



Lansweeper

Lansweeper | Committed to provide visibility

Lansweeper
2004 | Founded in Belgium

Founded in 2004 | Belgium **Customer** | +24000 with 90% retention **Funding in 2021** | \$158M by Insight Capital Partners
Employee Growth | 100 in 2020 to 342 today **Partner ecosystem** | +460 active partners & +35 integrations



Empowering **IT Heroes** with **accurate data** and **actionable insights** about their **technology environment**.



I(o)T Discovery Leadership

Conclusive data on all devices,
software, users and their relations.



Data to Intelligence

Rationalized information driving
decisions across the organization.



Solution Ecosystem

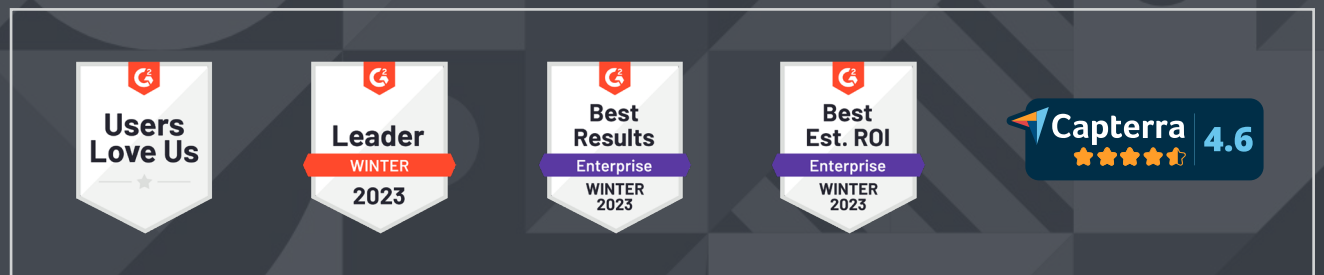
Value delivered with our data, but
beyond our scope.

25,000+
Customers

Across

130+
Countries

Inspire & motivate us
to continue improving Lansweeper.



Lansweeper

"You cannot protect
something you don't know you have!"

30% of organizations admit
to not knowing which IT Assets they own.

43% of organizations still use
spreadsheets to track IT assets.

Knowing your IT at all times enables you to
save up to **30%** of your IT budget.

By 2024, the number of enterprise internal and external hardware and software asset audit requests will increase by **100%**.

