

# ISO 27001 COMPLIANCE WITH LANSWEEPER: A PRACTICAL GUIDE



ISO 27001 is a widely recognized standard for Information Security Management Systems (ISMS) and serves as the foundation for many other security frameworks. Organizations often use it as a baseline for regulatory compliance, risk management, and overall security posture. Its structured approach helps businesses protect sensitive data, demonstrate compliance, and build trust with stakeholders.

## **Lansweeper for ISO 27001 Compliance**

This guide is designed to help you on your journey toward ISO 27001 compliance, breaking down the key steps—assessing your current security measures, implementing an ISMS, and preparing for certification. Whether you're pursuing full certification or simply strengthening your security framework, this resource provides a clear path forward.

It offers an overview of the four sections of controls that make up Annex A, with a deeper dive into the controls where Lansweeper can make the biggest impact—primarily in sections 5 and 8. Lansweeper helps you cover 75% of the technology-dependent controls, providing a solid foundation for your compliance efforts.

## Annex A

Annex A of the ISO 27001 policy describes **a series of controls that provide guidance on the implementation of information security policies**. They provide direction on how to implement your policies to meet relevant laws and regulations while still in line with your organization's requirements. Not all of these controls are mandatory. You can choose the controls that best align with your organization's security needs, as established during your risk assessment and in your ISMS. The controls in Annex A are divided into 4 sections:

- **A.5 Organizational Controls**
- **A.6 People Controls**
- **A.7 Physical Controls**
- **A.8 Technological Controls**

## Lansweeper for ISO 27001 Compliance

### Annex A

<b>Annex A.5: Organizational Controls</b> .....	01
5.7 Threat Intelligence .....	01
5.9 Inventory of Information .....	04
5.10 Acceptable Use of Information and Other Associated Assets .....	06
5.11 Return of Assets .....	08
5.12 Classification of Information .....	09
5.13 Labelling of Information .....	10
5.14 Information Transfer .....	12
5.15 Access Control .....	15
5.16 Identity Management .....	16
5.17 Authentication information .....	18
5.18 Access Rights .....	19
5.23 Information Security for Use of Cloud Services .....	19
5.25 Assessment and Decision on Information Security Events .....	20
5.26 Response to information security incidents .....	22
5.28 Collection of Evidence .....	22
<b>Annex A6: People Controls</b> .....	24
<b>Annex A7: Physical Controls</b> .....	24
7.4 Physical security monitoring .....	24
7.7 Clear desk and clear screen .....	25
7.8 Equipment siting and protection .....	26
7.9 Security of assets off-premises .....	28
7.14 Secure disposal or re-use of equipment .....	28

<b>Annex A8: Technological Controls</b> .....	29
8.1 User End Point Device .....	29
8.2 Privileged Access Rights .....	32
8.3 Information Access Restriction .....	33
8.6 Capacity Management .....	34
8.7 Protection Against Malware .....	36
8.8 Management of Technical Vulnerabilities .....	38
8.9 Configuration Management .....	39
8.10 Information Deletion .....	41
8.12 Data Leakage Prevention .....	42
8.13 Information Backup .....	43
8.15 Logging .....	43
8.16 Monitoring Activities .....	45
8.17 Clock Synchronization .....	46
8.18 Use of Privileged Utility Programs .....	47
8.19 Installation of Software on Operational Systems .....	46
8.20 Networks Security .....	48
8.21 Security of Network Services .....	48
8.22 Segregation of Network .....	48
8.24 Use of Cryptography .....	49
8.27 Secure System Architecture and Engineering Principle .....	50
8.31 Separation of Development, Test and Production Environments .....	50
8.32 Change Management .....	51
<b>Discover What Lansweeper Can Do for Your ISO 27001 Certification</b> .....	52

## Annex A.5: Organizational Controls

Section 5 of Annex A deals with organizational controls and consists of 37 controls. These controls focus on policies, procedures, responsibilities, and any other measures that can be taken on the organizational level to improve the effectiveness of your information security strategy. This includes controls about:

- Security policies and other core business policies supporting your ISMS
- The duties and responsibilities of the management and any other staff responsible for the day-to-day implementation of your ISMS
- Contact with relevant authorities and other relevant interest groups
- Threat intelligence and monitoring
- Identity and access management
- Classification and labeling of information
- Vendor and supply chain management
- Incident response and business continuity
- Asset management

Of the 37 controls in section 5, Lansweeper can directly or indirectly assist with 15.

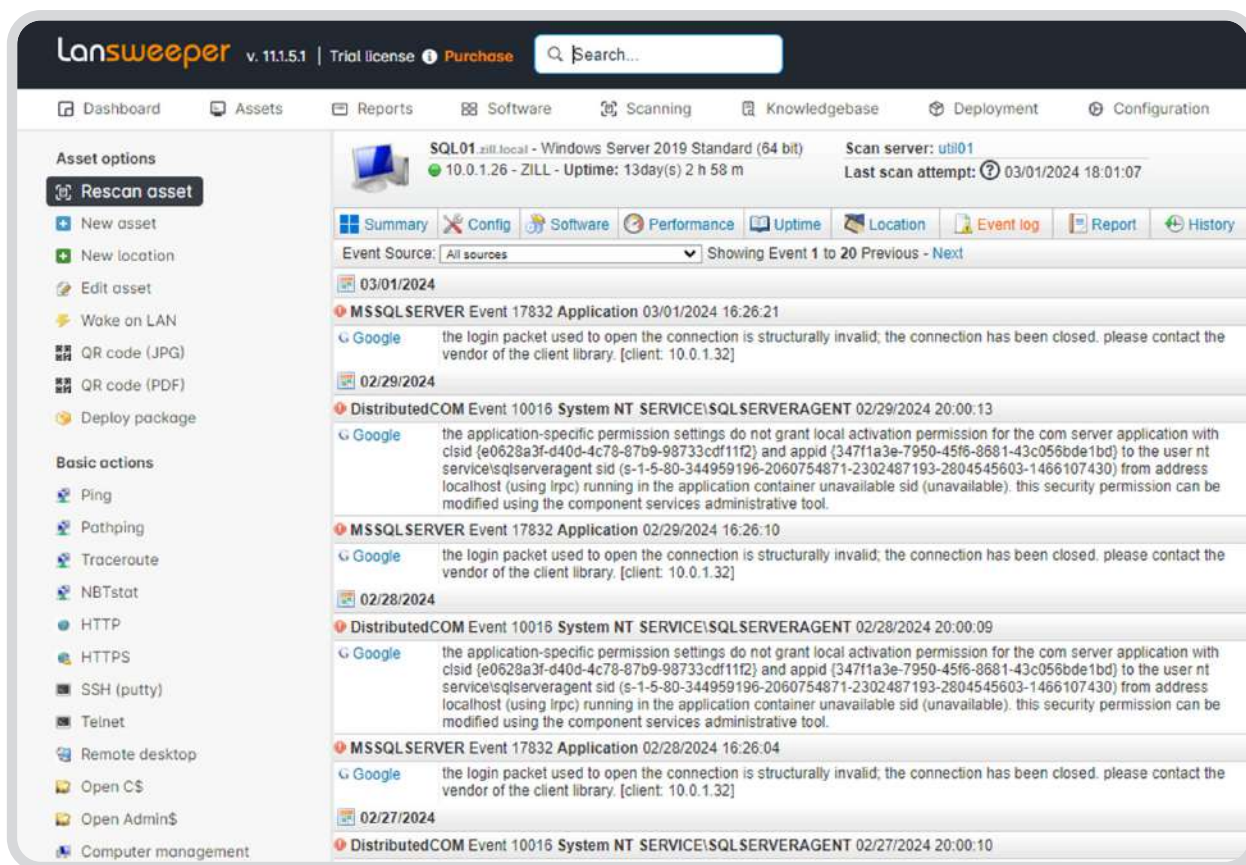
### 5.7 Threat Intelligence

Control 5.7 is about gathering and examining information on potential security threats to create what's known as threat intelligence. This involves collecting data on the kinds of security risks that could affect your organization and then analyzing this information to understand how these threats could impact your day-to-day operations. This allows you to stay ahead of potential security issues so that you can prepare and protect yourself more effectively against cyber threats. There are several ways Lansweeper helps you collect relevant data for threat intelligence.

**Lansweeper's Risk Insights feature** compares the comprehensive asset data Lansweeper collects to known vulnerability data from the VulnCheck, CISA, and MS databases. Based on this information it compiles a list of at-risk assets in your network and the vulnerabilities that are threatening them. For each vulnerability, you will also find additional details like CVSS scores, patch availability, and additional resources. This allows you to prioritize and address vulnerabilities promptly, cutting down response times and strengthening your defenses against potential breaches.

Vulnerable assets					
<input type="checkbox"/>	NAME	SEVERITY: CRITICAL	SEVERITY: HIGH	SEVERITY: MEDIUM	TYPE
<input type="checkbox"/>	ZORLSRV01.zorin.local	150 vulnerabilities	855 vulnerabilities	727 vulnerabilities	Linux
<input type="checkbox"/>	METLHYP01	98 vulnerabilities	252 vulnerabilities	186 vulnerabilities	Citrix XenSe...
<input type="checkbox"/>	CONHQLWS02.contoso.local	90 vulnerabilities	362 vulnerabilities	403 vulnerabilities	Linux
<input type="checkbox"/>	10.40.32.4	87 vulnerabilities	392 vulnerabilities	415 vulnerabilities	Linux
<input type="checkbox"/>	UVMFRANK-SQL	86 vulnerabilities	1096 vulnerabilities	568 vulnerabilities	Windo...
<input type="checkbox"/>	UVMMac-Esben	83 vulnerabilities	839 vulnerabilities	582 vulnerabilities	Apple M...
<input type="checkbox"/>	UVMSTMAC-ESBEN	76 vulnerabilities	576 vulnerabilities	479 vulnerabilities	Apple M...
<input type="checkbox"/>	CONHQLWS01.contoso.local	74 vulnerabilities	311 vulnerabilities	348 vulnerabilities	Linux
<input type="checkbox"/>	UVMCentOS-Esben.dmz.lab.local	74 vulnerabilities	315 vulnerabilities	362 vulnerabilities	Linux
<input type="checkbox"/>	UVMDEVTOOLS01	65 vulnerabilities	877 vulnerabilities	381 vulnerabilities	Windo...
<input type="checkbox"/>	CONHQLWS03.contoso.local	62 vulnerabilities	309 vulnerabilities	351 vulnerabilities	Linux
<input type="checkbox"/>	UVM-W11-BART	59 vulnerabilities	1111 vulnerabilities	413 vulnerabilities	Windo...
<input type="checkbox"/>	UVMW10-ROOROO	57 vulnerabilities	589 vulnerabilities	346 vulnerabilities	Windo...
<input type="checkbox"/>	Android-4.fritz.box	55 vulnerabilities	485 vulnerabilities	555 vulnerabilities	Mobile
<input type="checkbox"/>	Android.fritz.box	55 vulnerabilities	485 vulnerabilities	555 vulnerabilities	Mobile

**Lansweeper collects and monitors event logs** from across the network, to help identify patterns and anomalies that could indicate security threats. It gives you detailed visibility into system events, which helps with early detection of potential issues, enabling timely analysis and response to security incidents, and improving your organization's overall security posture and resilience against information security threats.



**Lansweeper's asset change history tracking** feature systematically records any changes made to your hardware, software, configurations, and permissions. These records provide a comprehensive overview of your IT environment's evolution. Thanks to the detailed tracking, you can easily identify unusual or unauthorized changes, contributing to your threat intelligence by highlighting potential vulnerabilities or indicators of compromise. This approach lets you proactively enhance your security posture and plan your timely response to any emerging threats.

**Lansweeper's powerful and granular reporting capabilities** can help you create a security baseline. Compare your assets to these baselines and alert on any deviation. Over 400 built-in or custom reports provide you with detailed insights into the status of your entire IT network. Antivirus status, running services, required software and/or agents, registry key values and file versions, unapproved software, unauthorized local administrators, and more - Lansweeper helps ensure compliance to your baseline security standards.

**Integrate Lansweeper's technology asset data with your tech stack.** Lansweeper integrates into leading cybersecurity applications like Splunk, Palo Alto Cortex XSOAR, Threat-Aware, DeepSurface, Microsoft Sentinel, and more. Lansweeper's detailed asset data helps to improve your threat intelligence quality and provides additional context to threat intelligence already detected.

