Reducing Attack Surface with the Next Generation of CAASM

Executive Summary:

Background:

73% of organisations surveyed say they are worried about their growing attack surface. Furthermore, 43% describe their attack surface management as "**spiralling out of control**."

Limited visibility is a stated obstacle in Attack Surface Management, with 62% admitting to security "**blind spots**". In fact, on average, organisations estimate they have only 62% visibility of their attack surface.

Over half (54%) need more confidence in their risk assessment methods. Only 45% have a well-defined process, and only 23% review risk exposure daily.

These statistics illustrate how attack surfaces are growing faster than organisations can manage, resulting in blind spots, poor risk management, and an increased number of successful cyberattacks.

Introducing Cyber Asset Attack Surface Management:

Cyber Asset Attack Surface Management (**CAASM**) has emerged as a solution to these challenges. It offers organisations the ability to understand, manage, and reduce their attack surface.

The initial generation of CAASM systems acted an overlay to existing IT systems. They, therefore, added cost and could amplify errors and gaps due to issues in the underlying "feeder" systems. This means that despite implementing CAASM, the very blind spots they aim to eliminate and critical vulnerabilities can remain undetected.

The Next Generation CAASM:

The answer to these issues is to discover the assets directly, integrate the analysis of vulnerabilities and insecure configuration issues without needing to buy and operate multiple, underlying and separate toolsets.

Such an approach will deliver the aims of CAASM:

1) More complete, up-to-date asset inventory
2) Improved cyber security by reducing the attack surface
3) Reducing the number of systems to operate and integrate

4) Ultimately lowering costs

In this paper, we will examine the problems with of attack surface management using generation 1 CAASM tools and how to overcome them.

What is CAASM?

CAASM emerged from a new Gartner category. It is focused on reviewing systems that enable security teams to overcome asset visibility and exposure challenges.

CAASM systems start with allowing organisations to see all assets (internal and external). This data is then fed into vulnerabilities and secure configuration systems to identify risk and gaps in cyber-security controls.

The outcome is that organisations can more effectively prioritise the most critical risk and better focus remediation and mitigation activities.

What it does

CAASM's acronym says it succinctly:

1) Discover and catalogue IT **Assets**
2) Analyse these assets for vulnerabilities and cyber-security issues (the **attack surface**)
3) Help organisations **manage** those issues that are the most critical to the organisation.

How it helps

Two factors impact cyber security: 1) the management control of the assets to be secured and 2) managing down the risk from continuously changing threats.

Reliably bringing together of these 2 areas (asset plus vulnerabilities and secure configuration) helps identify potential security gaps and vulnerabilities and prioritise risks. Using tools means that human error can be eliminated and technology can be used to pin-point the most important aspects.

A CAASM system helps reduce/eliminate the management control of the assets and thus act as a feed to the security assessment process.

Why it's important

In today's world of growing attack surfaces, organisations need proactive measures to protect their critical systems and sensitive data. CAASM is a key component of the Continuous Threat Exposure Management (CTEM) framework.

CAASM vs IT Asset Management (ITAM)

While they both manage assets, CAASM extends ITAM to meet the needs of cybersecurity:

Design	IT Asset Management	CAASM
Data collection	Hardware, operating system and installed application.	ITAM plus extended security related data, such as configuration.
Timeliness	Infrequent scans or updates, sufficient for reporting	Aims for real-time visibility to reduce the exposure time.
Integration	Integrates mainly with IT service management (ITSM) tools.	Integrates with various security tools (e.g., vulnerability scanners, SIEMs, EDR).
Automation	Often manual and limited.	Highly automated to detect and analyse security gaps.

Generation 1 CAASM vs Next Generation CAASM

The simple premise of V1 CAASM systems was to collect data from existing IT systems and try to correlate any gaps in asset understanding. Next Generation CAASM aims to improve and reduce costs:

Aspect	Gen 1 CAASM	Next Gen CAASM
Data collection	API integration for underlying systems.	Native discovery plus API integration to improve accuracy.
Timeliness	Relies on feeder system timings, so can be out of date.	Real time without the constraint of feeder system collection frequency.
Integration	Often requires external vulnerability scanners.	Integrated vulnerability assessment. No scanning or separate systems needed and reduced cost.

