategy goes beyond the identification of all connected assets, users, and systems. It must also be capable of providing contextual information in real time.

Ideally, it should also enable quick action directly from the source of knowledge, enabled by integration into SIEM/SOAR and your other best-of-breed cybersecurity systems. With these specifications in mind, below are the seven primary benefits you'll obtain when you invest in a best-of-breed Cyber Asset Attack Surface Management platform.

LUCIDUM

7 R EASONS WHY

YOU NEED CAASM STRATEGY

A Cyber Asset Attack Surface Management strategy goes beyond the identification of all connected assets, users, and systems. It must also be capable of providing contextual information in real time. Ideally, it should also enable quick action directly from the source of knowledge, enabled by integration into SIEM/SOAR and your other best-of-breed cybersecurity systems. With these specifications in mind, below are the seven primary benefits you'll obtain when you invest in a best-of-breed Cyber Asset Attack Surface Management platform.

#1 OBTAIN A FULLY SCOPED, REALISTIC VIEW OF YOUR ACTUAL TECH LANDSCAPE

Traditional methods of revealing items within the attack surface rely on agents and scans. Unfortunately, agents only reveal assets that still have an active agent attached. Scans only reveal one-time informational pings about a connection. These results obscure critical information while creating a record of IPs and other "identifiers" that identify little – and tend to expire quickly.

A Cyber Asset Attack Surface Management discovers all connected assets, users, and systems. Lucidum, in particular, identifies these entities regardless of whether they have agents installed. It also reveals contextual information about each discovery so that the item can be understood and acted upon, such as adding it to the CMDB or setting up new events for SIEM to activate.

Performing an inventory of company assets is cumbersome enough with partial information. But organizations also need to have a wider view of their digital ecosystem that encompasses partners, service providers, and outside presences like API connections.

A comprehensive CAASM product gives the full picture of everything, along with the information and the capabilities needed to act on that information.

LUCIDUM

#2 UNDER RISK VECTORS AND ASSESS VULNERABILITIES

Discovering all connected entities is just the first step to protecting your company's most precious digital assets. IT and cybersecurity leaders will leverage this information to map out their vulnerabilities and assess where the highest level of threats could come from.

IT leaders can incorporate the revised threat model into vulnerability testing, automating tasks like brute force attempts against a hitherto unknown attack vector. They can also prioritize risks based on the assets affected and the likelihood of a compromising incident.

This intel is particularly important for External Attack Surface Management (EASM), which reveals the assets standing on the front line and most at-risk of campering, breaches, or critical threat exposure.

7 R EASONS WHY

YOU NEED CAASM STRATEGY

#3 ENFORCE EXISTING INTERNAL POLICIES AND VALUES

All organizations have technology-related policies in place to reduce risk and exposure to liability. These policies exemplify due diligence. It's the organization saying: "we handle things a certain way because that is the best method of reaching our goals, which touch both upon our assets and the sensitive data of customers."

Yet, enterprise ecosystems are full of connected assets and systems that do not comply with stated policies. They may also have sensitive data lying undiscovered and under protected.

CAASM shines a light on all the dark corners within your infrastructure to see what messes people may have left behind and what undesirable elements have found their way into your network.

Enterprise leaders can then address these shortcomings, put everything in compliance, or cut it off from the tech stack to eliminate unsanctioned practices.

LUCIDUM

THREATS MAY LURK WITHIN SHADOW IT

According to Hubspot surveys, Shadow IT has grown explosively since 2020.

59%

INCREASE IN TICKET
related to practices and platforms that lie outside the scope of official technology acquisitions

54%

IT LEADERS FEEL
they are now significantly at risk" because of unsanctioned activities.

97%

OF APPS OPERATING
within enterprise clouds are technically "shadow" installations lying outside formal policies!

While not every instance of Shadow IT is risky or harmful, IT leaders must know what they don't know yet in order to be able to act on that information – which potentially includes shutting down risky activities right at the source.

7 R EASONS WHY

YOU NEED CAASM STRATEGY

#4 GAIN REAL-TIME VISIBILITY OF CHANGE ACTIVITIES WITHIN YOUR ECOSYSTEM

Today's IT leaders need to avoid being blindsided. Or, at the very least, they need to be able to quickly identify where and how an unexpected threat has come through.