## Relevant Reports:

- Windows Error events generated in last 7 days
- Software Changes in the last 7 days
- Newly Discovered Software in the Last 7 Days
- Antivirus Installed Audit
- BitLocker Drive Encryption Audit
- Hardware Lifecycle Overview

## 5.9 Inventory of Information

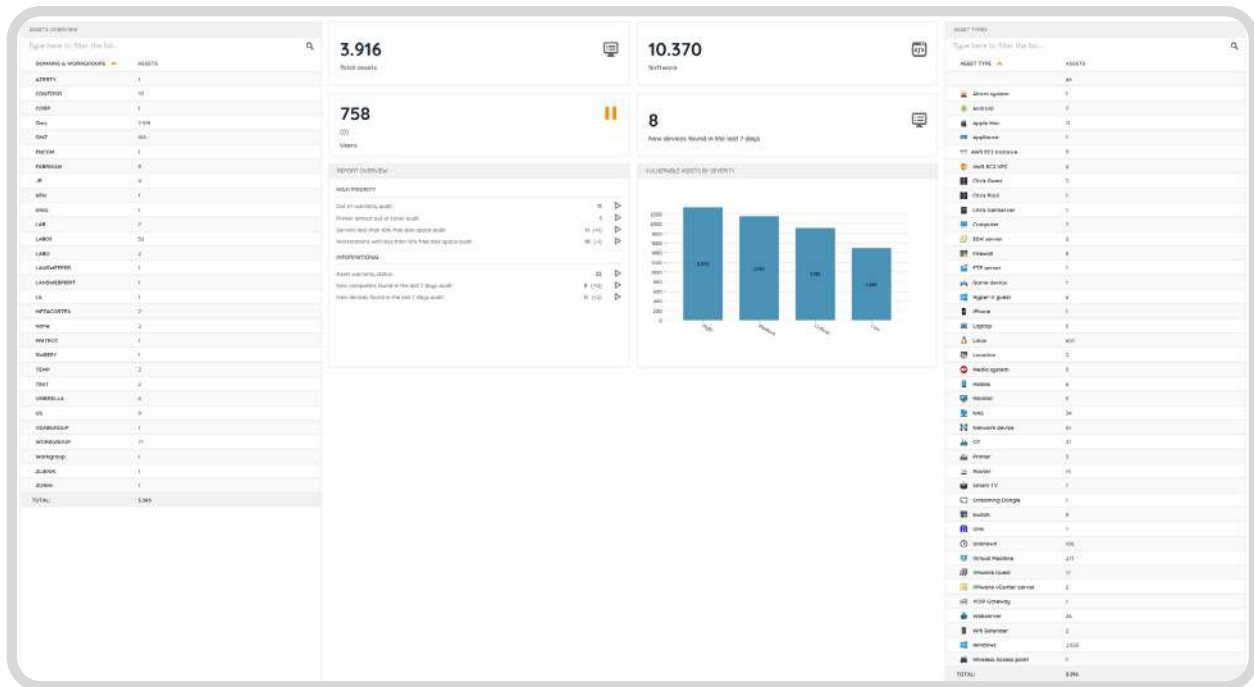
**Control 5.9 calls for the creation and upkeep of a detailed list of all information and assets related to the organization's operations**, including identifying who is responsible for each. This inventory helps in understanding what assets the organization has, where they are located, and who is accountable for them, ensuring that all assets are properly managed and protected. Keeping this inventory updated is crucial for effective information security and asset management.

**Lansweeper automates asset discovery and inventory**, eliminating manual entry and reducing the risk of human error. This not only saves time but also ensures your inventory is as accurate and up-to-date as possible. By leveraging a combination of agentless and agent-based discovery, along with passive scanning, Lansweeper detects every hardware device and software installation on your network—even those that might be overlooked in manual checks. Any device that so much as touches your network is identified, providing a comprehensive and reliable inventory.

**Classify your assets** based on Lansweeper's detailed, comprehensive, and customizable inventory data. You can organize assets by type, location, model, and more, helping you determine the importance and sensitivity of each asset.

**Track which user is using which asset**, to make it easier to assign ownership. Thanks to the integration with Active Directory, EntraID, and Exchange you can link devices to specific users or departments, simplifying ownership assignment.

**Create a central unified inventory** of all assets, which can be accessed and customized through a web-based interface. This means you always have an up-to-date single source of truth for all IT-related projects and processes. Information about each asset is detailed, including specifications, current status, and associated users.



**Tracks changes to assets** over time. Lansweeper logs when software is installed or removed, when hardware components are changed, and when other alterations are made, ensuring that the inventory remains up-to-date. It also creates a historical record of said assets and the changes made to them over time.

**Lansweeper reporting feature** provides you with 400 built-in that can help identify risks, such as unauthorized software installations or hardware changes, as well as a report builder to create your own custom reports. Customized alerts can notify the appropriate personnel of these risks when the report picks them up. **Vulnerability and Risk Insights** give you a comprehensive list of assets that are being threatened by known vulnerabilities, based on vulnerability data from the VulnCheck, VulDB, CISA, and MS databases.

**Integrate Lansweeper** with your tried and trusted ITAM solutions like Asset Panda, Setyl, Timely, and more to improve data quality and so that no asset goes unnoticed. Populating your inventory with granular asset data about all network-connected hardware and software assets.

### Relevant Reports:

- Asset to user relations
- Computer Memory Changes
- Startup Applications History
- IP History

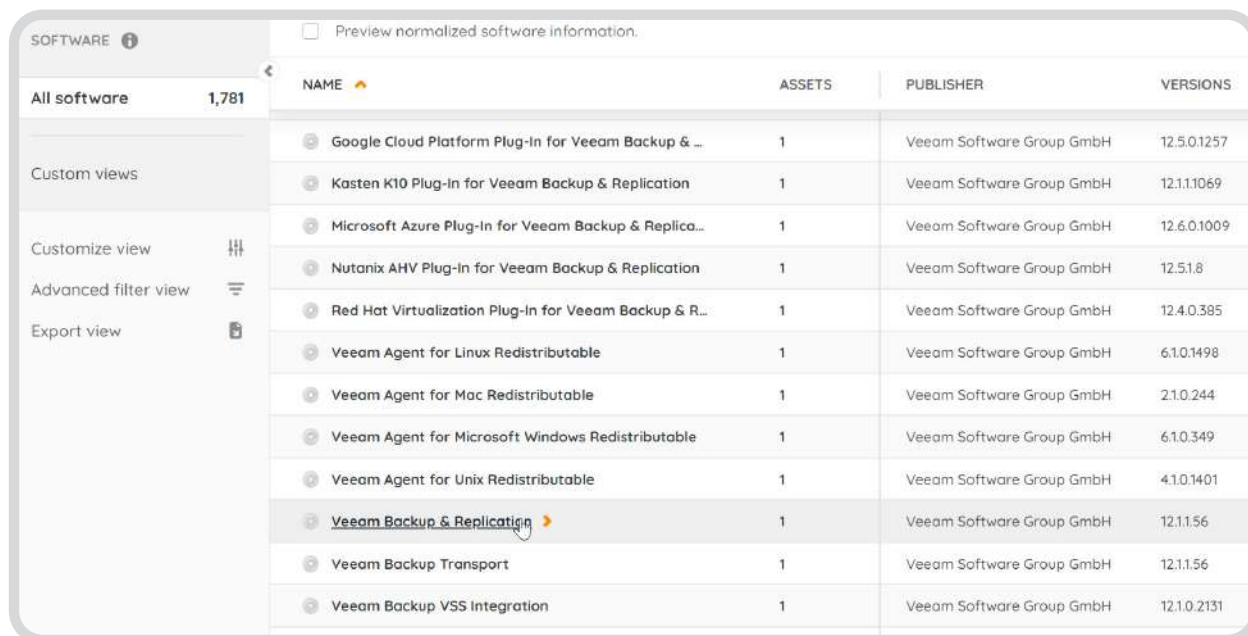
## 5.10 Acceptable Use of Information and Other Associated Assets

**Control 5.10 focuses on establishing clear rules for how information and related assets should be used, along with procedures for their management.** This involves defining, documenting, and putting into practice guidelines that dictate acceptable and secure ways to handle and interact with organizational assets. The aim is to ensure that all individuals understand their responsibilities and the correct procedures for using and managing information assets, thereby protecting the organization's data from misuse or unauthorized access.

Lansweeper can help you collect the asset data you need to create guidelines for use and handling of your critical technology assets.

**Through inventory analysis:** By providing a complete inventory of assets, Lansweeper can help identify what rules and procedures are needed for different asset types. The acceptable use of software can differ from hardware, and specialized equipment might need specific handling procedures. For example, Lansweeper can help you identify critical infrastructure servers that contain critical or confidential information so that you can set up specific policies to better protect them.

**Classify your assets** based on Lansweeper's detailed, comprehensive, and customizable inventory data. You can organize assets by type, location, model, and more, helping you determine the importance and sensitivity of each asset.

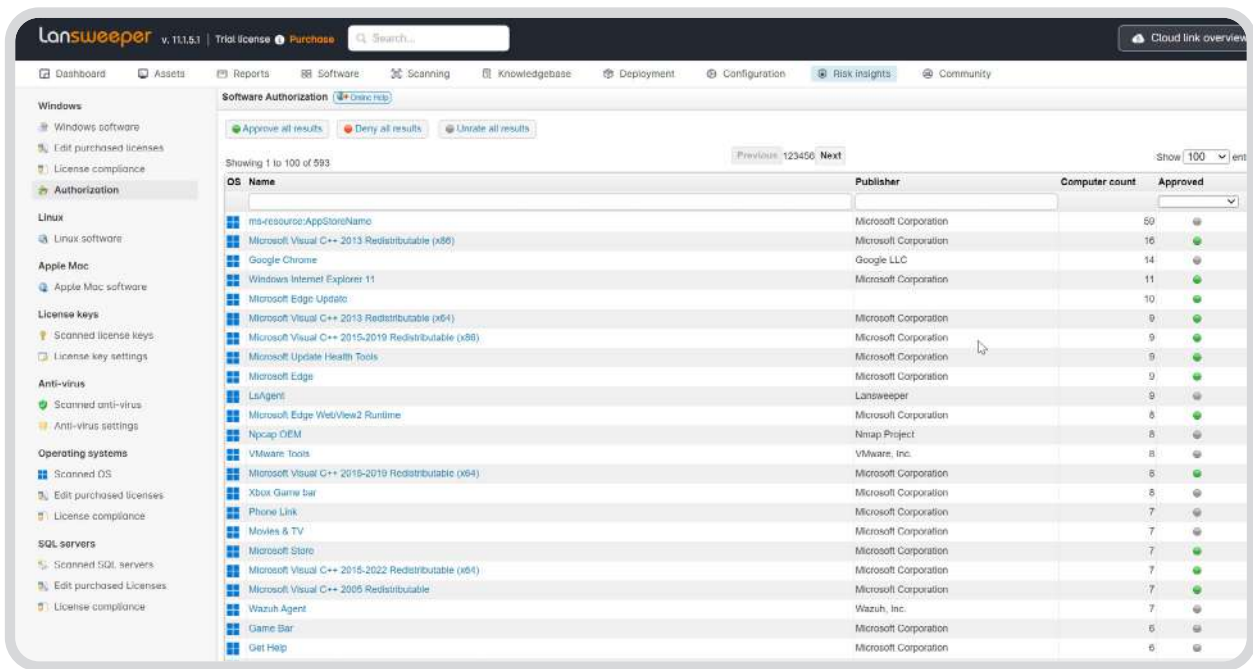


The screenshot displays the 'SOFTWARE' section of the Lansweeper interface. It features a sidebar on the left with options for 'All software' (1,781 items), 'Custom views', 'Customize view', 'Advanced filter view', and 'Export view'. The main area shows a table of software assets with columns for 'NAME', 'ASSETS', 'PUBLISHER', and 'VERSIONS'. A checkbox at the top right allows for 'Preview normalized software information.' The table lists various Veeam software components, including Google Cloud Platform Plug-In, Kasten K10 Plug-In, Microsoft Azure Plug-In, Nutanix AHV Plug-In, Red Hat Virtualization Plug-In, and several Veeam Agent versions for different operating systems. The 'Veeam Backup & Replication' entry is highlighted with a mouse cursor.

NAME	ASSETS	PUBLISHER	VERSIONS
Google Cloud Platform Plug-In for Veeam Backup & ...	1	Veeam Software Group GmbH	12.5.0.1257
Kasten K10 Plug-In for Veeam Backup & Replication	1	Veeam Software Group GmbH	12.1.1.1069
Microsoft Azure Plug-In for Veeam Backup & Replica...	1	Veeam Software Group GmbH	12.6.0.1009
Nutanix AHV Plug-In for Veeam Backup & Replication	1	Veeam Software Group GmbH	12.5.1.8
Red Hat Virtualization Plug-In for Veeam Backup & R...	1	Veeam Software Group GmbH	12.4.0.385
Veeam Agent for Linux Redistributable	1	Veeam Software Group GmbH	6.1.0.1498
Veeam Agent for Mac Redistributable	1	Veeam Software Group GmbH	2.1.0.244
Veeam Agent for Microsoft Windows Redistributable	1	Veeam Software Group GmbH	6.1.0.349
Veeam Agent for Unix Redistributable	1	Veeam Software Group GmbH	4.1.0.1401
Veeam Backup & Replication	1	Veeam Software Group GmbH	12.1.1.56
Veeam Backup Transport	1	Veeam Software Group GmbH	12.1.1.56
Veeam Backup VSS Integration	1	Veeam Software Group GmbH	12.1.0.2131

**With comprehensive asset data:** The detailed asset records provided by Lansweeper can also be used to create document handling procedures for each asset type based on specifics such as location, model, serial numbers, and users. This can be useful for creating use and handling guidelines. The OT Discovery feature even collects details from critical industrial equipment that can help you document use policies.

