WHITEPAPER

CAASM - Lansweeper for Cyber Asset Attack Surface Management

Lansweeper

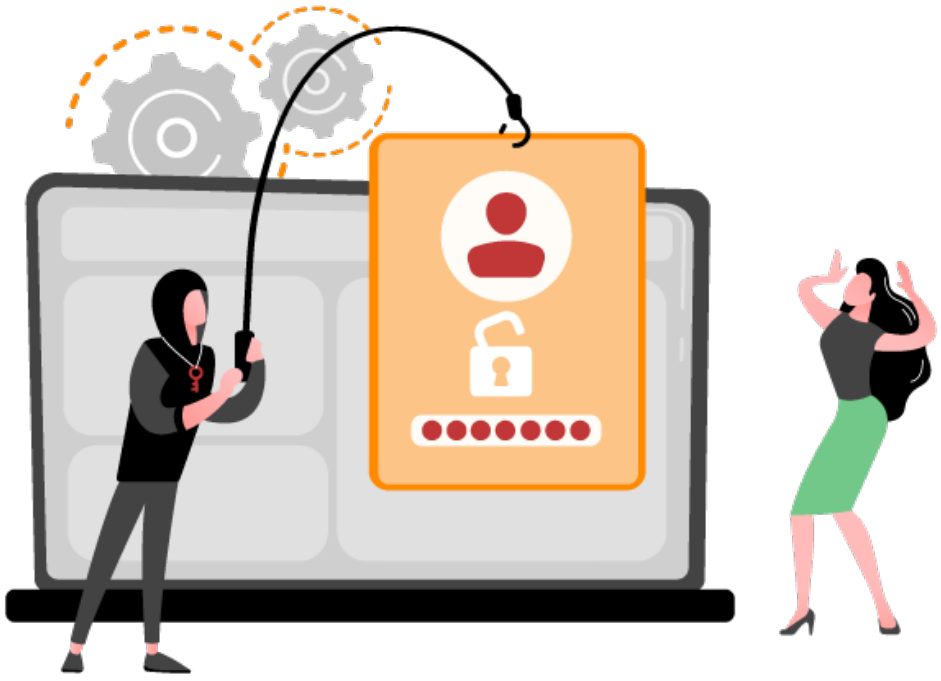
Overcoming the Obstacles of Cyber Asset Attack Surface Management (CAASM): A Quick Guide

You've probably heard the saying, "Only two things in life are certain: death and taxes." Today, we'll have to add another certainty to that phrase: Cybercrime.

While digital transformation, increased adoption of cloud-first initiatives, and the rise of the hybrid workforce are driving unprecedented innovation, increasing productivity and efficiency, and improving customer experience, they also introduce risk. Social engineering scams and ransomware attacks are rampant, and a recent study found that 93% of companies were vulnerable to an external attacker breaching the network perimeter and gaining access to local network resources. Even worse, only 45% have a well-defined way to assess their exposure to risk. The stakes are high – financial losses, data theft or loss, and reputational damage can put an organization out of business.

It's no wonder the market for Cybersecurity solutions is exploding. Growing at a CAGR of 13.4% between now and 2029, the global market for cybersecurity is projected to reach $376.32 billion. In the first half of 2022 alone, a whopping $12.5 billion of venture capital was invested across 531 deals in the cybersecurity space.

While these investments will fuel the development of modern solutions capable of detecting and mitigating threats – and hiring and training IT security specialists to use them – all of the money will be wasted without comprehensive data about the hardware and software assets they promise to protect. Unfortunately, obtaining that critical data is extremely challenging.



More Assets, Not Enough Data

To protect the corporate network, you need to first know exactly what devices and software you have. It's like installing a security system in your home – for reliable protection against a break-in, you need to know how many doors and windows you have to secure. Organizations struggle with discovering and identifying their massive and distributed IT estates, which now consist not only of physical devices and software assets, but virtual assets, operational technology (OT) and Internet of Things (IoT) devices.

