



The Future of CAASM | 2023

Cyber Asset Attack Surface Management

Gain better asset visibility
and improve your security
with CyAmast

CyAmast.com

Digital Assets - The New Face of Risk

We saw the Steam Age shape the Industrial Revolution, giving way in turn to the Electronic and then Digital Age. Now the Digital Age is growing into a more physical-human incarnation. We're at an inflection point produced from the culmination of compute maturity and the ubiquity of network connectivity. We've arrived at a new technological paradigm where our reliance on digital assets, where everything is 'smart' and everything is networked, is almost total.

From manufacturing equipment, to medical devices, to traffic lights, both the sophistication and prevalence of digital assets are exponentially increasing. Used properly, these assets provide unprecedented levels of efficiency, control, and insight that may well mark a new age of prosperity. With the adoption of low-latency and high-bandwidth 5G connectivity paired with the ever-increasing power of edge computing, these devices will continue to become even more prevalent in our lives, bringing a much larger and evermore complex attack surface.

The adoption rate of digital technology is staggering. We already see billions of devices deployed globally, and that number is projected to climb by at least 300% within the next few years, and to continue in its acceleration. While smart homes certainly boost the overall devices numbers, the primary adoption of OT & IoT digital assets will fall to enterprise organisations due to their collective scale.

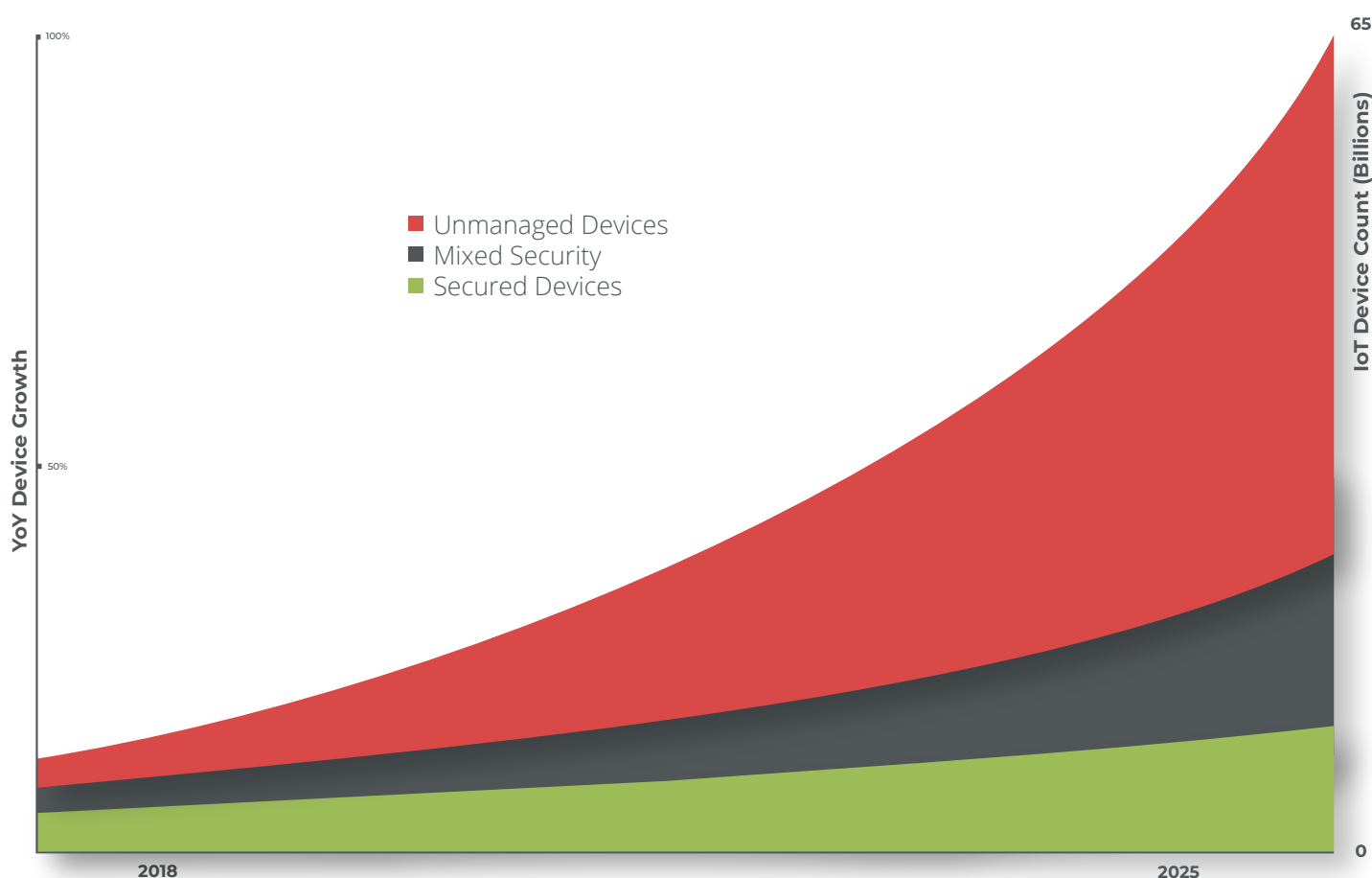



Figure 1. The Growing Risk of the Asset Attack Surface

A Changing World

The vast majority of businesses are still using spreadsheets to track and manage their networked assets, while threat actors are employing the force-multiplier that AI/ML provides to identify and exploit vulnerabilities in these very same assets. Organisations are rapidly losing this game of cat & mouse, and need to use the sophisticated tools at their disposal to level the playing field.

Organisations are still overwhelmed with managing the surge of devices brought about from the Bring Your Own Device (BYOD) movement of the past fifteen years. With the explosion of new OT/IoT devices getting connected to enterprise networks and the expansion of attack surfaces, many are now at the point where new threats are being introduced faster than they can be identified, let alone addressed. And with the COVID-19 Pandemic fuelling a much wider adoption of a Working From Home (WFH) policy, even more haphazard digital transformation efforts have been attempted introducing more poorly secured devices to corporate networks.



The world is changing, and it's changing fast. With so many devices connected to networks, from manufacturing, critical medical devices, to your home security, we're gaining huge increases in terms of automation and overall productivity. The problem is that this speed of adoption and growing reliance on digital assets has led - in so many cases - to security and safety concerns. And that's precisely what we at CyAmast are solving.

- Adam de Jong, CEO