The problem

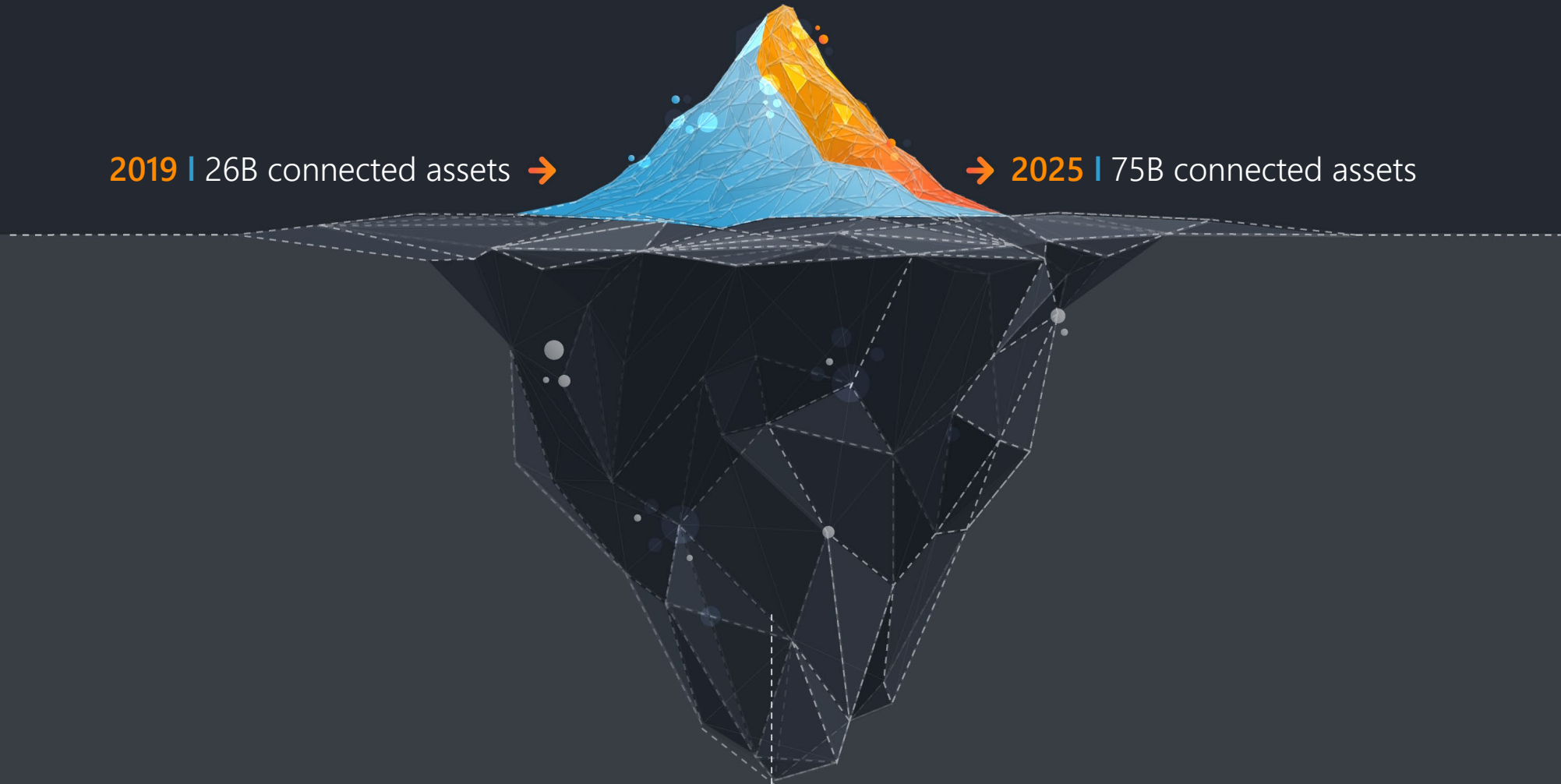
2019 | 26B connected assets →

→ 2025 | 75B connected assets

Technology estate of companies
is increasingly complex



Reduced visibility into IT estate



The problem

You can't manage or protect technology assets you don't know you have



Unmanaged assets create **risks, inefficiencies** and unexpected **costs**



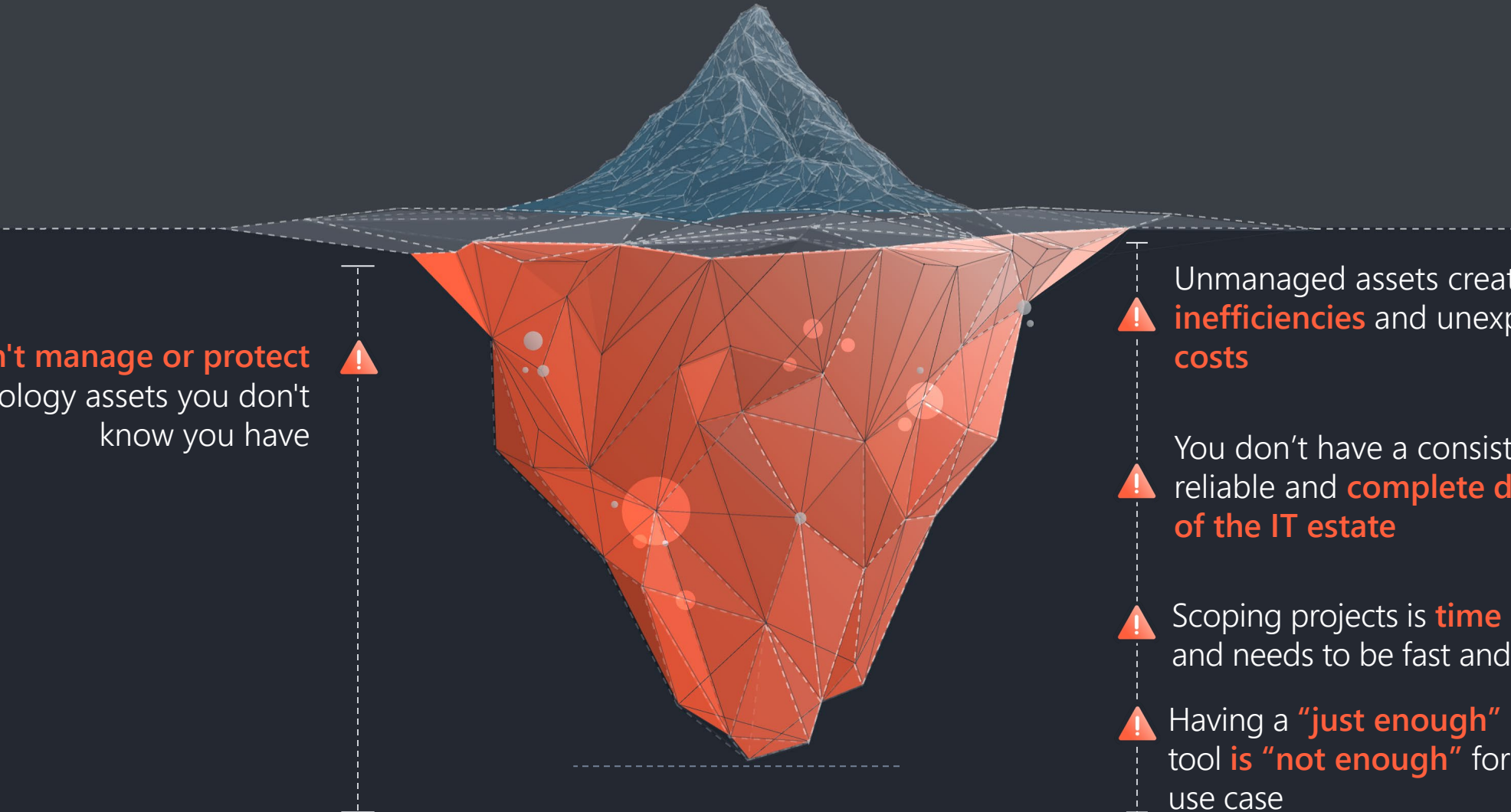
You don't have a consistent, reliable and **complete database of the IT estate**



Scoping projects is **time intensive** and needs to be fast and accurate



Having a **"just enough"** discovering tool is **"not enough"** for customer's use case



The Impact

The High Cost of a Fragmented Approach



Underleveraged &
Redundant Data Silos



Inefficiency &
Misinformed Decisions



Enterprise-wide
Misalignment



Money Being Lost Across
the Board

Creating a new inventory every time a new IT-specific use case is introduced,
is an enormous waste of time and resources.

Common Challenge



Inventory of Assets



Inventory of Devices and Software



Dedicated to ITAM



Inventory of Hardware and Software Assets



Physical Inventory of deployed technology



Service Asset and Configuration Management



Managed I&T Assets



Special Publication on ITAM



Dedicated Industry Body

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



From Directive to Practice

GETTING READY FOR NIS2



The NIS2 Directive provides legal measures to boost the overall level of cybersecurity in the European Union. Compliance is crucial - and mandatory - for organizations operating within the EU or providing services to EU member states. NIS2 introduces significant changes, broadening the scope of compliance and imposing stringent measures to enhance your overall security posture.

The requirements for the NIS2 directive are extensive and meeting them will require a concerted effort from all stakeholders, but **everything starts with knowing your IT environment.**



Lansweeper can help you prepare!