**Through software policy enforcement:** Lansweeper can detect unauthorized or non-compliant software installations, helping to enforce software use policies.



The screenshot displays the Lansweeper Software Authorization interface. The main content area shows a table of software assets with the following columns: OS Name, Publisher, Computer count, and Approved. The table lists various software products such as Microsoft Visual C++ Redistributable, Google Chrome, and Microsoft Edge. The 'Approved' column contains green and grey circular icons indicating the status of each software installation.

OS Name	Publisher	Computer count	Approved
ms-resource:AppNameName	Microsoft Corporation	50	●
Microsoft Visual C++ 2013 Redistributable (x86)	Microsoft Corporation	16	●
Google Chrome	Google LLC	14	●
Windows Internet Explorer 11	Microsoft Corporation	11	●
Microsoft Edge Update		10	●
Microsoft Visual C++ 2013 Redistributable (x64)	Microsoft Corporation	9	●
Microsoft Visual C++ 2015-2019 Redistributable (x86)	Microsoft Corporation	9	●
Microsoft Update Health Tools	Microsoft Corporation	9	●
Microsoft Edge	Microsoft Corporation	9	●
LSAgent	Lansweeper	9	●
Microsoft Edge WebView2 Runtime	Microsoft Corporation	8	●
Npcap OEM	Nmap Project	8	●
VMware Tools	VMware, Inc.	8	●
Microsoft Visual C++ 2015-2019 Redistributable (x64)	Microsoft Corporation	8	●
Xbox Game bar	Microsoft Corporation	8	●
Phone Link	Microsoft Corporation	7	●
Movies & TV	Microsoft Corporation	7	●
Microsoft Store	Microsoft Corporation	7	●
Microsoft Visual C++ 2015-2022 Redistributable (x64)	Microsoft Corporation	7	●
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	7	●
Wazuh Agent	Wazuh, Inc.	7	●
Game Bar	Microsoft Corporation	6	●
Get Help	Microsoft Corporation	6	●

**Integrate Lansweeper** with your CMDB and ITSM tools like Jira Service Management, ServiceNow, HaloITSM and more to fuel them with rich asset data. These tools facilitate the documentation, implementation, and enforcement of policies by integrating them into daily IT service workflows. They ensure that every interaction with IT assets, from deployment to maintenance and decommissioning, adheres to the organization's acceptable use policies. This makes them invaluable for maintaining compliance and enhancing overall information security governance.

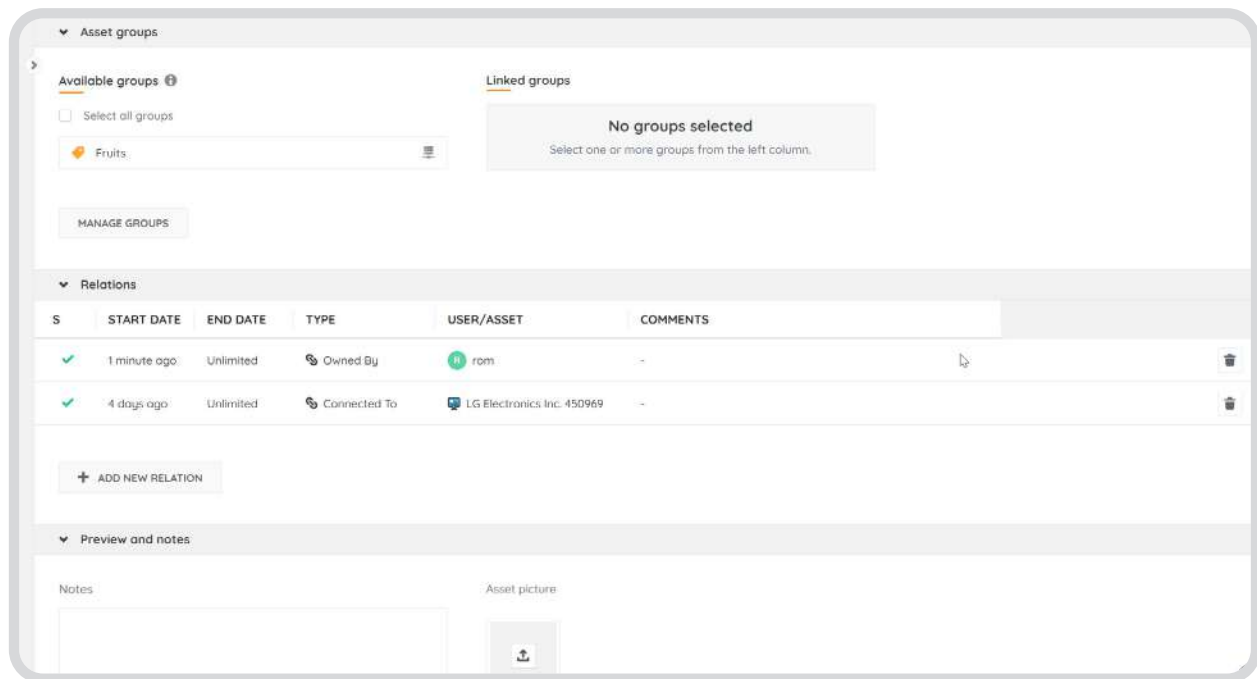
## Relevant Reports:

- **Unauthorized Software Audit**

## 5.11 Return of Assets

**Control 5.11 mandates that employees and other relevant individuals must return any assets belonging to the organization when their employment or agreement ends.** This ensures that all organizational assets are accounted for and secured, preventing unauthorized use or loss of assets after someone's departure or contract termination. Establishing clear procedures for asset return helps maintain control over the organization's resources, supporting information security management.

**Lansweeper lets you link assets to their individual user,** so you always have a record of who has which assets, and, by extension, who has to return what upon leaving the organization. If you are using Lansweeper on-prem, Lansweeper will also maintain a history of asset statuses and user assignments. This can be incredibly useful to ensure that all assets assigned to a person are returned and it provides receipts of where an asset has been in case of asset loss.



**Lansweeper also contains a number of reports** that help you keep track of your assets and who is currently in charge of them. These reports can be used during exit interviews to remind employees of their obligation to return company assets.

If you are using Lansweeper on-prem you can use the built-in "Assets: Asset to user relations" report. Our team has also put together the 2 reports below for you that list disabled AD accounts that still have active equipment associated with them and the last logon on your active Windows machines respectively.

**All reports can also be linked to automated alerts** or you can set an alert for asset return dates tied to the end of employment contracts or other agreements.

**In case of a compliance audit**, these reports can be used to verify that all assets have been returned when an individual has left the company. Alternatively, the detailed asset information gathered by Lansweeper can also simply be used in the documentation of procedures for asset return.

**Lansweeper integrates** with your ITSM and CMDB applications like Jira Service Management, ServiceNow, HaloITSM and more. Thanks to Lansweeper's detailed asset data your tools can accurately track devices and their owners and smoothen on- and offboarding with automation.

### Relevant Reports:

- **Asset to user relations**
- **Active Directory - Disabled AD accounts that still have equipment active**
- **Last Logon for Active Windows Devices**

## 5.12 Classification of Information

**Control 5.12 underlines the importance of categorizing information based on its sensitivity and the need for protection, focusing on confidentiality, integrity, and availability.** This classification guides how information should be handled and protected, ensuring that security measures align with the level of sensitivity and the requirements of relevant stakeholders. By doing so, you can apply appropriate security controls to safeguard information effectively.

**Lansweeper helps with discovering and classifying your information, by identifying and categorizing all your IT assets that store, process, and transmit said information.** Knowing where your information resides is the first step in knowing what information exists to begin the classification process. Once said classification is in place, the same hardware and software inventory can support the implementation of security controls based on the classification levels. For example, more robust encryption may be necessary for assets handling highly confidential information.

Based on your classification, you want to make sure that only authorized personnel have access to your information. **By mapping assets to users and keeping a history of the logins of each user, Lansweeper can aid in enforcing access controls.** Detailed asset reports can be generated to document which assets contain classified information, supporting the overall information security management documentation. On top of that, Lansweeper creates an audit trail that can support compliance efforts by providing evidence that classified information is stored on appropriate assets with the necessary security controls.

## Relevant Reports:

- Windows Server DHCP Role
- Installed software by computer
- Asset to user relations
- Last user logon
- Windows user logons detected during scan (last 7 days)
- SQL Server Databases
- Failed Login Attempts
- Software Overview

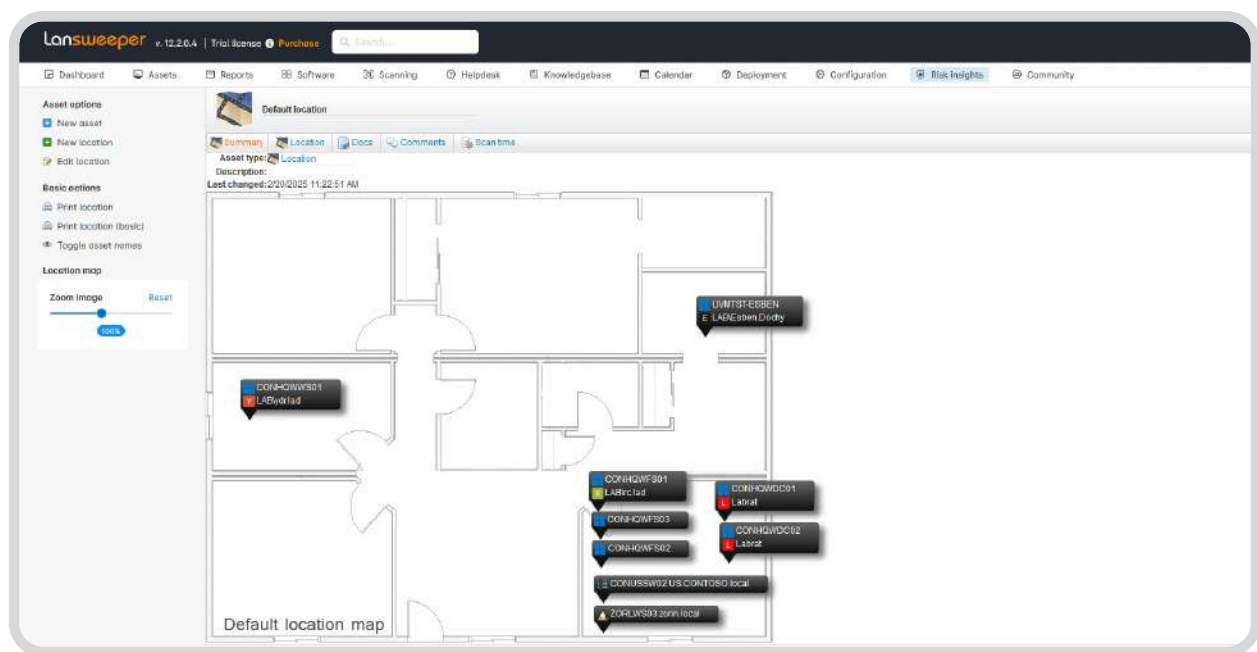
## 5.13 Labelling of Information

**Control 5.13 emphasizes the need for organizations to establish and follow procedures for labeling information according to its classification level.** This involves marking information in a way that clearly indicates its sensitivity and how it should be handled, as well as ensuring that all personnel understand and respect the security requirements associated with different types of information. Proper labeling supports the effective implementation of security controls, helping to maintain the confidentiality, integrity, and availability of information as per the organization's information security standards.

It is important to note here that **Lansweeper is not a data classification or labeling tool. However, you can add some labeling using custom fields. More importantly though, Lansweeper provides necessary asset information and management capabilities to support your organization's data labeling procedures.** It contributes to the overall governance of information security by ensuring that the infrastructure handling sensitive information is known, managed, and controlled. Here are some ways Lansweeper can support you in labeling your organization's sensitive information:

- **Identification of Storage Locations:** Lansweeper can help identify where classified information is stored within the organization by providing a detailed inventory of all IT assets. This knowledge is essential for ensuring that the labeled information is appropriately protected.
- **Asset Documentation:** Lansweeper can document which assets should contain labeled information according to the classification scheme, which is helpful for audits and ensuring compliance with labeling procedures.
- **Verification Support:** While Lansweeper cannot verify the labels on the information itself, it can help verify that the systems supposed to contain labeled information have the proper security controls in place.