Another problem is "shadow IT" – hardware and software assets that are unsanctioned by the IT department and often unprotected – which consumes 30 - 40% of IT spending. What's more, the technology estate is rapidly changing and expanding to accommodate new modes of work and increased digitization.

The majority of security tools available today are focused on threat detection and mitigation, not device discovery and recognition. As a result, they must rely on data from outdated spreadsheets or CMDBs that contain inaccurate or incomplete data. These manual methods of creating and maintaining inventories are slow and error-prone, and can't keep pace with the rate of expansion. As a result, **the vast majority of organizations don't have a complete or accurate technology asset inventory – and therefore cannot possibly understand or protect the attack surface.**

The sheer volume of physical and virtual technology assets IT organizations must track, manage and maintain necessitates new solutions that provide greater visibility and insights – and a reliable, proactive way to manage the rapidly growing cyber-attack surface.

The Problem with IOT and OT

IoT and OT devices are prime targets for hackers and cybercriminals. Even the largest brands with strict security practices are susceptible to attacks:

- About 1.5 billion cyber attacks on IoT devices were reported in 2020, and 80% of organizations do not routinely test their IoT apps for security vulnerabilities.
- OT systems are critical to organizations and the public at large. They're also expensive and intended for long-term use, which means many are old and outdated. Increasingly they're more connected to corporate networks, and without regular patches and upgrades, they can be rife with vulnerabilities that hackers can easily exploit.

A recent study by Trend Micro found that 43% of global organizations said the digital attack surface is "spiraling out of control".

— Trend Micro

Managing the Attack Surface

Not surprisingly, decision-makers are increasing their budgets for cybersecurity tools and solutions. One critical tool to implement will be an effective and comprehensive **Cyber Asset Attack Surface Management (CAASM)** solution that enables an organization to detect and identify any and all assets on the network that could potentially open the door for an attack, via outdated or unpatched software, encryption issues, weak passwords, or misconfigurations. CAASM enables enterprises to isolate and disable shadow IT, unknown or orphaned assets, or any other potential entry points and attack vectors.

CAASM is essential in the modern enterprise, and Lansweeper enables effective CAASM by helping organizations understand the asset attack surface, minimize risk and strengthen its overall cybersecurity posture.

What is the Attack Surface?

The attack surface encompasses all points of entry that can serve as attack vectors for unauthorized users to gain access to a system for malicious reasons.

Lansweeper is uniquely positioned for CAASM, because our technology actually scans all of the devices on the network and extracts it's data from the "bare metal," which means it's more accurate, and provides always up-to-date, trustworthy information – and delivers faster time to value in doing this, compared to other CAASM solutions who often have to rely on ingested IT asset data from other sources before they can start. And what if the data source they work from, is not up to date, incorrect or lacking crucial assets? This could give a false sense of security.

> Cybercrime has increased by 600% since the onset of the pandemic and, by 2025, will cost companies worldwide about $10.5 trillion annually.
>
> — Cybersecurity Ventures

Why CAASM?

To properly manage the growing attack surface, IT organizations must have full visibility into the technology assets they have – including shadow IT. However, for most, there's often no central source of truth containing complete and accurate technology asset data. Manual paper-based processes are error-prone and incomplete, and forgotten or missed assets may be running outdated software or malware, creating security vulnerabilities that will inevitably compromise an organization's data and infrastructure.

What's more, in the hybrid workforce, the BYOD trend has led to employees using personal devices – mobile phones, tablets and laptops – to access corporate resources from anywhere, and they're extremely difficult to track and manage.

Gartner reports that 70% of organizations don't know what assets their organization has, despite governance IT frameworks providing guidance on IT asset management and numerous solutions on the market for managing IT infrastructure.

CAASM helps IT security teams overcome asset visibility and exposure challenges, by providing full visibility into all internal and external technology assets. CAASM tools need accurate, up to date IT Asset data to start from – by either ingesting data via an integration, or by actively scanning the network itself – as this is the starting point. **First you must know what you have, before you can secure it.** Security professionals can query the data to look for potential vulnerabilities and get the information they need to take immediate action to correct any vulnerabilities, misconfigurations or gaps in security controls.