Activities like scans and inventories are not only incomplete, but they have a high degree of latency. By the time everything is cataloged, it may have changed.

A CAASM platform is capable of maintaining visibility of assets over time, even as they change IPs or shift their identifiers. It can also discover new assets live, as they happen, without requiring an agent installation or a manual re-scan.

The ability to monitor everything going on in your airspace in real-time is huge! It provides constant contextualized information. It also augments mitigation and response capabilities thanks to accurate, up-to-date data.

LUCIDUM

#5 MASTER LIFECYCLE MANAGEMENT FOR ALL PRODUCTS, SERVICES, AND CONNECTED ENTITIES

Tech stacks can be overwhelming, especially as the new replaces the old. Much like Shadow IT, legacy systems and other additions that didn't go through official channels often end up lying well outside the scope of lifecycle management.

Letting things sit, like an old IAM system, can mean lots and lots of backdoors. Companies that have undergone a merger or acquisition (M&A) particularly invite huge risks during tech stack consolidation!

CAASM reveals all important entities that may not lie on your CMDB or other official sources. It allows IT leaders to keep everything properly patched and up to date – or, as necessary, decommissioned.

#6 EMPOWER COMPLIANCE WITH REGULATIONS FOR PRIVACY, DATA HANDLING, AND DUE DILIGENCE

CAASM not only reveals unexpected stores of sensitive data; it also shows everything capable of looking at that data. Having this understanding is critical for maintaining compliance with data and privacy regulations, as well as preventing a possible incident.

7 R EASONS WHY

YOU NEED CAASM STRATEGY

CONT. EMPOWER COMPLIANCE WITH REGULATIONS FOR PRIVACY, DATA HANDLING, AND DUE DILIGENCE

Laws like General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) carry hefty fines. Major incidents can mean multiple violations, quickly racking up a huge tab with regulatory bodies and adding to the pre-existing costs of incident management and response.

Understanding data stores, data sources, and entities capable of accessing data is critical to protect, mitigate risk, and demonstrate due diligence to agencies and any incident-related inquiries.

LUCIDUM

#7 PROTECT SERVICES, EARNINGS, AND REPUTATION

Modern enterprises have multiple bottom lines for all stakeholders. A breach or incident means that no one is happy. When an incident happens, it damages any (or all) of the following:

Reputation
Earnings
Trust from vendors and partners
Operational efficiency
Service delivery
Investment activity
Growth
Ability to market

Preventing an incident is easier than trying to clean up after damage to any (often all) of these. Step 1 in incident prevention is gaining a complete view of everything you need to protect – and, often, what you need to protect it from.

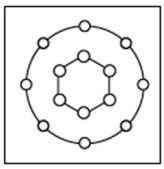
CAAS M I S A

MUST-HAVE, NOT NICE-TO-HAVE

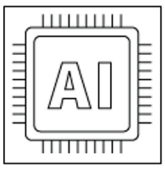
Companies can no longer afford to be flying behind a blackened windscreen. With so many dangers coming from all angles, they need full 360° awareness of everything going on in their airspace.

Lucidum acts as your co-pilot: reading out the radar, keeping you aware of threats, and ensuring that assets remain well-protected within your airspace.

LUCIDUM'S CAPABILITIES:



DISCOVER ALL
assets, users, and data without limits



LEVERAGE AI
to rapidly identify, quantify, and evaluate risks

GAIN MORE CONTEXT
than you ever could with a scan, agents, or CMDB inventory

TAKE ACTION
from a single dashboard integrated into best-of-breed cybersecurity tools

ENJOY PERSISTENT
support from our installation and customer care teams

Have more questions about Cyber Asset Attack Surface Management, or looking for a demo? Contact us today!

About Lucidum

Lucidum is the Cyber Asset Attack Surface Management company that eliminates blind spots across cloud, security, and IT operations. Fortune 500 companies rely on the Lucidum platform and its patent-pending Machine Learning to discover, triangulate, and identify all assets. Lucidum helps you find your company's risk factors, focus your attention, and take action.

To learn more about Lucidum's Cyber Asset Attack Surface Management platform, please visit: Learn more at www.lucidum.io

LUCIDUM