- **Custom Fields:** While not a labeling tool, Lansweeper does offer you the possibility to add additional information to your assets through custom fields, which you can label any way you want, and can be reported on.
- **Lifecycle Tracking:** Lansweeper can track the lifecycle of assets that contain labeled information, ensuring that any asset that is decommissioned is handled correctly according to the labeling and classification of the information it contains. Lansweeper Sites also contains multiple lifecycle reports to simplify your lifecycle management.
- **Reporting:** You can build your own reports in Lansweeper based on custom fields you add to your asset data. If you create a custom field to add a classification to your asset data, you can build custom reports to easily track classification. Our own team has also created a report to audit folder share permissions. You can find this report in your Lansweeper Site, or below for on-prem.
- **Enforcement of Policies:** Lansweeper can enforce security policies on assets that should contain labeled information. For example, if a particular asset is documented to contain “confidential” information, Lansweeper can ensure that only software and configurations approved for handling such information are present on that asset.
- **Physical tracking of assets: QR codes** for assets can be generated from Lansweeper for physical asset tracking. This way you can easily access the asset details of any asset, including whether it contains any labeled information, from its physical location. Additionally, you can **create a map of your assets** by uploading a blueprint of your offices and indicating where assets are physically located.



## Relevant Reports:

- Hardware Lifecycle Overview
- OS Lifecycle Overview
- Hardware and OS lifecycle information
- Hardware End of Support
- Hardware End of Support between 12 and 24 months
- Hardware End of Support in the next year
- OS End of Life
- OS End of Life in the next year
- OS End of Life between 12 and 24 months
- OS End of Support
- OS End of Support in the next year
- OS End of Support between 12 and 24 months
- Windows Folder Shares Audit

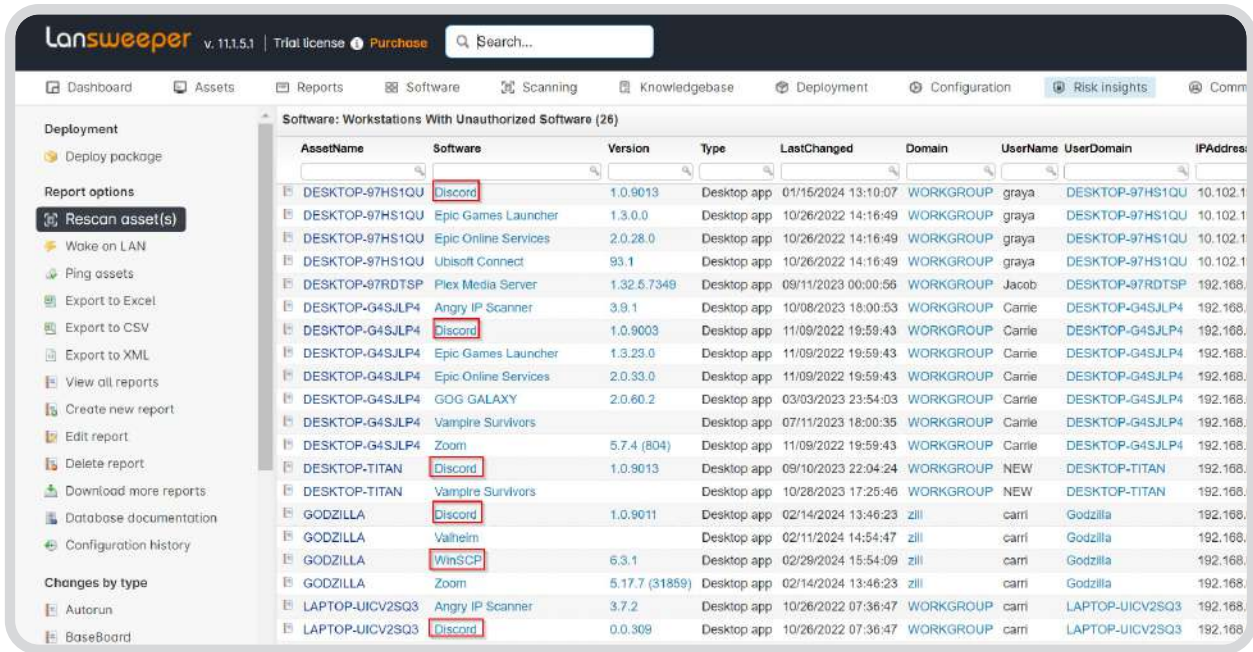
## 5.14 Information Transfer

**Control 5.14 requires the establishment of clear guidelines and procedures for the secure transfer of information within the organization and to external parties.** This ensures that all information transfers, regardless of the method used, are conducted securely and in line with the organization's information security policies. Effective management of information transfer helps protect against unauthorized access and data leaks, maintaining the confidentiality, integrity, and availability of the information during and after the transfer process.

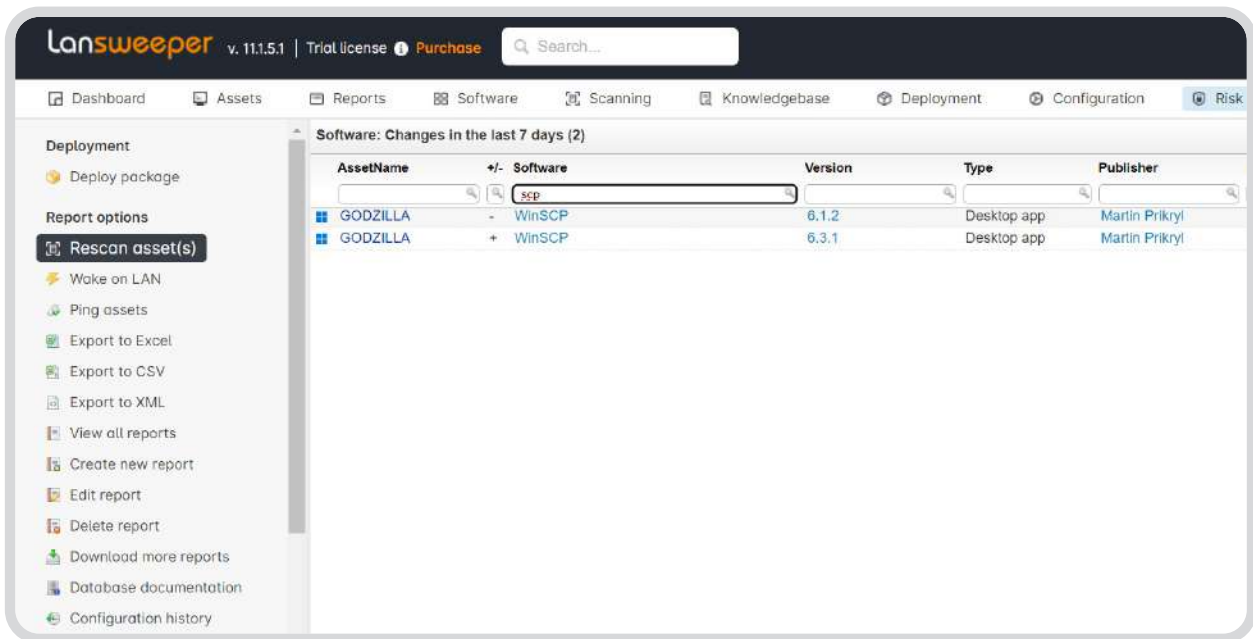
Again, Lansweeper is not a tool for managing the actual data transfer processes, but it provides essential infrastructure visibility, configuration management, and compliance reporting to support the secure transfer of information. These capabilities can help you in ensuring that the rules, procedures, and agreements for information transfer are effectively implemented and maintained. Here is what Lansweeper can do:

- **Identify transfer mechanisms:** Lansweeper can provide a detailed inventory of all the assets that could be involved in information transfer, such as servers, workstations, network devices, and removable media devices. It also maps the network, showing how assets are connected, which can help identify potential transfer pathways.





- **Support agreements and audits:** Detailed reports generated by Lansweeper can support the creation and enforcement of transfer agreements by documenting what transfer facilities are in place and how they are configured.
- **Create an audit trail:** Lansweeper provides an audit trail for asset changes that can be invaluable during information security audits, especially for tracing the history of assets used for data transfer.



- **Support incident investigation support:** In the event of a security incident related to information transfer, Lansweeper can provide crucial data about the devices, software, and configurations involved, supporting the investigation process.

### Relevant Reports:

- Windows Folder Shares Audit
- Unauthorized software
- Software Changes in the last 7 days
- Installed software by computer
- Windows Error events generated in last 7 days
- Common FTP Software Installed

## 5.15 Access Control

**Control 5.15 emphasizes the importance of creating and applying rules for both physical and digital access to information and related assets, guided by business needs and security requirements.** This control ensures that access is granted appropriately, safeguarding sensitive data and systems from unauthorized access, thereby protecting the organization's assets in alignment with its security objectives and operational needs.

**Lansweeper can assist with IAM by providing inventory data on assets that are associated with certain users, as well as a login history for each user.** With this information, you can ensure that users only access those assets they are authorized to, and that when a user leaves the organization, all assets assigned to them are also returned and their access to those assets is revoked. Additionally, Lansweeper can identify unused or underutilized accounts that may be tied to inactive user identities, which can then be reviewed and potentially deactivated.

**Integrate Lansweeper with your ITSM and CMDB tools** like Jira Service Management, ServiceNow, HaloITSM and more and fuel them with always-accurate asset data. Your ITSM allows for the management of access controls through ticketing, approval workflows, and role-based access management. It ensures that access requests are properly managed and that access rules are enforced based on business and security needs. Furthermore, Lansweeper's API and ITSM tools allow integration with IAM tools for even stricter access control.

## Relevant Reports:

- Active Directory Enabled/Disabled Users
- Last Logon for Active Windows Machines
- Last user logon
- Windows user logons detected during scan (last 7 days)

## 5.16 Identity Management

**Control 5.16 focuses on effectively managing the entire lifecycle of user identities within an organization, from creation and maintenance to deactivation or deletion.** This comprehensive approach ensures that access rights and permissions are always aligned with the current roles and responsibilities of individuals, enhancing security and reducing the risk of unauthorized access. Proper identity management is crucial for maintaining the integrity and security of the organization's information systems and resources.

By providing valuable asset information and supporting the infrastructure that IAM processes depend on, Lansweeper indirectly assists with identity lifecycle management in terms of the IT assets they use. There are various ways Lansweeper can support your identity management:

- **User-device association:** Lansweeper can keep track of which devices are assigned to each user, which is helpful when managing the asset component of a user's identity. For example, if a user leaves the organization, Lansweeper can help ensure that all devices assigned to that user are accounted for.
- **Active Directory user information and history:** Lansweeper collects all Active Directory User Objects, and allows the importing of custom attributes, as well as group memberships.

Active Directory user and their groups

USER NAME	USER DOMAIN	FIRST NAME	LAST NAME	NAME	DISPLAY NAME	NAME	DESCRIPTION
\$142000-2R51QGFR8LM	CONTOSO	-	-	Exchange Online-ApplicationAccount	CONTOSO\142000-2R51QGFR8LM	Domain Users	All domain users
AalChe	CONTOSO	Aait	Cheung	Aait Cheung	Cheung, Aait	Domain Users	All domain users
AalRoo	CONTOSO	Aaitje	Roorda	Aaitje Roorda	Roorda, Aaitje	Domain Users	All domain users
AbdGro	CONTOSO	Abdou	Groenink	Abdou Groenink	Groenink, Abdou	Domain Users	All domain users
AbdHun	CONTOSO	Abdelhak	Hunting	Abdelhak Hunting	Hunting, Abdelhak	Domain Users	All domain users
Administrator	CONTOSO	-	-	Administrator	Administrator	Domain Admins	Designated administrator
Administrator	CONTOSO	-	-	Administrator	Administrator	Enterprise Admins	Designated administrator
Administrator	CONTOSO	-	-	Administrator	Administrator	Domain Users	All domain users
Administrator	CONTOSO	-	-	Administrator	Administrator	Schema Admins	Designated administrator
Administrator	CONTOSO	-	-	Administrator	Administrator	Group Policy Creator Owners	Members in this group ca
Administrator	US	-	-	Administrator	US\Administrator	Group Policy Creator Owners	Members in this group ca
Administrator	US	-	-	Administrator	US\Administrator	Domain Users	All domain users
Administrator	US	-	-	Administrator	US\Administrator	Domain Admins	Designated administrator
Administrator	JP	-	-	Administrator	JP\Administrator	Group Policy Creator Owners	Members in this group ca
Administrator	JP	-	-	Administrator	JP\Administrator	Domain Users	All domain users
Administrator	JP	-	-	Administrator	JP\Administrator	Domain Admins	Designated administrator
Administrator	UMBRELLA	-	-	Administrator	UMBRELLA\Administrator	Group Policy Creator Owners	Members in this group ca
Administrator	UMBRELLA	-	-	Administrator	UMBRELLA\Administrator	Domain Admins	Designated administrator
Administrator	UMBRELLA	-	-	Administrator	UMBRELLA\Administrator	Schema Admins	Designated administrator

- **User logon history:** (on-prem only) Lansweeper provides records of what devices and software users have been accessing. This can be useful for auditing purposes and to support compliance with access control policies.

Lansweeper v. 11.1.5.1 | Trial license Purchase Search...