Business Impact of CAASM

The business impact of CAASM is significant. According to Gartner:

"CAASM enables security teams to improve basic security hygiene by ensuring security controls, security posture, and asset exposure are understood and remediated. Organizations that deploy CAASM reduce dependencies on homegrown systems and manual collection processes, and remediate gaps either manually or via automated workflows. Organizations can visualize security tool coverage, support attack surface management (ASM) processes, and correct systems of record that may have stale or missing data."

Source: Hype Cycle for Security Operations, 2022

CAASM provides:

- Complete visibility into your technology assets – IT, IoT and OT – to analyze existing security controls and spot potential vulnerabilities.
- A single source of truth into consistent, complete and accurate data via integrations with other tools such as CMDB, SIEM and ITSM.
- Rapid access to data to satisfy compliance reporting requirements and simplify audits.
- The ability to report on and share data with stakeholders across teams, to achieve various business objectives.
- Better governance and control over shadow IT.

Barriers to CAASM Adoption

Despite the clear benefits of CAASM, many organizations struggle to adopt the practice. IT teams are resistant to implement another tool or solution, or may find it difficult to justify spending budget on one, especially if they have other tools in place that provide partial visibility. Some of the available CAASM solutions don't monitor anything outside of traditional IT, leaving IoT and OT vulnerable – and if they do, they are often cost-prohibitive, especially for large organizations with millions of assets to manage. Scalability and licensing are major factors in the decision-making process, as well as ease of integration with other tools in the technology stack.

When selecting a solution, Gartner recommends the following:

- Ask the vendor for a proof-of-concept or a trial version before you purchase to ensure the products are easy to implement in your environment.
- Determine what you'll be using your CAASM solution for, so you choose a solution with the right capabilities.
- Look for solutions that cover internal and external asset visibility.
- Make sure the solution covers not only IT systems, but IoT and OT systems, as well.
- Prioritize solutions that can be leveraged for various use cases by multiple departments within the organization.

Lansweeper for CAASM

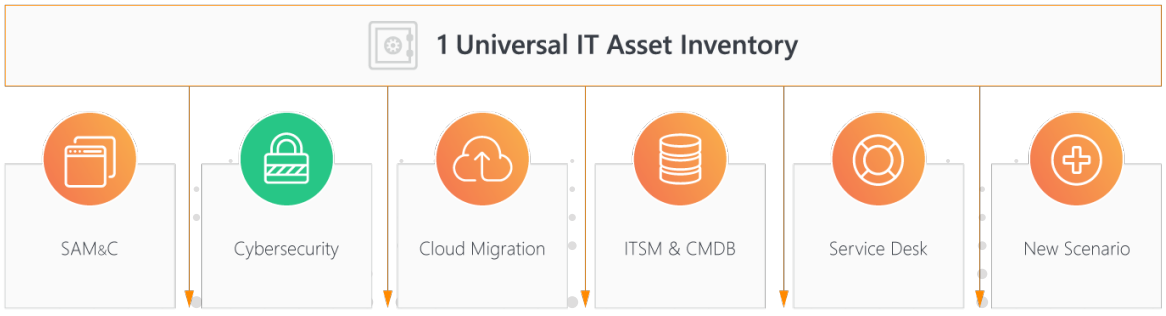
The Importance of Agentless Discovery

The first step to assessing the attack surface area is knowing what technology assets you have to protect.

The first step to assessing the attack surface area is knowing what technology assets you have to protect. Lansweeper leverages an agentless deep scanning engine and credential-free device recognition (CDR) technology to automatically and continuously discover and recognize all IT assets across your infrastructure — servers, laptops, desktops, virtual machines, operating systems, software, OT and IoT assets — to create a comprehensive inventory with detailed IT asset data without the need to install any agent on the devices before you can get started. Because Lansweeper works without agents — and can do an initial scan without the need for credentials — it's fast and easy to implement. In fact, customers can be up and running in minutes, instead of weeks or months with an agent-based solution, and the data is far more complete and accurate.