Our Solution

→ **Discover all assets**

IT, OT, IoT and cloud assets with Lansweeper's agent based or agentless scanners

→ **Unify your inventory**

Create and maintain a reliable, centralized database that contains the data on your entire technology estate

→ **Analyze your inventory**

Analyze your technology estate with vulnerability risk assessments, network diagrams & lifecycle information

→ **Integrate seamlessly**

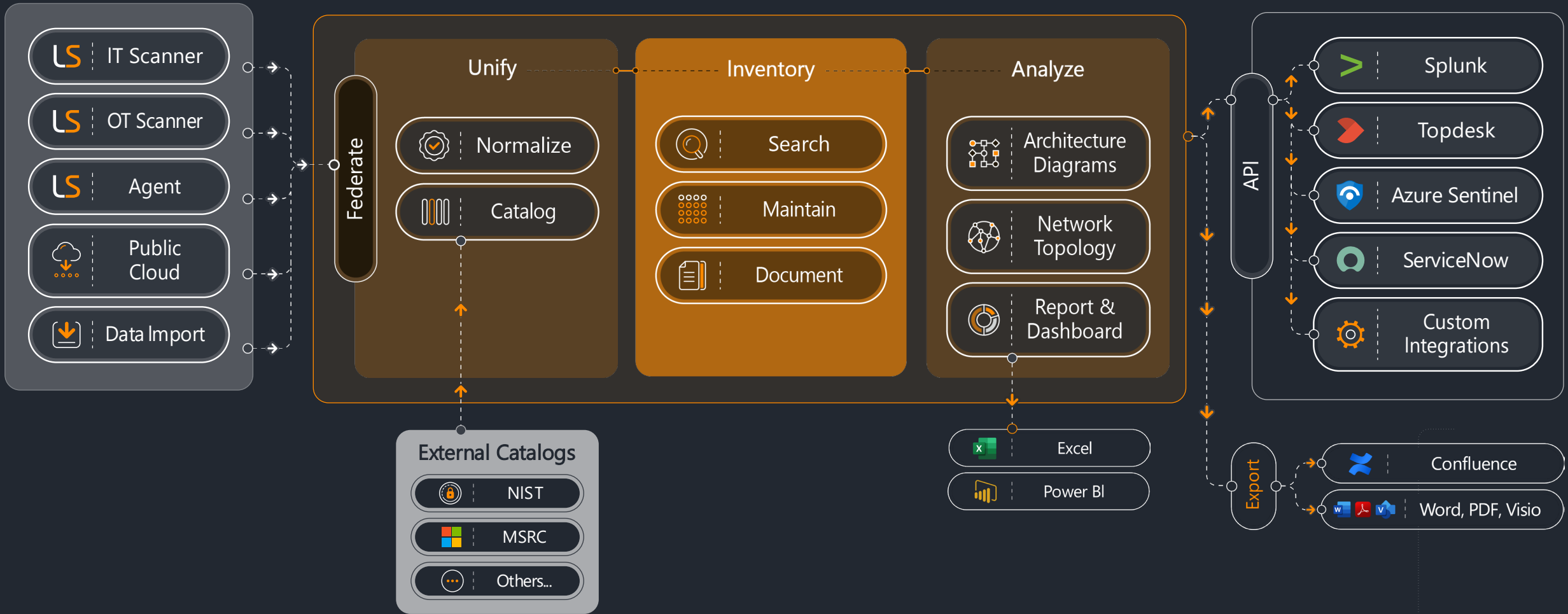
Take action with Lansweeper data in third party applications