Dashboard Assets Reports Software Scanning Knowledgebase Deployment Configuration Risk insights

Deployment  
Deploy package

Report options  
Rescan asset(s)  
Wake on LAN  
Ping assets  
Export to Excel  
Export to CSV  
Export to XML  
View all reports  
Create new report  
Edit report  
Delete report  
Download more reports  
Database documentation  
Configuration history

Changes by type

Windows: User logons detected during scanning in last 7 days (1-250/283)

AssetName	Domain	IPAddress	IPLocation	Manufacturer	Model	OS
DESKTOP-97HS1QU	WORKGROUP	10.102.191.160	Undefined	Eiuktronics Inc.	MAX-17	Win 11
DC1	zill	10.0.1.10	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
DC1	zill	10.0.1.10	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
UTIL04	zill	10.0.1.32	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
DESKTOP-97HS1QU	WORKGROUP	10.102.191.160	Undefined	Eiuktronics Inc.	MAX-17	Win 11
MSI	WORKGROUP	192.168.0.217	Internal LAN - Orbi	Micro-Star International Co., Ltd.	Raider GE78HX 13VH	Win 11
DESKTOP-97RDTSP	WORKGROUP	192.168.0.177	Internal LAN - Orbi	Dell Inc.	Latitude E7450	Win 10
UTIL02	zill	10.0.1.28	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
GODZILLA	zill	192.168.0.20	Internal LAN - Orbi	Gigabyte Technology Co., Ltd.	B550M DS3H AC	Win 11
GODZILLA	zill	192.168.0.20	Internal LAN - Orbi	Gigabyte Technology Co., Ltd.	B550M DS3H AC	Win 11
DC1	zill	10.0.1.10	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
DC1	zill	10.0.1.10	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
UTIL04	zill	10.0.1.32	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
SQL01	zill	10.0.1.26	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
UTIL05	zill	10.0.1.34	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
UTIL01	zill	10.0.1.25	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
SQL01	zill	10.0.1.26	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
UTIL05	zill	10.0.1.34	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
UTIL02	zill	10.0.1.28	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
UTIL01	zill	10.0.1.25	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019
SQL01	zill	10.0.1.26	Lab Internal Subnet - Ubiquiti	VMware, Inc.	VMware7,1	Win 2019

- **Reporting for audits:** Lansweeper can generate reports that detail the configuration and status of assets, which can be used to support audits of identity management processes, particularly in verifying that assets are properly provisioned or deprovisioned along with user identities.
- **Network asset discovery:** Lansweeper can identify all devices connected to the network, which supports network access control (NAC) solutions by ensuring that only devices associated with current and valid user identities are allowed network access.
- **Orphaned account detection:** While directly managing accounts is beyond Lansweeper's capabilities, it can help identify assets that may be related to orphaned accounts (accounts that remain active after the user has left the organization) by showing the last known user of an asset.
- **Custom integrations:** Lansweeper integrates with leading ITSM and CMDB tools like Jira Service Management, ServiceNow, HaloITSM and more. With Lansweeper granular asset data as a solid foundation for Identity-focussed workflows these tools can manage the creation, modification, and termination of user identities through workflows and approval processes.

### Relevant Reports:

- All Active Directory Users
- Active Directory user and their groups
- Last User Logon
- Windows Computer Logon History
- Active Directory Enabled/Disabled Users

## 5.17 Authentication information

**Control 5.17 emphasizes the need for a structured management process to oversee the allocation and handling of authentication information, such as passwords.** Employees should be guided and trained in secure practices for managing their authentication information to prevent unauthorized access. By ensuring that this sensitive information is handled correctly, you can significantly enhance the security of your organization's data and systems.

While Lansweeper itself does not handle authentication information, it's rich asset data can be used to **fuel your ITSM and CMDB tools like Jira Service Management, ServiceNow, HaloITSM and more through seamless integrations.** Lansweeper's technology asset data can serve as a foundation for these tools to manage user access, including authentication credentials. They support password resets, multi-factor authentication processes, and the overall management of how authentication information is distributed and used through ticketing and automations.

## 5.18 Access Rights

**Control 5.18 stresses the importance of managing access rights systematically, ensuring they're granted, reviewed, changed, or revoked in line with specific organizational policies and rules on access control.** This process is key to maintaining secure and appropriate access to information and assets, helping to prevent unauthorized access and ensuring that individuals have the access they need to fulfill their roles effectively.

Lansweeper provides detailed asset and user data, aiding in the management of access rights. **Through its comprehensive scanning and reporting capabilities, Lansweeper can identify which users have access to what assets,** supporting the process of provisioning, reviewing, modifying, and removing access rights in compliance with the organization's access control policies and rules.

Lansweeper identifies which users have access to specific assets and allows you to generate reports on access rights. This way you can easily review and adjust access rights and permissions to align with organizational policies. Track and document changes in access rights to ensure they are being updated and revoked as needed and you always have the documentation on hand in case of audits.

Furthermore, **Lansweeper integrates seamlessly with leading ITSM and CMDB solutions** like Jira Service Management, ServiceNow, HaloITSM and more. With Lansweeper's always-accurate asset data as their foundation, these tools can more effectively manage user access, including reviewing, modifying, and reviewing access through ticketing and automations.

### Relevant Reports:

- **Asset to User Relations**

## 5.23 Information Security for Use of Cloud Services

**Control 5.23 requires setting up clear processes for handling all phases of cloud service utilization**—acquisition, usage, management, and termination—ensuring these processes align with the organization's security standards. This comprehensive approach helps safeguard sensitive data throughout the cloud service lifecycle, from selection and deployment to discontinuation, maintaining information security, and compliance with organizational policies.

**Lansweeper's cloud discovery** feature automatically collects the cloud data you need, cataloging all assets within your cloud infrastructure, including virtual machines, storage buckets, databases,

and more. You can use Lansweeper on **AWS, Amazon Web Services, Google Cloud Platform (GCP)**, Virtual Private Clouds, and your own individual servers. Lansweeper retrieves all available fields exposed by the manufacturer's API. You can scan every device and group of devices hosted on hybrid or cloud-based server environments as well as manage multiple cloud environments at once.

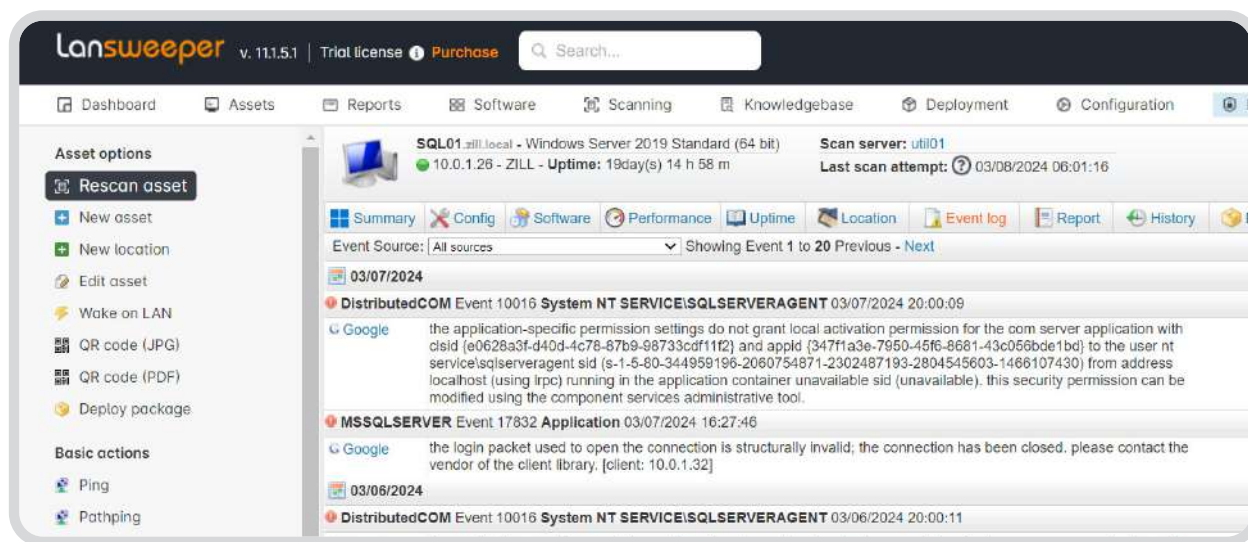
On top of that, Lansweeper is also able to **scan any cloud-hosted resource running a Windows, Linux or Mac OS** using its traditional scanning capabilities to get the same level of device-specific details as physical machines including hardware, software, and user information.

**All data will be collected and stored in one single system**, accessible through a handy interface with asset pages that are easy to navigate. This cloud asset inventory forms the foundation of your security, compliance, and resource optimization strategies. Achieving full visibility of your IT estate, including cloud assets, is crucial for promptly identifying and addressing security risks.

## 5.25 Assessment and Decision on Information Security Events

**Control 5.25 emphasizes the need to evaluate information security events to determine if they should be classified as security incidents.** It involves a systematic process for assessing events based on their impact and relevance to security policies, ensuring that significant events are identified and managed as incidents, allowing for timely and appropriate responses to potential threats.

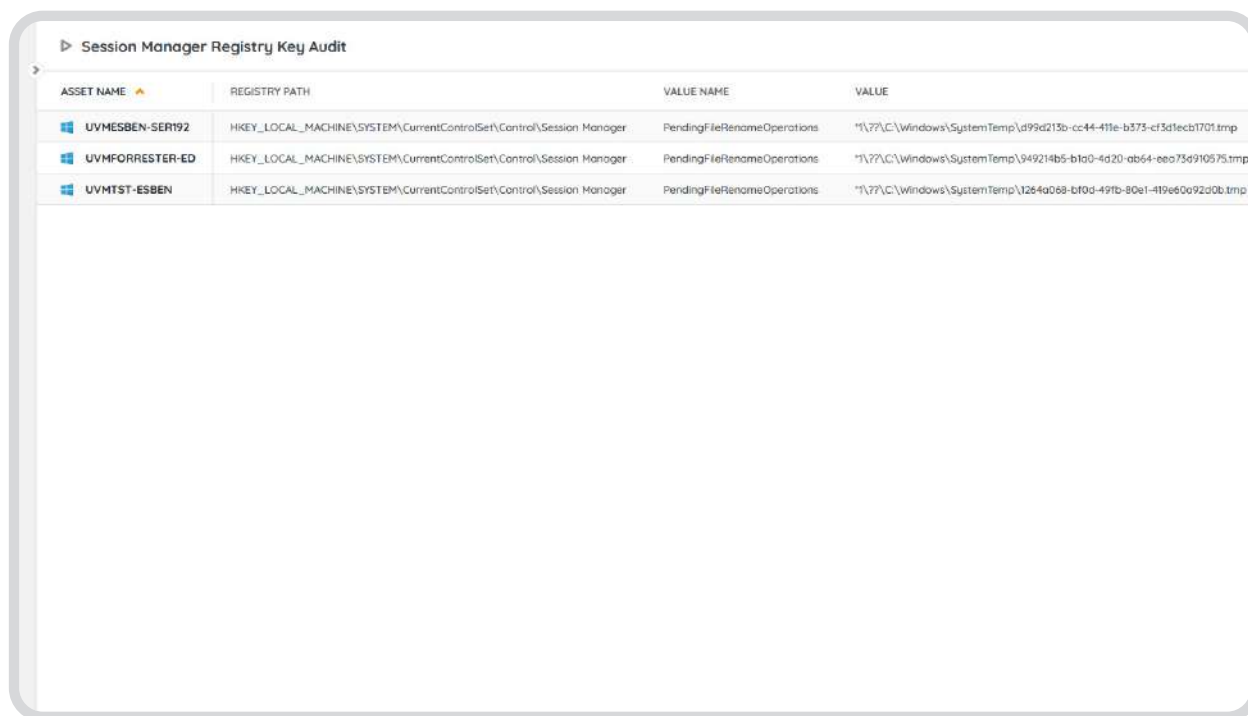
**Lansweeper's event log monitoring** helps with swiftly identifying and assessing security events by providing insight into event logs across the IT infrastructure. This facilitates early detection of potential incidents, so you can quickly respond to and mitigate risks, protecting operational integrity and data security.



**Create event log alerts** to notify you as soon as a critical event is scanned. By combining Windows event log scanning targets and email alerts, you will be notified within minutes when vital assets are having difficulties. And of course, email notifications also work for non-critical event logs. Simply modify the criteria for your alerts in the Reports & Alerts section of your Lansweeper web console.

**Track your asset change history** to enhance security by meticulously recording changes in hardware, software, configurations, and user permissions. This allows you to detect unauthorized changes, ensuring that all modifications align with security policies. By maintaining a comprehensive audit trail, Lansweeper aids in accountability and forensic analysis, crucial for mitigating risks and ensuring compliance with regulatory requirements.