As with many trends, device manufacturers typically rush to market to try and grab market-share quickly. This unfortunately means that there's predictably only nominal security measures taken, if indeed any are taken at all. The rate of device adoption is in itself an issue too. We're dealing with a relatively fixed capability to identify, respond, and remediate security issues, while we have a near infinite appetite for IoT adoption; a seemingly unsolvable conundrum.

While the sheer and obvious potential wider device adoption provides fuels many enterprise implementations, numerous concerns are restricting unfettered adoption. The unique nature of these devices, coupled with their implementation on existing networks, creates new vulnerabilities for enterprise systems and data. It's one thing for a robot vacuum or stereo to be compromised, quite another for the water supply or pacemakers to fail.

Key Challenges for IT Departments



Explosive Growth; There are now billions of connected devices; IoT-related attacks alone are expected to double by 2025



Device Management; Devices are not centrally managed, and many aren't visible to IT departments



Always Accessible; Devices have to be connected to be useful, thus providing a perpetual attack surface



Many OT/IoT devices have limited capacity for embedded security measures, and their heterogeneity makes traditional solutions (firewalls, NAC, etc.) relatively ineffective



Devices are sourced from a diverse set of manufacturers, many of which are vulnerable to low-end, low-quality manufacturing, and high-risk data handling practices

Challenges for IT Leadership



Finding the ideal talent to fundamentally understand security is hard enough, let alone to understand the methods specific to your organisation for asset management



The suite of tools required to monitor increasingly large and complex networks is itself unwieldy, with CISOs needing to now maintain overwatch on countless panes of glass



Compliance challenges are understandably harder to meet with the growing complexity and volume of tools, and the subsequent reporting for any regulatory requirements



To properly protect the organisation, leaders need to be able see and understand the interrelationships between assets, and how that continuously changes

CAASM - A NEW WHOLE FIELD

As one of the most widely-known and influential thinkers on management, Peter Drucker, often quipped; “You can't manage what you can't measure.”. And while organisations are growing increasingly sophisticated with their use of automations seated firmly on top of digital assets, the governance of these assets is all too often from a bygone era.

In the face of increasing risk, what are organisations to do to combat potential catastrophe? By avoiding the move to this new asset-rich paradigm altogether, restricting functionality by limiting data availability, or using air-gapped networks to make them safe, then we've lost the opportunity promised in the first place. So, if you don't have resources to police your entire IT ecosystem manually, what do you do?

And that's where CAASM comes into the picture...

Cyber Asset Attack Surface Management (CAASM) is a rapidly emerging approach to cybersecurity that involves identifying, assessing, and mitigating potential vulnerabilities across digital assets, both inside and external to the organisation.