Rebasoft's Next Generation CAASM

Rebasoft has been helping customers with real-time asset management and security for more than 10 years. The latest version includes an integrated vulnerability assessment service that correlates discovered asset data with the latest vulnerability, threat and secure configuration guidelines.

Rebasoft's platform means CAASM is easily delivered at a lower cost. The following capabilities extend all the features you'd expect in a V1 CAASM system:

Capability	How it works	Benefit
Asset discovery via the Network	Network based discovery to identify assets.	This means any system connected to the local network will automatically be found. Network, End-user, IoT and OT systems are automatically found even is there is no API based system to ask.
Agent-less and scan-less	Unlike V1 CAASM, these methods are used after the asset has been discovered, rather than being used to find assets.	Improved asset discovery while retaining the deep data collection needed for CAASM.
Integrated vulnerability services	Using data from the Asset Database, vulnerabilities and threats can be analysed without the asset needing to be present on the network or any agent installed.	More complete, timely vulnerability assessment
Vulnerability and secure configuration issue tracking by assets	Logging issues related tightly to assets.	Reduces repeats, increases understanding and helps reduce time to remediate.
Integrated traffic monitoring	Using NetFlow, system compromise or malware spread can be detected in real-time.	Can Identify asset compromise independently of known vulnerabilities.

Rebasoft next generation CAASM does not completely rely on the feeder systems this means:

1) Improved accuracy
2) Fewer integrations to build and manage
3) Fewer systems to acquire and operate

4) Fewer system to learn and understand

All of this results in lower capital and operational costs.

Summary:

Rebasoft's CAASM solution revolutionises asset management by utilising the network layer as the foundation, providing unparalleled asset visibility and resilience. Combined with vulnerability mapping and an integrated secure configuration approach, Rebasoft delivers a best-in-class solution for reducing security breaches, improving risk posture and operational overhead, and protecting against emerging threats.

This ensures organisations not only react to security challenges but stay ahead of them.

Data breaches that point to a lack of visibility as a route course.

Several notable data breaches have been attributed to a lack of asset visibility, where organisations failed to properly account for or monitor their IT assets, such as devices, servers, or software applications.

Here are examples based on publicly available information:

1. Equifax (2017)

- Details: The breach, which exposed the personal data of 147 million individuals, was partly attributed to an unpatched vulnerability in Apache Struts, a web application framework. The company failed to identify and update the affected system, an asset under their responsibility.
- Cause of Breach:
  - Poor visibility into software vulnerabilities.
  - Failure to maintain an accurate inventory of systems running Apache Struts.
- Impact: Estimated cost of $1.4 billion in settlements and security improvements.
- Data source: https://www.fca.org.uk/news/press-releases/equifax-ltd-fine-cyber-security-breach

2. Marriott International (2018)

- Details: This breach, involving the data of 500 million customers, stemmed from a lack of visibility into systems inherited from Starwood Hotels after an acquisition. The compromised database had been vulnerable since 2014, but Marriott only discovered the breach in 2018.
- Cause of Breach:
  - Inadequate monitoring and management of newly acquired IT assets.
  - Lack of comprehensive asset mapping during the merger.
- Impact: Significant fines, including a $23.8 million GDPR penalty in 2020.
- Data source: https://www.bbc.co.uk/news/technology-54748843

3. Target (2013)

- Details: Hackers exploited credentials stolen from a third-party HVAC vendor to infiltrate Target's network. Once inside, they moved laterally to access the company's payment system.
- Cause of Breach:
  - Poor segmentation and insufficient monitoring of third-party systems.
  - Lack of visibility into network assets allowed attackers to traverse undetected.
- Impact: The cost to Target is approximately $292 million in damages and settlements.
- Data source: https://redriver.com/security/target-data-breach