**Lansweeper's file and registry scanning** capabilities offer deep insight into system configurations and file integrity, helping you maintain security standards. By scanning and tracking file and registry changes, Lansweeper facilitates the detection of unauthorized modifications, contributing to data security and compliance. This function is key for identifying potential vulnerabilities or breaches, allowing for prompt remediation actions to safeguard information assets.



ASSET NAME	REGISTRY PATH	VALUE NAME	VALUE
UVMESBEN-SER192	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager	PendingFileRenameOperations	"\??\C:\Windows\SystemTemp\cf99d213b-cc44-411e-b373-cf5d1ecb1701.tmp
UVMFORRESTER-ED	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager	PendingFileRenameOperations	"\??\C:\Windows\SystemTemp\949214b5-b1a0-4d20-ab64-be075d910575.tmp
UVMTST-ESBEN	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager	PendingFileRenameOperations	"\??\C:\Windows\SystemTemp\1264a068-bf0d-49fb-80e1-419e60a92d0b.tmp

**Seamlessly integrate Lansweeper** with leading SIEM and SOAR tools, including Splunk ES, Palo Alto Cortex XSOAR, IBM QRadar, MSFT Sentinel, Splunk SOAR, providing complete and accurate technology asset data automatically, to enrich alerts and enable swift incident remediation. Linking Lansweeper's data to security events greatly simplifies and speeds up the process of identifying and remediating the issue. IT teams can also use this information to proactively protect the infrastructure by identifying assets in need of upgrades and automatically rolling out critical software updates.

## Relevant Reports:

- Scanned Registry Keys
- Windows: Error events generated in last 7 days
- Event Log Cleared Audit
- Failed Logon Event Audit
- Windows Firewall Service Stopped Event Audit

## 5.26 Response to information security incidents

**Control 5.26 requires you to define, document, and follow procedures when responding to information security incidents.** This ensures a consistent, effective approach to managing and mitigating the effects of security breaches, minimizing damage and restoring normal operations promptly.

**Lansweeper integrates seamlessly with your ITSM and CMDB applications** like Jira Service Management, ServiceNow, HalolTSM and more is that you always have accurate and up-to-date asset information on hand to enhance your incident response. Reliable asset data allows for more informed decision-making and a quicker, more organized response to security incidents using ticketing or automation. This ensures that responses are thorough and consistent with the organization's predefined incident management procedures.

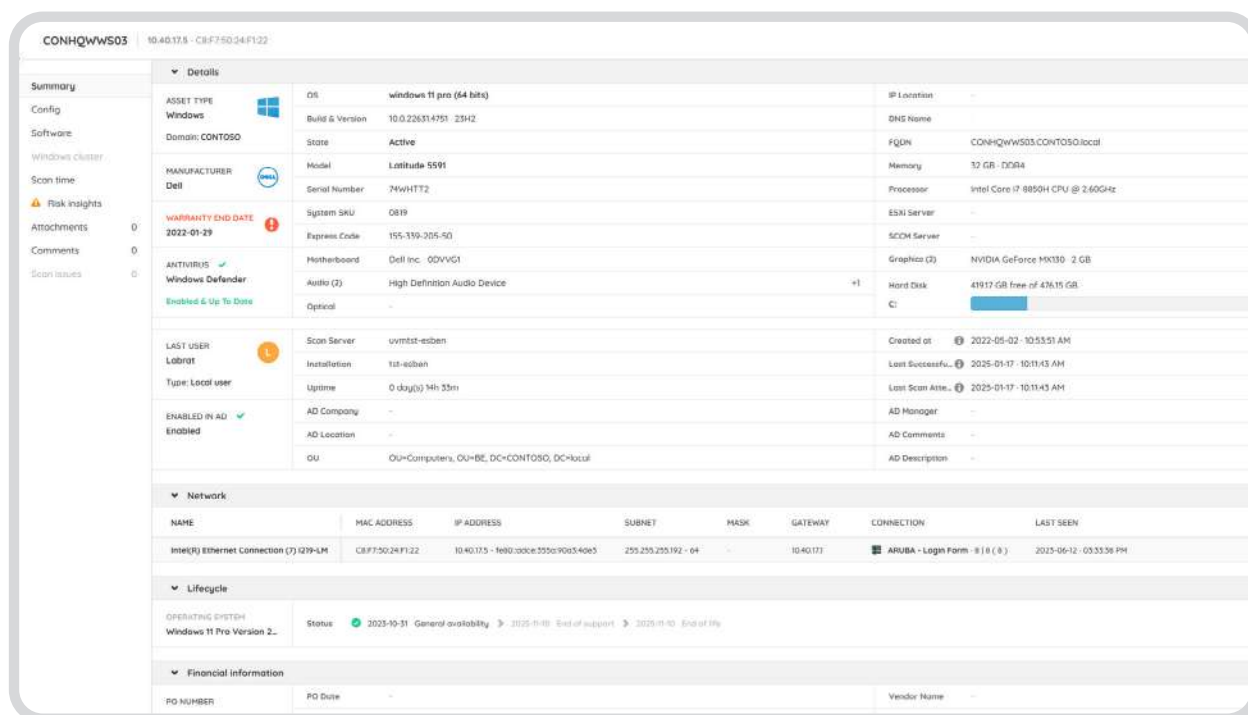
## 5.28 Collection of Evidence

**Control 5.28 mandates the creation of procedures for efficiently handling evidence related to security events.** This includes identifying, collecting, securing, and preserving evidence to support investigations and ensure accountability. Establishing these protocols is crucial for analyzing incidents thoroughly, facilitating legal processes, and enhancing future security measures.

Lansweeper's detailed and comprehensive asset discovery and inventory help with the identification, collection, acquisition, and preservation of evidence in the event of a security incident:

- **Evidence identification:** Lansweeper's detailed asset inventory helps in pinpointing devices involved in security events, aiding in the identification of potential evidence. The quick identification of assets linked to security events ensures that all relevant evidence is accounted for.
- **Evidence collection:** Lansweeper's event log collection features allow for the aggregation of system and application logs, which can serve as evidence. Detailed event logs capture digital activities related to security incidents, providing a wealth of information for analysis.

- **Evidence acquisition:** Detailed scanning and reporting capabilities can be used to acquire configurations and system states, further contributing to evidence gathering. Lansweeper's ability to scan and report on current and historical configurations of assets allows organizations to acquire critical evidence on how and when a security event impacted their systems.
- **Evidence preservation:** Lansweeper stores asset and event log information securely, aiding in the preservation of digital evidence. This also preserves the integrity of digital evidence, ensuring it remains untampered for analysis and potential legal proceedings.



Furthermore, Lansweeper seamlessly integrates a wide range of supporting tools such as Splunk, Axonius, Jira Service Management, ServiceNow, FortifyData, ManageEngine ServiceDesk Plus, Oomnitza, and more that can each provide strong indirect support for Control 5.28. More specifically, they help with the collection of evidence by ensuring that evidence related to security events is properly identified, collected, and preserved for investigation purposes.

## Annex A6: People Controls

Section 6 of Annex A deals with people controls and consists of 8 controls. These controls focus on regulating the human component of your information security strategy. It gives guidance on how to structure the way personnel interact with your data and each other. The main focus of the 8 controls lies on:

- Secure human resource management
- Personnel security and confidentiality
- Information security awareness and training
- Remote working

As these controls are people-focussed and Lansweeper is at its core an IT Asset Management solution, there are, unfortunately, no controls where Lansweeper can be of assistance in this section.

## Annex A7: Physical Controls

Section 7 of Annex A deals with physical controls and consists of 14 controls. These controls focus on the measures taken to ensure the security of your physical assets and infrastructure. These safeguards protect the physical bearers of your confidential information. These controls emphasize:

- Entry systems and access protocols
- Security perimeters and secure areas
- Equipment maintenance and asset disposal processes
- Supporting utilities
- Clear desk and clear screen policies

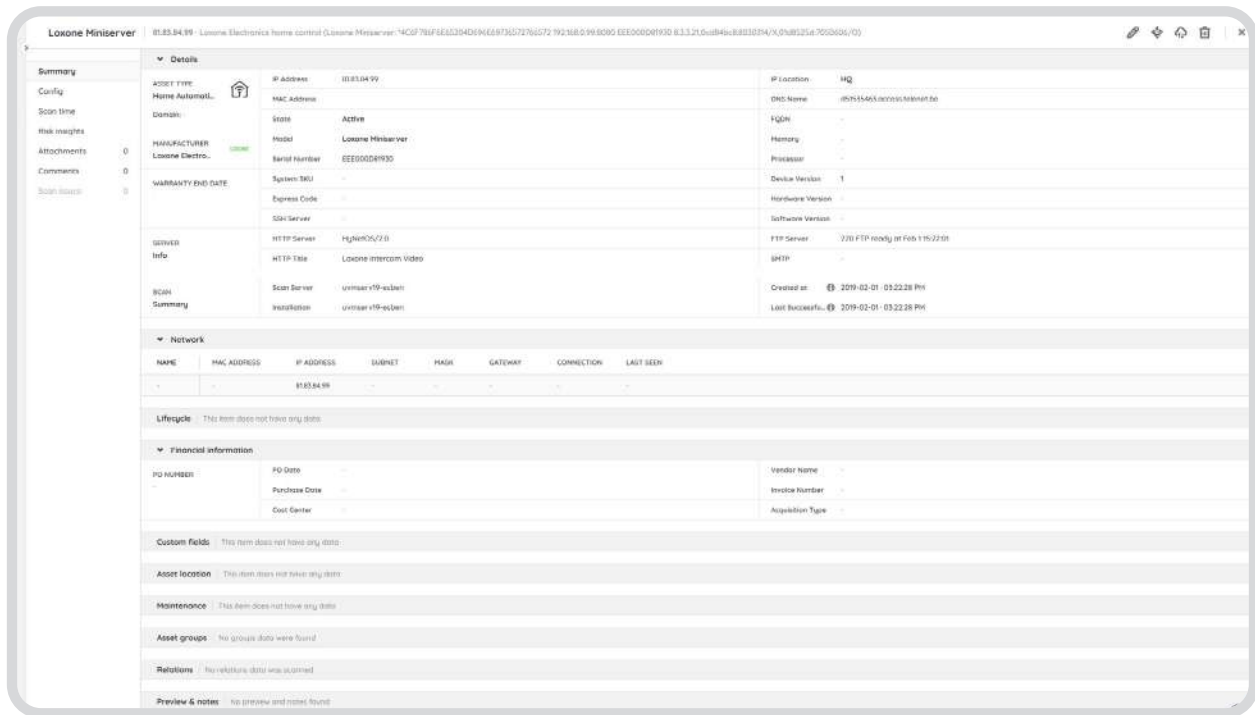
As these controls are focused on physical security and Lansweeper is at its core an IT Asset Management solution, Lansweeper can't be of much assistance in this section. However, there are 5 controls it can help with.

### 7.4 Physical security monitoring

**Control 7.4 calls for the premises to be monitored continuously for unauthorized physical access.** This can be achieved with proper surveillance tools that can detect and prevent intruders from entering restricted areas like video monitoring systems, detectors, alarms, or even just good locks.

**Many of these systems, even some locks, would fall into the category of IoT, which means Lansweeper can scan them.** After all, if it is connected to the corporate network, Lansweeper can find it. This makes it easy to track and manage your security systems and ensure they are functioning

properly so that they can continue to monitor and protect your premises to the best of their ability.



## 7.7 Clear desk and clear screen

**Control 7.7 requires organizations to define and enforce rules regarding clear desk and clear screen.** This ensures that no sensitive information is left lying around on papers or removable storage media that can be swiped up, or left exposed on open screens where it is left vulnerable to unauthorized access.

**A staple in the enforcement of a clear screen policy is setting an idle time that automatically locks the screen and then requires a password to regain access.** This reduces the risk of sensitive data being exposed on an unlocked screen when the user steps away and no unauthorized individuals can access information while the workstation is left unattended. This can be enforced through group policy, registry setting, or corporate policies.