However, with networks becoming increasingly mobile and complicated, certain assets become harder to reach. Think for example of laptops out on the road, devices at remote locations or machines in protected zones (DMZs). Lansweeper also offers a solution for keeping track of those devices through our installable scanning agent where an agentless approach just can't reach, offering you the best of both worlds.

Lansweeper also aggregates the technology asset data it gathers from other sources, providing an always-accurate single source of truth to inform all business and IT scenarios and enable strategic decision-making. Importantly, IT security professionals can leverage this system of record to analyze the attack surface, pinpoint vulnerabilities and security gaps, and strengthen an organization's security posture to prevent cyber attacks.



Lansweeper for CAASM

Lansweeper's approach differs from that of other vendors because it extracts asset data from the "bare metal." **Developed as a solution for IT asset management (ITAM), the platform is designed to create an always-accurate IT asset inventory, and its deep scanning and asset detection & identification technologies are built on 15 years of expertise in this area.** Other vendors must ingest IT asset data from other sources before assembling an inventory – and those other sources may not be completely accurate or up to date.

Lansweeper detects and recognizes every connected asset across the technology estate:

- All connected hardware assets – workstations, servers, network devices, IoT devices, mobile devices, cloud assets and more.
- Devices that aren't properly encrypted, such as unprotected devices used by remote workers.
- Rogue devices that only touch your network briefly or operate behind the firewall.
- All software with version number, publisher and install date.
- Unauthorized software installs.

How Lansweeper Overcomes Obstacles to CAASM

Let's examine key cybersecurity capabilities of the Lansweeper platform that enable effective CAASM:

- **Unique Deep Scanning Engine:** Lansweeper combines active and passive agentless and agent-based scanning with data aggregation for unprecedented visibility across the IT estate. The solution locates and identifies devices both inside and outside the four walls of a business, in hard-to-reach places and from unexpected sources – all Windows, Linux and Mac devices as well as routers, printers, switches, ports, virtual computers and mobile devices.

- **Instant Credential-free Device Recognition (CDR):** Using Asset Radar, Lansweeper detects assets the moment they connect to the network, however briefly. Lansweeper then applies machine learning techniques and big data to network fingerprinting, to enrich this IT asset data with information about manufacturers, models, users, operating systems and more. It already delivers unmatched inventory accuracy across the entire IT estate, without the need for complex configurations or adding scanning credentials or agents, by using CDR. Additionally, this makes Lansweeper ideal for detecting and managing all kinds of IoT devices on your network.

- **Data from your entire technology estate:** On top of this, Lansweeper also ingests technology asset data from a variety of business-critical systems, such as SCCM, Windows Active Directory, Office 365, Chrome OS and more, providing a complete 360-degree picture of your technology estate. Through an integration with Cloudockit, it also provides detailed information about your cloud environment, via detailed cloud diagrams and documentation.

- **Identify industrial OT devices:** Leveraging proprietary discovery capabilities, Lansweeper for OT correctly detects and identifies OT devices and systems such as programmable logic controllers (PLCs), flow meters, card scanners and other equipment that is traditionally managed separately from IT assets. It collects detailed information about devices from manufacturers such as Siemens, Rockwell Automation, Mitsubishi Electric and Schneider Electric, working with specialized protocols such as Siemens S7 Communication, EtherNet/IP, MELSEC, Modbus (Modicon), BACnet and OPC UA. Organizations gain the visibility and insights they need to reduce the risk of failure and security incidents across their OT infrastructure.

Integrations

There is no single tool that can do it all, so we focus on what we do best - discovering, detecting, and identifying assets on the network. But, we are open and interoperable by design. Through our partnerships, Lansweeper seamlessly connects to a myriad of operational systems across an organization's technology stack, including CMDB, ITSM, SIEM & SOAR tools, and much more.