Typically, the relevant assets include everything from networks & systems, applications, and devices, and through integrations, allow the organisation to centralise the visibility and control of all these assets. This level of integration and visibility translates to better management of the organisation's attack surfaces, and is therefore essential in protecting against cyber threats.

The Power of CAASM

- ☑ Maintain an exact inventory of all devices and their behaviour characteristics, and their operational health in near real-time
- ☑ Understand the complex interrelationships between networked assets to improve security posture
- ☑ The manual collection of asset data is inefficient and infeasible, particularly at scale
- ☑ Automate your organisations audits and compliance
- ☑ Reach beyond the network boundary into cloud-based - as well as on-premises - assets

The Right Solution

Security solutions on the market primarily rely on signatures of malicious behaviours, where the detection system looks for a match in individual elements of network traffic that have already been catalogued. CyAmast has evolved beyond this limited approach, and without needing to limit any operational capabilities.

CyAmast is changing the way networks are secured. I look forward to seeing how they catalyse the full power of more integrated digital networks by providing a more robust asset management and security solution. It's very early days in the emerging and complex space of CAASM, but I believe CyAmast and their unique approach to be well-placed to ensure the safety of all networks – from tiny SMEs to large expertises – as digital transformation fulfils its global promise, and helps usher in a more empowered world.

- Paul Barrett, CEO, Hysata



Asset Discovery

The architecture of CyAmast is such that it can practically scale without limits. From a handful of devices to hundreds of thousands, CyAmast doesn't suffer from increased device scale.



Device Classification

CyAmast is able to passively detect and classify all new and existing IoT devices and sensors, even if using encrypted traffic. This provides an unprecedented level of visibility and control over your device-rich networks.



Continuous Monitoring

CyAmast provides passive (non-invasive) network monitoring without disturbing connected devices. It can integrate (via APIs) with active monitoring tools, optimising their operation.



Analysis and Action

CyAmast protects your critical assets by detecting and stopping anomalous behaviours before they are fully executed, regardless of design or purpose as we examine the fingerprints of network behaviours, not just explicit packet contents.

How It Works

Our dashboards provide a highly informative overview of your network and the connected devices, and users can zoom down to the individual networked assets to see the unique flow of data that provides their unique ‘fingerprint’ and their baseline normal operation.

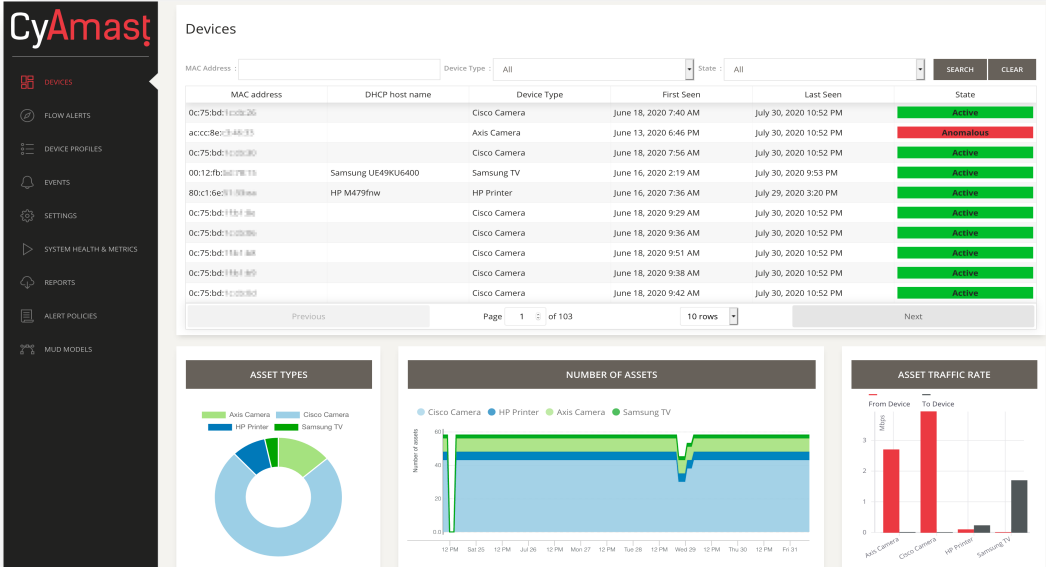


Figure 3. The CyAmast Dashboard - Intelligence at a Glance

Our proprietary solution fully leverages the new advances in Software Defined Networking (SDN), Machine Learning and pattern recognition to define this ‘fingerprint’ for each connected device, specific to its deployed environment. This allows for a solution that can respond to abnormal behaviours as well as unwanted characteristics or configurations; a blind spot for other solutions.