Automatic Screen Lock Audit

ASSET NAME	ASSET DOMAIN	USER NAME	USER DOMAIN	IP ADDRESS	MANUFACTURER	MODEL	WINDOWS NAME
UVMTST-ESBEN	dmz	Esben.Dochy	LAB	10.37.0.201	VMware	VMware7,1	Win 10

### Relevant Reports:

- [Automatic Screen Lock](#)

## 7.8 Equipment siting and protection

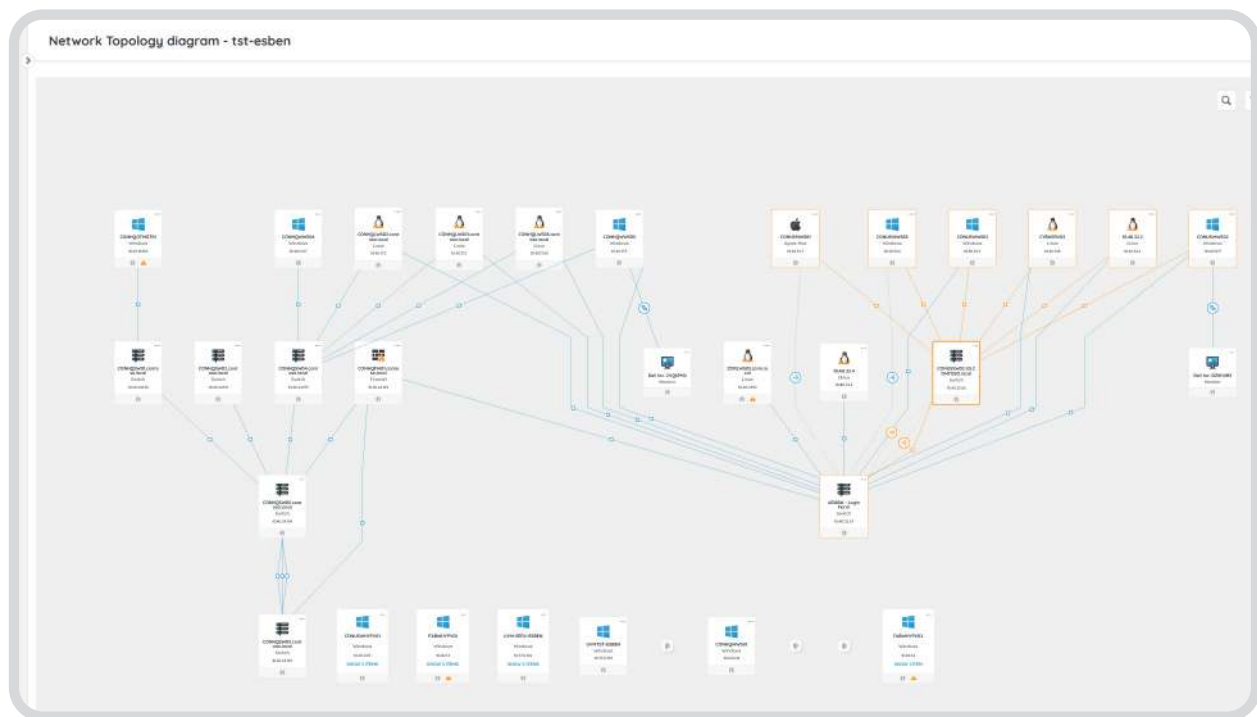
**Control 7.8 calls for the secure siting and protection of all equipment hosting information assets.** This includes placing them in secure area and implementing appropriate measures to protect them against physical and environmental hazards such as power outages, theft, interference with communications, and electrical interference, as well as humidity and temperature changes.

**Lansweeper lets you discover, track, and physically locate your equipment.** Through its network discovery, Lansweeper ensures that IT teams have full visibility over their infrastructure, helping to ensure that devices are properly sited and protected from unauthorized access or environmental risks.

1. **Lansweeper performs comprehensive network scans to discover devices** across the organization, including hardware like switches, routers, and other network infrastructure. This ensures

that all equipment is accounted for and more easily physically located, even across multiple sites.

- Lansweeper's ability to port scan switches and routers** enhances visibility into network devices. By identifying devices in a remote location, Lansweeper helps IT teams physically locate and verify the positioning of their network infrastructure, ensuring that these devices are placed and managed securely.
- Lansweeper keeps a detailed inventory of all discovered devices**, so that you have eyes on every single piece of equipment, whether local or remote, and they tracked and managed securely. This allows IT teams to maintain oversight over the physical placement and security of key infrastructure components.
- By providing continuous, real-time visibility into the organization's hardware**, Lansweeper allows IT teams to ensure that equipment is sited according to security policies. If a device is moved or improperly located, Lansweeper's network discovery features can quickly identify it, supporting compliance with physical security controls.



## 7.9 Security of assets off-premises

**Control 7.9 urges organisations to protect assets even when they are not located on the main site or sites.** This reduces the chance that these assets would be lost, damaged, destroyed, or exposed to unauthorized access. With the rise of remote work and home offices, this control has gained significant importance.

**Lansweeper's IT Agent (or if you are using Lansweeper Classic on-premise, LsAgent) lets you track, monitor, and enforce security for assets that are used outside of corporate locations.**

This way IT teams can maintain continuous oversight over off-site devices, ensuring they are protected according to the organization's security standards, even when they are not physically on the premises. Lansweeper helps by:

- 1. Tracking Off-Site Assets:** The IT Agent allows Lansweeper to track assets, even when they are not connected to the corporate network. This includes laptops, mobile devices, and other equipment that employees use while working remotely. This way IT teams can keep an eye on devices that are off-premises, making sure they remain compliant with security policies.
- 2. Real-Time Asset Inventory:** With the IT Agent installed on devices, Lansweeper can maintain a real-time inventory of all off-site assets. This ensures that IT teams have visibility over these devices, including software, hardware configurations, and potential vulnerabilities, which helps enforce security controls and protect off-premises assets from unauthorized access or misuse.
- 3. Monitoring Security Configurations:** IT Agent can collect detailed information about the security configurations of off-site assets, such as installed software, antivirus status, firewall settings, and operating system patches. It allows you to ensure that off-premises assets maintain the same level of security as on-premises devices, reducing the risk of security breaches.
- 4. Offline Data Collection:** Even when off-premises assets are temporarily disconnected from the corporate network, the IT Agent can continue collecting data about the device. Once the asset reconnects this information is uploaded to Lansweeper, ensuring that there are no gaps in monitoring or security oversight.
- 5. Incident Response for Off-Site Assets:** If an off-premises asset is compromised or missing, Lansweeper's inventory and the IT Agent's data provide crucial details, such as the device's last known location, installed software, and current security status. This helps IT teams take action to protect the asset or remotely manage it if necessary.

## 7.14 Secure disposal or re-use of equipment

**Control 7.14 stresses the importance of secure disposal or re-use of any equipment to ensure that any sensitive data and licensed software has been removed or securely overwritten.** This ensures that no sensitive data can be accessed by unauthorized parties when old assets are handed over or disposed of.

**Lansweeper lets you track assets throughout their lifecycle, detecting unauthorized reactivation, and verifying that data is removed before disposal:**

- 1. Asset Lifecycle Tracking:** Lansweeper allows organizations to track the entire lifecycle of an asset, including custom statuses such as 'decommissioned', 'recycled', or 'pending disposal'. By monitoring and updating asset statuses, IT teams can ensure that devices flagged for disposal or re-use are properly tracked, helping maintain oversight of assets during the disposal process.
- 2. Monitoring for Unauthorized Reactivation:** Lansweeper's real-time network scanning capabilities can detect if decommissioned or disposed devices come back online. This acts as a security control, ensuring that equipment intended for disposal or re-use is not unintentionally reactivated and reintroduced into the environment without following the appropriate procedures.
- 3. Asset Verification for Disposal:** Lansweeper can be used to generate reports of assets that are due for disposal, including details on their software, hardware, and storage media. This ensures that IT teams can verify the removal of licensed software and the secure wiping or removal of sensitive data from storage media prior to disposal or re-use.

**Lansweeper further helps with the disposal or re-use process by integrating with leading ITSM tools** like Jira Service Management, ServiceNow, HaloITSM and more. This allows you to leverage Lansweeper's rich asset data to more effectively manage and automate the entire disposal lifecycle, from requesting decommission to verifying data removal, software wiping procedures, or device re-assignment.

## Annex A8: Technological Controls

Section 8 is the largest section of Annex A, consisting of 34 controls and focuses on technological controls. This means the digital regulations and processes that you should adopt in order to keep your IT infrastructure secure and compliant. This includes:

- Authentication protocols
- Information logging and monitoring
- Backup and disaster recovery processes
- Network security and segregation
- Protection against malware
- Development and coding practices

Of the 34 controls in section 8, Lansweeper can directly or indirectly assist with 22.

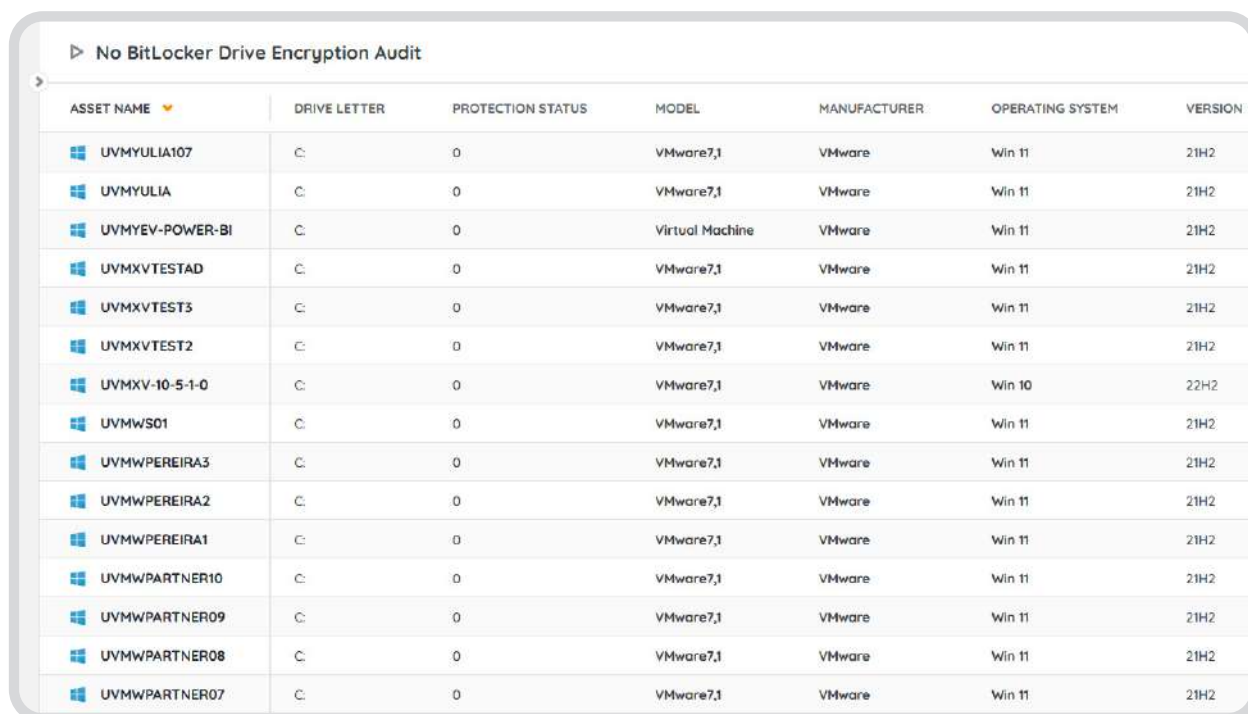
### 8.1 User End Point Devices

**Control 8.1 emphasizes safeguarding information accessible via endpoint devices.** The data should be protected whether it is stored, processed, or accessed through these devices. This protects sensitive information against unauthorized access, loss, or compromise, underscoring the need for

robust security measures like encryption, access controls, and malware protection on all user endpoints.

There are a whole range of Lansweeper features and reports that can help you protect data on endpoint devices:

**Lansweeper’s BitLocker Encryption** offers insight into the encryption status of endpoint devices, ensuring that any information stored on or accessible through these devices is protected. This allows you to verify compliance with company encryption policies and enhance data security across user devices. By systematically reporting on BitLocker status, Lansweeper lets you identify unencrypted devices, so you can take the necessary actions to safeguard sensitive information.



ASSET NAME	DRIVE LETTER	PROTECTION STATUS	MODEL	MANUFACTURER	OPERATING SYSTEM	VERSION
UVMYULIA107	C:	0	VMware7,1	VMware	Win 11	21H2
UVMYULIA	C:	0	VMware7,1	VMware	Win 11	21H2
UVMYEV-POWER-BI	C:	0	Virtual Machine	VMware	Win 11	21H2
UVMXVTESTAD	C:	0	VMware7,1	VMware	Win 11	21H2
UVMXVTEST3	C:	0	VMware7,1	VMware	Win 11	21H2
UVMXVTEST2	C:	0	VMware7,1	VMware	Win 11	21H2
UVMXV-10-5-1-0	C:	0	VMware7,1	VMware	Win 10	22H2
UVMWS01	C:	0	VMware7,1	VMware	Win 11	21H2
UVMWPEREIRA3	C:	0	VMware7,1	VMware	Win 11	21H2
UVMWPEREIRA2	C:	0	VMware7,1	VMware	Win 11	21H2
UVMWPEREIRA1	C:	0	VMware7,1	VMware	Win 11	21H2
UVMWPARTNER10	C:	0	VMware7,1	VMware	Win 11	21H2
UVMWPARTNER09	C:	0	VMware7,1	VMware	Win 11	21H2
UVMWPARTNER08	C:	0	VMware7,1	VMware	Win 11	21H2
UVMWPARTNER07	C:	0	VMware7,1	VMware	Win 11	21H2

**Lansweeper recognizes attached USB drives** so that you can more easily identify unauthorized device usage that could be threatening the integrity of your data. That way you can take timely measures to prevent potential security breaches, maintaining the integrity and confidentiality of information stored on or accessible via user endpoint devices.

