ITAM and Cybersecurity: Gain Visibility Across Your Technology Assets to Reduce Risk

Across all industries and market sectors, cybercrime is increasing exponentially, putting intense pressure on IT teams to implement security measures that prevent cybercriminals from launching attacks. About 300,000 thousand new pieces of malware are created every day, and a ransomware attack happens every 11 seconds. Global losses from cybercrime hit $6 trillion in 2021, and 64% of all companies worldwide have experienced at least one form of a cyber attack.

What's driving the surge in cybercrime? The global pandemic was a catalyst for digital transformation across industries, resulting in unprecedented IT sprawl as trends such as BYOD and the hybrid workplace gained momentum. In a typical enterprise, "ghost assets" – assets that are missing – comprise 30% of the IT estate. Meanwhile, IT teams must now manage potentially vulnerable, unprotected, and unauthorized personal and IoT devices that may connect to the corporate network as a result of employees working from home.

Shadow IT is also a problem; teams across the organization often circumvent IT and implement IT infrastructure and services without formal approval, which makes them impossible to track and protect. Forgotten or missed assets may be running outdated software, drivers or even malware, creating security vulnerabilities that can compromise your data and infrastructure and lead to huge financial losses.

Anticipating and intercepting potential cybersecurity attacks is of paramount importance, and requires enforcing best practices and IT policies across the organization in a consistent and thorough way.

Unfortunately, most IT teams still manage their technology assets manually on spreadsheets or by using disparate systems. Since they lack a unified and accurate IT asset inventory, there's no way to standardize cybersecurity protocols across the enterprise or gain full visibility across all the technology assets connected to the network. **If you don't know what's there, how can you secure it?**

Lansweeper

ITAM and Cybersecurity: Data + Insights: Proactive Protection and Threat Isolation

The first step to safeguarding your business is creating a complete and accurate IT asset inventory that provides full visibility across the IT estate. Lansweeper's deep scanning engine and AI-powered Credential-free Device Recognition (CDR) technology deliver unprecedented insight across the entire IT estate, making it easy to scan, detect, recognize and document every IT asset on the network – even rogue devices that only connect briefly.

This enables IT teams to:

- Identify vulnerabilities and apply patches and updates, to ensure security and data protection.
- Monitor the expiration of contracts, software licenses and hardware maintenance, enabling a proactive approach to data protection and management.
- In case of an attack, quickly determine what devices are impacted and where the devices reside, and who's accessing those devices.
- Isolate and shut down impacted devices in minutes, to minimize damages.

> "Lansweeper delivers detailed information about a security incident in minutes, providing incredible time savings and helping us to minimize or eliminate potential damage."
> – Kristopher Russo, Information Security Analyst Architect, Herman Miller

Lansweeper

Deep Scanning Engine

Lansweeper's deepscan engine automatically discovers every device, software and users in your network in minutes. Configure the solution to scan the network by IP range, set critical servers to be scanned, or use active scanning and integrate Active Directory to continuously keep the IT asset inventory up-to-date.

Credential-free Device Recognition

Lansweeper's Credential-free Device Recognition (CDR) technology detects and recognizes every device on the network — even non-scannable devices — without the need for credentials or complex configurations. Lansweeper applies machine learning techniques and big data to network fingerprinting, to enrich IT asset data with information about manufacturers, models, users, operating systems and more, delivering unmatched inventory accuracy across the entire IT estate.

Key Benefits of Lansweeper for Cybersecurity

- Full visibility: Create a complete and always-accurate IT asset inventory in minutes.
- No blind spots: Detect and recognize all connected hardware, software and users – even rogue devices and shadow IT.
- Proactive protection: Roll out patches and upgrades before software and hardware vulnerabilities are exploited.
- Streamlined compliance: Meet CIS® requirements with automatic and continuous scanning and reporting.

Integrations

Organizations can use Lansweeper to enrich incident alerts from SIEM/SOAR solutions with relevant IT asset data, as well. Lansweeper integrates seamlessly with leading security solutions such as Splunk, Palo Alto Cortex XSOAR, MSFT sentinel, IBM QRadar, ArcusTeam and more, unlocking enriched IT asset data and making it instantly accessible from within these tools. This not only makes them more effective and useful, it eliminates data silos and the operational overhead associated with chasing down information and toggling between tools to investigate and resolve security incidents.

Lansweeper

ITAM and Cybersecurity: How We Add Value

Across all industries and market sectors, cybercrime is increasing exponentially, putting While a complete and accurate IT asset inventory is the foundation for any cybersecurity solution, creating one is hard work, especially if you're relying on time-consuming manual processes that are prone to error. Lansweeper does heavy lifting and provides accurate and complete data in minutes.

As a Lansweeper partner, we are familiar with the Lansweeper platform and how to use it correctly to give customers full visibility across their technology estate. Leveraging our extensive expertise in cybersecurity, we can guide you on what data to track and monitor to safeguard your infrastructure and prevent an attack. We can build custom reports depending on your needs and recommend best practices for taking action on data insights. We can also help your team understand what to look for when it comes to potential threats, and how to enforce security policies consistently.

Case in point: B2B Cyber Secure, a cybersecurity advisory company, installed Lansweeper agents on every student's device in a couple of school districts up in Canada. This enabled the students and teachers to work remotely and the IT team to ensure network security. Teams at the various districts can track every device that connects to the network and push out updates and patches to keep all the hardware and software up to date and protected. Read the full case study here.

Contact us today to learn more or get started using Lansweeper to Fight Cybercrime.

Lansweeper