4. Capital One (2019)

- Details: A former employee of Amazon Web Services exploited a misconfigured web application firewall to access sensitive data stored in the cloud. Capital One's failure to detect the misconfiguration highlighted gaps in asset monitoring and management.
- Cause of Breach:
  - Misconfiguration of cloud assets due to inadequate oversight.
  - Lack of robust tools for cloud asset visibility.
- Impact: Estimated $190 million in penalties and settlements.
- Data Source: https://dl.acm.org/doi/10.1145/3546068

5. SolarWinds Supply Chain Attack (2020)

- Details: Hackers injected malicious code into SolarWinds' Orion software, which was widely used by government and corporate entities. The breach exposed a lack of visibility into the software supply chain.
- Cause of Breach:
  - Insufficient vetting and monitoring of third-party software.
  - Limited ability to track and audit dependencies.
- Impact: Over 18,000 organisations were affected, with costs running into billions.
- Data Source: https://www.fortinet.com/uk/resources/cyberglossary/solarwinds-cyber-attack

6. Uber (2016)

- Details: Attackers accessed a database of sensitive customer and driver data through credentials found in a mismanaged GitHub repository. Uber's lack of visibility into its code repositories and who had access led to the breach.
- Cause of Breach:
  - Poor oversight of developer assets and repositories.
  - Lack of inventory of exposed credentials.
- Impact: $148 million settlement for violating data breach notification laws.
- Data Source: https://help.uber.com/riders/article/information-about-2016-data-security-incident?nodeId=12c1e9d1-4042-4231-a3ec-3605779b8815

7. Anthem (2015)

- Details: Anthem, one of the largest health insurance providers in the U.S., was breached in 2015, compromising the personal information of 78.8 million individuals. The attackers gained access to Anthem's database using stolen credentials.
- Cause of Breach:
  - Insufficient visibility and monitoring of user accounts and internal assets.
  - Lack of strong access controls and oversight on privileged accounts.
- Impact: The breach led to $115 million in settlements, and Anthem spent over $100 million on cybersecurity improvements.

- Data Source: https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm#:~:text=What%20happened%3F,employment%20information%20and%20income%20data.

8. Yahoo (2013-2014)

- Details: The Yahoo breach, which affected all 3 billion accounts, was discovered in 2016. Hackers exploited vulnerabilities in Yahoo's systems over several years, taking advantage of weak internal asset management and security oversight.
- Cause of Breach:
  - A lack of visibility into systems, especially those used for user authentication.
  - Failure to adequately monitor the company's extensive infrastructure.
- Impact: The breach severely impacted Yahoo's valuation and delayed its acquisition by Verizon, which was ultimately sold for $4.8 billion (down from $44 billion).
- Data Source: https://en.wikipedia.org/wiki/Yahoo_data_breaches

9. British Airways (2018)

- Details: British Airways suffered a breach that exposed the personal and financial data of over 380,000 customers. Hackers intercepted user data from its website and mobile app.
- Cause of Breach:
  - Failure to monitor and secure assets across the company's website and mobile applications.
  - Lack of awareness about vulnerabilities in the payment system and customer data storage.
- Impact: British Airways was fined £20 million under GDPR in 2020, down from an initial £183 million due to the company's cooperative response.
- Data Source: https://www.bbc.co.uk/news/technology-54568784

10. T-Mobile (2021)

- Details: In 2021, T-Mobile was breached, exposing data from over 40 million customers. The attack stemmed from the exploitation of a poorly managed API endpoint, which was not monitored adequately.
- Cause of Breach:
  - Inadequate visibility into the company's infrastructure, particularly APIs.
  - Failure to implement proper API security and access control measures.
- Impact: T-Mobile faced public backlash and had to offer free credit monitoring to affected customers. The company also faced a $350 million class-action settlement.
- Data Source: https://www.cshub.com/attacks/news/iotw-hackers-steal-the-data-of-37-million-t-mobile-customers

11. eBay (2014)