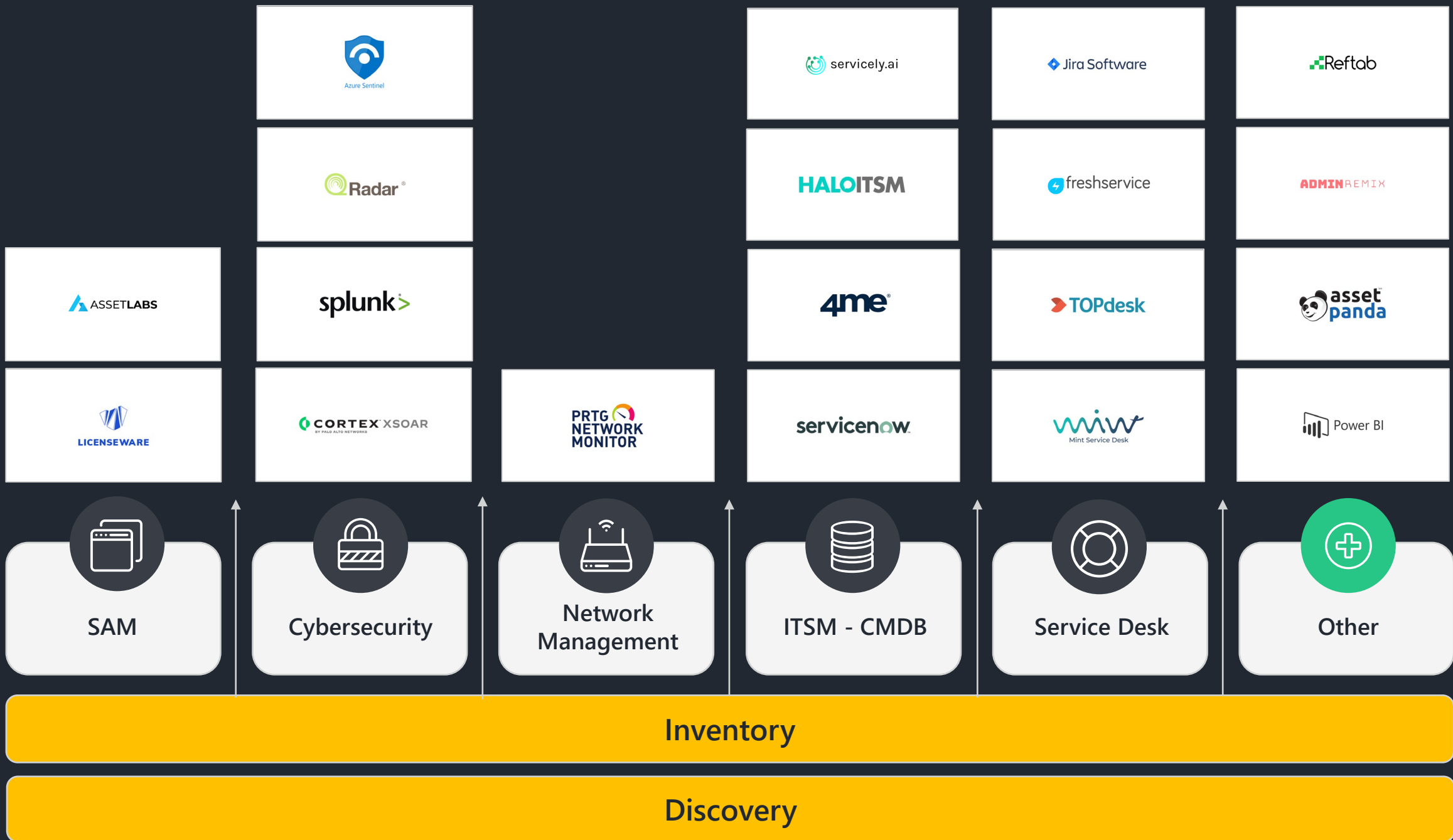


Discover

Analyze & Enrich

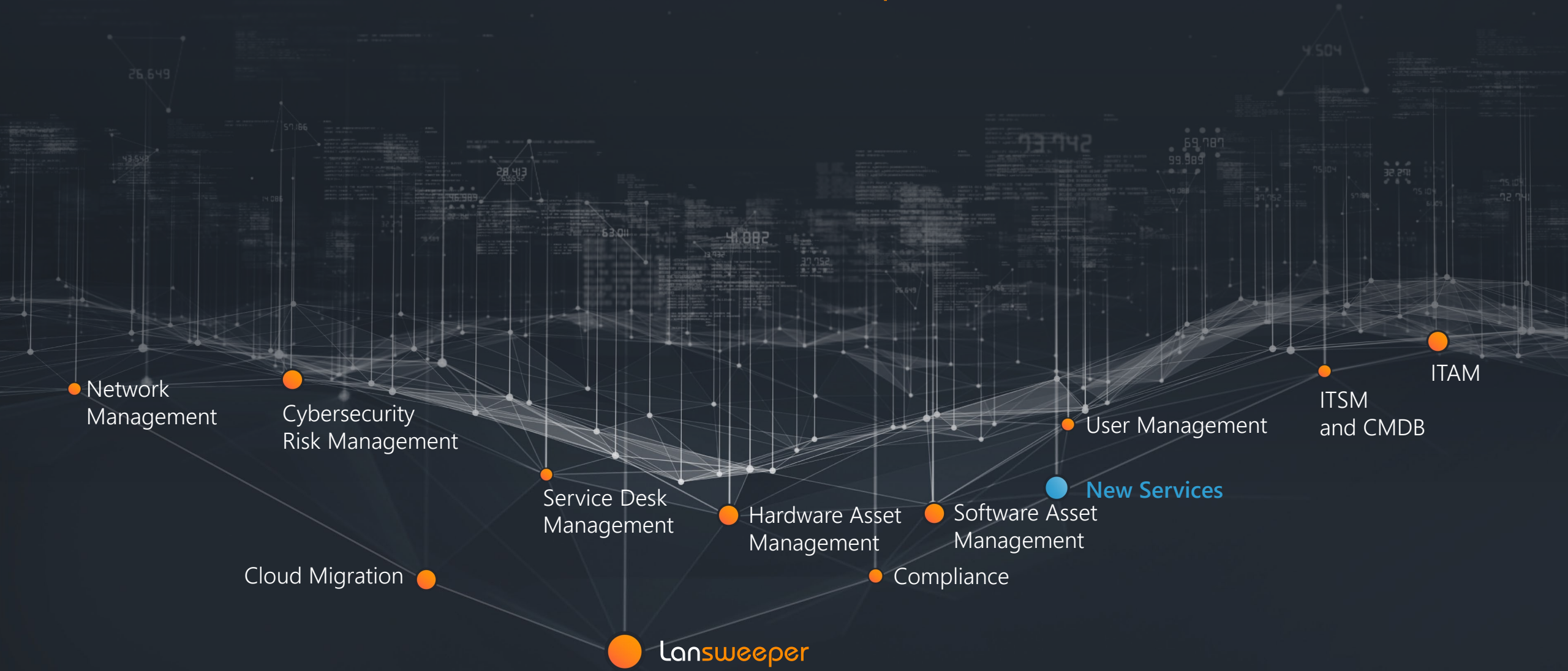
Connect





Scenarios & Use Cases

Technology Inventory Data should not be scenario-specific.



Network Management

Cybersecurity Risk Management

Service Desk Management

Hardware Asset Management

Software Asset Management

Compliance

Cloud Migration

New Services

User Management

ITSM and CMDB

ITAM

Lansweeper

Lansweeper | Our advantage

- Incredibly broad and deep endpoint discovery across Mac, Linux and Windows: IT, OT, IoT and Cloud
- Great time to value, configure and deploy in minutes; have complete inventory within hours.....not weeks
- Greatest value for money in the market
- On prem, hybrid or cloud based
- A single, consistent and thorough source of truth for all applications that require asset data to operate
- Integrations with 3rd party software allows you to get the full value out of the investments you've already made



What's in it for you?

→ **Complete Visibility**

Discover and manage all your IT, OT, IoT and public cloud assets from a single database

→ **Reduced security risks**