Feed those systems with always accurate and always up-to-date IT Asset data directly, and unlock enriched IT asset data and insights relevant for a broad range of use cases. This eliminates data silos and the operational overhead associated with chasing down information and toggling between tools to investigate and resolve security incidents. An extensive and growing library of APIs enable customers and partners to leverage Lansweeper data to derive their own unique insights.

- **Data visualization, reporting and BI:** Lansweeper organizes and contextualizes the data it collects according to an organization's projects and processes, making it usable and actionable for a variety of business scenarios. Users can visualize and analyze all data via pre-built and customizable dashboards and widgets to understand patch status, vulnerability exposure, security compliance, software licensing, hardware warranty information, and much more. Advanced reporting features enable teams to retrieve and analyze the data they need when they need it, and easily share that data with stakeholders. Lansweeper also integrates seamlessly with Microsoft Power BI, so you visualize Lansweeper's complete and up-to-date technology asset data alongside other business data for a 360-degree view.

- **Vulnerability reports:** Lansweeper enables you to stay on top of the latest vulnerabilities and run vulnerability reports to expedite patches and updates. We also regularly send new vulnerability reports to our customer base, to use directly in their environment to check for possible vulnerable devices. Additionally, Lansweeper provides a number of reports with information about the anti-virus status of your Windows machines, to help you ensure all devices have the most up-to-date anti-virus software installed.

- **Security Insights:** Lansweeper's Security Insights feature leverages the NIST Vulnerability Database to provide a complete overview of all known vulnerabilities that could pose a threat to your organization, enabling you to easily track what assets may be at risk and prioritize remediation activities in an automated way in Lansweeper Cloud.

> Lansweeper tells us exactly how many devices are still potentially vulnerable, so we can focus our efforts and eliminate that risk for our clients
>
> — Phil Blankenstein, IT Manager, Cerner Corporation

- **Patch Tuesday reports:** With Lansweeper, you can run a Patch Tuesday report to ensure the assets in your network are updated with the latest Windows Patch updates. These reports provide a quick overview so you know which assets are up to date, and which ones require updates, at a glance.

- **Cloud Security with Cloudockit:** Lansweeper has recently acquired Cloudockit, which makes it fast and easy to create complete documentation of all your cloud assets, simplifying and improving IT documentation to assist with security, incident resolution and compliance. The solution automatically visualizes all the details about your cloud components and applications – settings, network interfaces, security groups, tags, launch configurations, warnings and more – and easily spot misconfigurations and potential security risks.

- **Certificates and drivers management:** Lansweeper provides visibility across all certificates, along with details such as expiration dates, to help ensure your devices are always protected. Lansweeper can also scan system drivers, PnP (plug-and-play) drivers and printer drivers installed on Windows computers. Scanned data includes driver name, version, manufacturer, path, state, release date and much more.

Rentokil Initial

Rentokil, one of the largest business services companies in the world, with 44,500 employees and operating in over 80 countries, uses ServiceNow to manage digital workflows for enterprise operations, and they'd also been using its IT asset management capabilities to track and manage IT assets across the enterprise. However there were some gaps in capabilities – they needed a solution that would automatically identify and add assets to the inventory. With more than 25,000 assets to manage, this was a critical capability. After implementing Lansweeper, Rentokil:

- Gained complete visibility and security compliance reporting across all Windows assets.
- Fed accurate data into the CMDB to create a single verified data record for each managed asset.
- Rolled out Lansweeper globally, strengthening the company's security posture.

Read the full case

Lansweeper is our independent eyewitness - providing critical visibility and helping us validate the health and security posture of our IT estate.

— Mark Blackman, Global Configuration Manager, Rentokil Initial

Know Your IT!

Lansweeper simplifies and strengthens CAASM, helping IT teams to:

Maintain full visibility
across the ever-expanding technology estate

Analyze the attack surface
to ensure proactive protection

Streamline compliance
with automatic scanning and reporting

For more information visit www.lansweeper.com.

Lansweeper