- Details: In 2014, eBay experienced a breach where hackers stole encrypted passwords and personal details of 145 million users. The attack happened when

attackers accessed employee credentials and used them to infiltrate the company's network.
- Cause of Breach:
  - Lack of proper segmentation and monitoring of internal employee accounts and IT assets.
  - Failure to track and safeguard administrative credentials.
- Impact: eBay was forced to reset the passwords of millions of users and faced significant reputational damage.
- Data Source: https://www.bbc.co.uk/news/technology-27539799

12. Adobe (2013)

- Details: Adobe suffered a breach that resulted in the theft of 38 million user accounts, including email addresses and encrypted passwords. Attackers accessed Adobe's internal systems through a vulnerability in its content management system.
- Cause of Breach:
  - Inadequate security around internal assets, such as code repositories and sensitive data stores.
  - Weak password policies and encryption practices for stored customer data.
- Impact: Adobe spent $1.1 million on breach notification and related expenses, and it is also facing class action lawsuits.
- Data Source: https://www.bbc.co.uk/news/technology-24740873

13. Sony PlayStation Network (2011)

- Details: Sony's PlayStation Network (PSN) was breached, exposing the personal data of over 77 million accounts. Hackers exploited weak access controls on Sony's network.
- Cause of Breach:
  - Poor asset visibility, leading to lack of segmentation and insufficient network monitoring.
  - Failure to properly secure user databases and monitor for signs of intrusion.
- Impact: Sony incurred costs exceeding $170 million in direct costs, along with substantial reputational damage.
- Data Source: Sony PlayStation Network (2011)

14. Facebook (2019)

- Details: In 2019, an unsecured database exposed the personal data of over 540 million users. The database was stored on an unprotected Amazon Web Services (AWS) cloud server without proper security configurations.
- Cause of Breach:
  - Lack of visibility and monitoring over cloud-hosted assets, leading to the misconfiguration of security settings.
  - Failure to audit and ensure cloud data was properly secured.

- Impact: Although no direct financial penalties were incurred, Facebook faced significant reputational damage.
- Data Source: https://www.forbes.com/sites/larsdaniel/2024/11/18/facebook-data-breach-fallout-millions-may-receive-compensation/#:~:text=The%202019%20Facebook%20Data%20Breach,user%20data%20they%20could%20find.

15. Home Depot (2014)

- Details: Home Depot was breached in 2014, resulting in the theft of 56 million credit card numbers. Attackers entered through a third-party vendor's compromised credentials, exploiting poor asset management and oversight of vendor access.
- Cause of Breach:
  - Weak access controls for third-party vendors and failure to monitor their activities.
  - Insufficient visibility into the company's network and assets, allowing attackers to move laterally.
- Impact: Home Depot incurred an estimated $179 million in costs for breach-related expenses, including legal settlements and security enhancements.
- Data Source: https://www.reuters.com/article/technology/home-depot-reaches-175-million-settlement-over-2014-data-breach-idUSKBN2842W5/

Key Takeaways and Preventive Actions:

- Asset Visibility Gaps: A recurring theme is the failure to properly manage, monitor, and audit IT assets, whether internal infrastructure, cloud assets, or third-party services.
- Unpatched Vulnerabilities: Failing to identify and update software.
- Lack of Segmentation: In many breaches, attackers could move laterally within networks or exploit poorly isolated systems.
- Third-Party Risks: Several breaches highlight the danger of inadequate visibility into third-party relationships and external assets.
- Increased Focus on Cloud & API Security: Many breaches, especially recently, have been linked to cloud misconfigurations and unsecured APIs, emphasising the need for greater asset visibility in these environments.

Preventive Measures:

- Implement automated asset discovery tools to maintain real-time visibility.

- Use vulnerability management solutions to identify and patch risks promptly.
- Conduct regular audits to ensure IT and cloud environments are fully accounted for.
- Employ network segmentation to limit lateral movement within systems.

These cases underline how a lack of asset visibility can significantly increase the risk of breaches.

Third-party reports

https://newsroom.trendmicro.com/2022-06-06-Global-Organizations-Concerned-Digital-Attack-Surface-is-Spiralling-Out-of-Control

https://www.trendmicro.com/explore/trend_global_risk_research_2/the-challenge-of-man