Map out all the end points that need to be protected and identify security risks with our vulnerability risk assessment features

→ **Improved efficiency of IT and Cyber security teams**

All IT, OT, IoT and cloud asset data in one place allows for automated record keeping, reporting and more

→ **Cut costs**

Find devices that are EOL, identify underused assets and right size your software licenses based on actual use



Cross-platform Asset Discovery.

Dashboard | All assets

General overview

- Assets: 198
- Software: 5,374
- New devices found in the last 7 days: 1
- Devices not scanned: 45

All Assets

All IT assets were updated | Last full inventory sync: 1 minute ago

NAME	TYPE	DOMAIN
1766-L32XBKA C/21.07	OT	-
1769-1MER/B LOGIX316ER	OT	-
2080-LC20-20QwB	OT	-
AHCPUS9-EN	OT	-
AP2	Wireless Access Point	DEMO
ASM	Webserver	-
AUMac-190	Apple Mac	DEMO
AUMac-191	Apple Mac	DEMO
AUPC-163	Windows	DEMO
AUPC-189	Windows	DEMO
AUPC-198	Windows	DEMO
AUPC-192	Windows	DEMO
AUPC-195	Windows	DEMO
AXC F 252	Windows	DEMO
BMEH58604	Windows	DEMO
C7003D4X	Windows	DEMO
Chromeboo	Windows	DEMO
Chromecast	Windows	DEMO