This is tantamount to seeing detailed medical results in real time at the most granular of levels. This means that any possible issue can be investigated at the individual asset level to remediate any compromise or malfunction and enforce security policies.

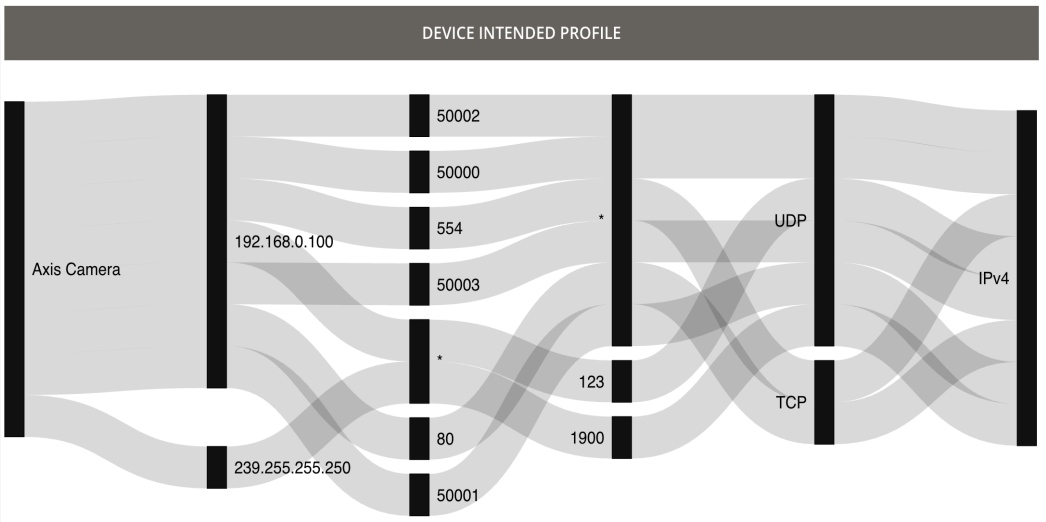


Figure 2. Intelligent Pathing Identification

Leveraging CyAmast for Your Organisation

The unique advantage of the CyAmast approach is it solves all of these problems that traditional security solutions cannot. The proven scalability coupled with attractive accuracy (significantly reduced false positives) is paramount for characterising the behaviour of agentless sensors/devices and detecting corresponding sophisticated cyber-attacks.

CyAmast provides enterprise IT teams with a powerful, cost-effective monitoring, compliance, and forensics tool better to manage the expanded attack surface of networked assets.

Agentless

CyAmast works with every IoT network, independent of the complexity and/or manufacturer of individual devices connected to the network.

A Light Footprint

The efficacy of the CyAmast platform, due to its incredibly small computing footprint, allows it to scale well beyond the needs of large and very large enterprise networks.

Get The Complete Picture

Discovers all networked IT and IoT assets and profiles the behaviour of all active IoT assets. Once identified, patented machine learning-based models classify each device by characteristics such as OS, make and type, and communication protocols. Once discovered and classified, a device inventory is kept and automatically updated in real time. The device behaviour is catalogued, and known behavioural risks are highlighted and explained.

Passive

CyAmast does not inject synthetic traffic (e.g., scans) to effectively monitor a network of assets. It sits parallel to the existing network infrastructure and passively ingests network traffic, providing insights into connected assets and their cyber health. This means zero risk and downtime with installation.

Behavioural Analytics

CyAmast generates a proprietary 'network fingerprint' of individual devices on your network, associated with their characteristics and behaviours. This behaviour identifier enables you to enforce your intended organisational policies and empowers our system to react appropriately once an anomaly is identified -- all on a device-by-device basis.

Forensics and Reporting

The CyAmast platform provides unprecedented forensic intelligence. By tracking the profiles of individual or groups of devices, the CyAmast reporting functionality can identify abnormalities and rogue activities faster and more accurately than any solution on the market.

CyAmast is a unique and proprietary network-level IoT cybersecurity solution that has developed with the enterprise user and cyber security operator in mind. The visibility that CyAmast supplies - from detection, to classification, to monitoring - is second to none. Our goal is to ensure each client has the ability to stay as close to 100% secure and efficient as possible.

- Hassan Habibi Gharakheili, CTO

Securing the Full Promise of Connection

Smart IoT is the future of our connected world. How businesses solve the problems of detection, classification, and active monitoring will separate those that wish to secure a competitive advantage.