Asset type details for AUPC-198:

- Asset type: Windows
- OS: Microsoft Windows 10 Ente
- OS Build: 10.0.19044.1826
- OS Version: 21H2
- IP Location: DEMO Subnet
- FQDN: Workstation2.company.local
- Manufacturer: Dell Inc.
- Model: Latitude 5521

A detailed view on every asset.

AUPC-192 | 192.168.2.70 | 74.78.27.FF.17.8E

Summary

- ASSET TYPE: Windows
- OS: windows 10 enterprise (64 bit)
- IP Location: DEMO subnet
- Domain: DEMO
- State: Active
- Model: Latitude 5511
- Memory: 16 GB - DDR4
- Processor: Intel Core i7-10850H CPU @ 2.70GHz
- Serial Number: Workstation2
- ESX Server: -
- SCCM Server: -
- Hardware: Intel(R) UHD Graphics - 1 GB
- Hard Disk: 347.84 GB free of 474.29 GB
- C OS: -

Network

NAME	MAC ADDRESS	IP ADDRESS	SUBNET	MASK	GATEWAY	CONNECTION	LAST SEEN
Intel(R) Ethernet Connection (I) 1219-L4	74.78.27.FF.17.8E	192.168.2.70	255.255.255.0	.64	128.64	192.168.0.1 - 1480.6402.8871.6455.c6	-

Financial information

PO NUMBER	PO Date	Vendor Name
-	-	-
Purchase Date	Invoice Number	Acquisition Type
-	-	-
Cost Center	-	-

Identify critical vulnerabilities and threads.

Active Vulnerabilities

CVE	RISK SCORE	SEVERITY	ASSETS	ATTACK VECTOR
CVE-2020-1350	10	Critical	16	Network
CVE-2020-1472	10	Critical	16	Network
CVE-2020-1102	9.8	Critical	16	Network
CVE-2021-24094	9.8	Critical	135	Network
CVE-2021-1694	9.8	Critical	135	Network
CVE-2021-56965	9.8	Critical	119	Network
CVE-2022-24491	9.8	Critical	16	Network

CVE-2021-1694 Details

- Summary:** Assets: 320, Comments: 0
- Description:** Windows 10 Update Assistant Elevation of Privilege Vulnerability
- Severity:** Critical
- Published:** 2019-07-12, 04:15:32 PM
- Updated:** 2019-07-12, 04:15:32 PM
- Source:** Microsoft Corporation
- Last calculated:** 2021-02-08, 12:35:08 PM
- CVSS v3.1:**
 - Attack vector: Local
 - Attack complexity: Low
 - Privileges required: None
 - Integrity: High
 - User Interaction: Required
 - Confidentiality: High
 - Availability: High

Track IT assets throughout the lifecycle & optimize costs.

Lifecycle

- HW already on EoL: 11
- HW already on EoS: 4
- OS already on EoL: 133
- OS already on EoS: 3
- HW EoL in 1 year or less: 0
- HW EoS in 1 year or less: 2
- OS EoL in 1 year or less: 203
- OS EoS in 1 year or less: 3

Visualize lifecycle information on your asset

Get insights from the Lifecycle dashboard

DEVICE	END OF LIFE	END OF SUPPORT	TOTAL ASSETS
No results			

Life cycle information for Operating system:

- Status: 2018-03-23 Available
- 2022-09-12 End of Life
- 2023-01-01 End of Service

Life cycle information for Hardware:

- Status: 2018-02-21 Available
- 2022-07-02 End of Life
- 2023-01-01 End of Service

Lansweeper

Francois LEENS

Head of Channel Partners EMEA – APAC Regions

Email: francois.leens@lansweeper.com

Mobile: +32.472.29.20.24

MULTIPOINT GROUP
Cyber Strong Solutions

Lansweeper