CyAmast assists in identifying and addressing potential security issues across the range of possible risks, supply chain issues, hardware, firmware, and software reviews, as well as penetration testing outcomes. This fully validates the end-to-end efficacy of the deployed controls in your OT/IoT environments, and because of our unique architecture, can be across nodes carrying encrypted traffic too.

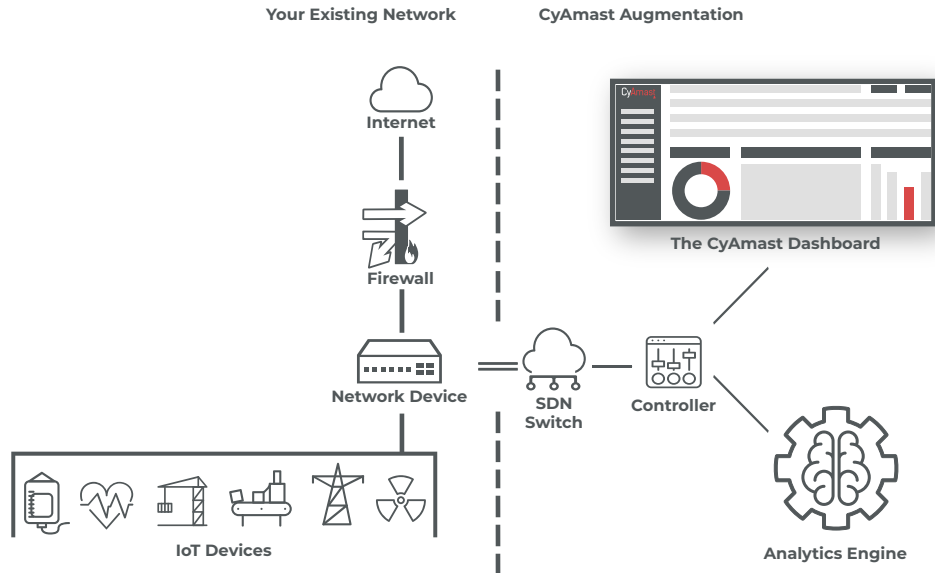


Figure 4. A Simplified CyAmast Architecture

CyAmast leverages programmable switches to provide dynamic and flexible management of high-throughput network traffic, much better and more effective than traditional hardware appliances. It can replace or augment existing infrastructure.

Our solution allows dynamic network management and a solution that is independent of specific devices connected to the network.

Unique Efficiencies

Like everything CyAmast does, we have ensured any of our network implementations - regardless of scale - must be effective and efficient. We have decoupled our inference engines from core infrastructure, and in doing so, allow for scaling into the range of terabits and without dependence on highly customised and expensive infrastructure. For networks requiring <10Gbps we deploy virtually, without the need for additional infrastructure. In cases where >10Gbps needs to be facilitated, we leverage commodity programmable switching (SDN switches).

Our solution is also incredibly efficient due to the tiny computational footprint, making it uniquely scalable, and thus ideal for large enterprises as well as centralised operation centres. These large-scale deployments also benefit our entire userbase by feeding our federated learning engine, improving the performance and security for every implementation across the globe, and providing live, detailed reporting 24/7.

If you wish to understand exactly how CyAmast can improve the performance and resilience of your entire IT ecosystem, reach out and talk with us about how you can address the security flaws in your asset deployments.



Download the CyAmast Trial

The CyAmast Advantage

- Deploy CyAmast across your entire network **without** downtime
- Real-time visibility** and control over your entire IoT-rich network
- Regardless of manufacturer or model, CyAmast provides insights into behaviours and characteristics of every connected asset.
- Instant **health and version status** of all devices with clear actionability
- CyAmast helps stop hackers **before** they can gain a foothold
- Increase the efficacy and security of **all the devices** inside your network and beyond

Detect. Classify. Monitor. Defend.

About CyAmast

CyAmast was built upon proprietary technology researched and developed over many years by our team of globally respected thought-leaders in Software Defined Networking (SDN) and Asset Cybersecurity.

Our Mission is to fulfill the promises that digital devices offer without compromising cyber safety. We have developed an incredibly scalable solution to detect, classify, monitor, and defend asset-rich networks while retaining full functionality for every device from enterprise to critical infrastructure.

Learn More



Join a Webinar



More Learning Resources



Schedule a Personal Demo

Contact Us



info@cyamast.com



+61 (0) 2 9385 4000



CyAmast.com