**The “Trusted Platform Module” report** lets you assess and ensure that user end-point devices are equipped with TPM chips, enhancing data protection and device integrity. By reporting on TPM presence and status, you can identify devices that meet security standards, facilitating compliance and safeguarding sensitive information processed or accessible via these devices.

**The “Endpoint Antivirus” report** ensures that your devices are properly safeguarded with up-to-date antivirus software, critical for defending against malware and cyber threats. By identifying

unprotected endpoints, you can enhance security measures, aligning with policies for information protection on user devices.

▶ Workstations with antivirus installed

ASSET NAME	ANTIVIRUS	PRODUCT UP TO DATE	ON ACCESS SCANNING ENABLED	OPERATING SYSTEM
DC1	Windows Defender	No	Yes	Microsoft Windows Server 2019 D
DESKTOP-97HS1QU	Windows Defender	Yes	Yes	Microsoft Windows 11 Home
DESKTOP-97RDTSP	Windows Defender	Yes	Yes	Microsoft Windows 10 Pro
DESKTOP-G4SJLP4	Windows Defender	Yes	Yes	Microsoft Windows 10 Home
DESKTOP-TITAN	Windows Defender	Yes	Yes	Microsoft Windows 11 Pro
GODZILLA	Windows Defender	Yes	Yes	Microsoft Windows 11 Pro
HORIZONCONN01	Windows Defender	No	Yes	Microsoft Windows Server 2019 S
LAPTOP-UICV2SQ3	Windows Defender	Yes	Yes	Microsoft Windows 11 Pro
MSI	Windows Defender	Yes	Yes	Microsoft Windows 11 Home
UTIL01	Windows Defender	No	Yes	Microsoft Windows Server 2019 S
UTIL02	Windows Defender	No	Yes	Microsoft Windows Server 2019 S
UTIL05	Windows Defender	No	Yes	Microsoft Windows Server 2019 S

**Lansweeper tracks your installed SSL certificates.** These SSL Certificates enable encrypted connections, safeguarding data from interception or tampering. Regularly tracking and managing these certificates prevents security lapses, such as expired certificates leading to vulnerabilities, ensuring continuous protection of sensitive data accessed or processed by endpoint devices.

Self-signed certificates, while useful in certain scenarios, can pose a security risk if not properly managed, as they might not offer the same level of trust and validation as those issued by recognized Certificate Authorities. Tracking and managing these certificates help ensure that only trusted and validated encryption is used, reducing the risk of man-in-the-middle attacks and maintaining the integrity and confidentiality of data.

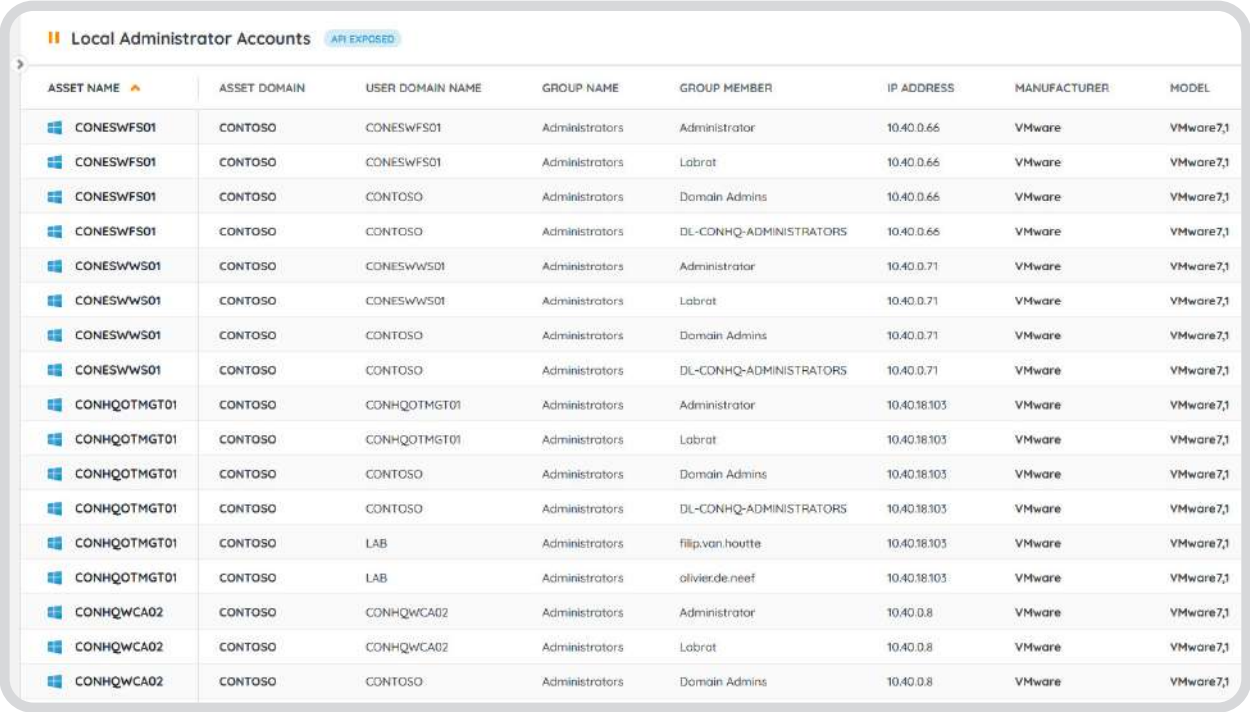
### Relevant Reports:

- [Bitlocker Drive Encryption Audit](#)
- [USB Connected Devices](#)
- [Windows Certificate Overview](#)
- [Windows Certificates With Expired Key](#)

## 8.2 Privileged Access Rights

**Control 8.2 focuses on tightly controlling and overseeing privileged access rights within an organization.** Privileged access, given its elevated permissions, is restricted to essential personnel and is subject to strict management to prevent misuse or unauthorized access. This control ensures that high-level access is only granted when necessary, with measures in place to monitor and review its use, safeguarding critical systems and information from potential security risks.

**Lansweeper provides detailed asset and software inventory reports, identifying systems with privileged access rights.** While it doesn't directly manage user rights, its comprehensive visibility into network assets allows IT administrators to pinpoint where privileged accounts are used. This facilitates the review and audit process of privileged access, ensuring only authorized users have elevated rights in line with organizational policies, thereby helping to restrict and manage the allocation and use of such privileges effectively.



The screenshot displays a table titled "Local Administrator Accounts" with a sub-label "API EXPOSED". The table lists various assets and their associated administrator accounts. The columns are: ASSET NAME, ASSET DOMAIN, USER DOMAIN NAME, GROUP NAME, GROUP MEMBER, IP ADDRESS, MANUFACTURER, and MODEL. The data rows show assets like CONESWFS01, CONESWWS01, CONHQOTMGT01, and CONHQWCA02, each with multiple entries for different users and groups.

ASSET NAME	ASSET DOMAIN	USER DOMAIN NAME	GROUP NAME	GROUP MEMBER	IP ADDRESS	MANUFACTURER	MODEL
CONESWFS01	CONTOSO	CONESWFS01	Administrators	Administrator	10.40.0.66	VMware	VMware7,1
CONESWFS01	CONTOSO	CONESWFS01	Administrators	Labrat	10.40.0.66	VMware	VMware7,1
CONESWFS01	CONTOSO	CONTOSO	Administrators	Domain Admins	10.40.0.66	VMware	VMware7,1
CONESWFS01	CONTOSO	CONTOSO	Administrators	DL-CONHQ-ADMINISTRATORS	10.40.0.66	VMware	VMware7,1
CONESWWS01	CONTOSO	CONESWWS01	Administrators	Administrator	10.40.0.71	VMware	VMware7,1
CONESWWS01	CONTOSO	CONESWWS01	Administrators	Labrat	10.40.0.71	VMware	VMware7,1
CONESWWS01	CONTOSO	CONTOSO	Administrators	Domain Admins	10.40.0.71	VMware	VMware7,1
CONESWWS01	CONTOSO	CONTOSO	Administrators	DL-CONHQ-ADMINISTRATORS	10.40.0.71	VMware	VMware7,1
CONHQOTMGT01	CONTOSO	CONHQOTMGT01	Administrators	Administrator	10.40.18.103	VMware	VMware7,1
CONHQOTMGT01	CONTOSO	CONHQOTMGT01	Administrators	Labrat	10.40.18.103	VMware	VMware7,1
CONHQOTMGT01	CONTOSO	CONTOSO	Administrators	Domain Admins	10.40.18.103	VMware	VMware7,1
CONHQOTMGT01	CONTOSO	CONTOSO	Administrators	DL-CONHQ-ADMINISTRATORS	10.40.18.103	VMware	VMware7,1
CONHQOTMGT01	CONTOSO	LAB	Administrators	Filip.van.houtte	10.40.18.103	VMware	VMware7,1
CONHQOTMGT01	CONTOSO	LAB	Administrators	olivier.de.neef	10.40.18.103	VMware	VMware7,1
CONHQWCA02	CONTOSO	CONHQWCA02	Administrators	Administrator	10.40.0.8	VMware	VMware7,1
CONHQWCA02	CONTOSO	CONHQWCA02	Administrators	Labrat	10.40.0.8	VMware	VMware7,1
CONHQWCA02	CONTOSO	CONTOSO	Administrators	Domain Admins	10.40.0.8	VMware	VMware7,1

On top of that, **Lansweeper integrates seamlessly with cybersecurity solutions** like Axonius, Armitis and more. Lansweeper's detailed asset insights allow those tools to more effectively manage, monitor, and control privileged access rights. This ensures that the allocation and use of privileged access are restricted and managed according to the organization's security policies.

### Relevant Reports:

- **Unauthorized Administrators**
- **Local Admin Accounts**
- **Active Directory Users In Specific Group**

## 8.3 Information Access Restriction

**Control 8.3 mandates that access to information and assets should align with specific access control policies.** This ensures that only authorized individuals can access certain information or resources, safeguarding against unauthorized use or breaches. Implementing stringent access controls according to defined policies protects sensitive data and supports the organization's overall information security strategy.

Lansweeper can support adherence to access control policies by providing detailed asset and user information as well as your users' login history. Through its inventory capabilities, **Lansweeper identifies which users have access to specific assets**, enabling IT administrators to review and adjust access rights in line with the organization's access control policies. This ensures that access to information and assets is appropriately restricted according to role-based permissions, enhancing the security of sensitive information and compliance with established policies.

**Lansweeper also integrates with ITSM and CMDB solutions** like Jira Service Management, ServiceNow, HaloITSM and more. These tools can use Lansweeper data as their foundation to manage user access, including reviewing and modifying access through ticketing and automations.

### Relevant Reports:

- **Last User Logon**
- **Windows Computer Logon History**

# 8.6 Capacity Management

**Control 8.6 underscores the necessity of monitoring and managing resource usage to align with both current and anticipated capacity demands.** This involves regularly reviewing your resource consumption against capacity and adjusting as necessary to ensure that your infrastructure can support your operations without interruption. Effective capacity management is essential for maintaining optimal performance and avoiding potential bottlenecks or system failures.

**Through performance metrics,** Lansweeper gives you insight into the capacity and resource usage of your IT assets. It gathers and analyzes data on resource usage across the IT infrastructure to identify current capacity levels and forecast future needs. This enables you to adjust your resources effectively, ensuring they meet current and anticipated demands without overutilization or underutilization, thereby maintaining optimal performance and supporting strategic capacity management.



**Lansweeper reports on the storage capacity** of your servers, computers, and SAN/NAS devices and provides detailed insights into storage utilization. This allows you to monitor disk space effectively, identifying potential capacity issues before they impact system performance or data storage capabilities. Thanks to precise, up-to-date reports, you can proactively manage your storage resources, ensuring they align with current and future requirements, thus maintaining system efficiency and avoiding potential disruptions.

(DS1520+)

Synology NAS

Scan server:

Last scan attempt: 08/05/2022 09:40:42

Summary
Location
Scanned OIDs (33)
Docs
Comments(1)
Tickets

#### Asset information

Asset type: NAS

DNS name:

OS: GNU/Linux

Domain:

Manufacturer: Synology

Model: DS1520+

Memory: 7.6 GiB

Processor: Intel Celeron J4125 CPU @ 2.00GHz

SKU: SKU0

DeviceVersion: DS1520+ 7.1-42661

OID: 1.3.6.1.4.1.8072.3.2.10

SSH server: SSH-2.0-OpenSSH\_8.2

#### Asset information continued

State: Active

Serial:

Purchased: 12/10/2021

Warranty: 12/09/2022

#### Scan summary

Scan status: ■■■

Scan server:

Created at: 12/10/2021 14:39:34

Last successful scan: 08/05/2022 09:40:42

Last scan attempt: 08/05/2022 09:40:42

#### Location

IP location:

Asset location: -

Location:

Contact:

Building:

#### Custom fields

Price: \$

#### Asset groups

Default group
NAS's

#### Partition information

Name	Size	Available	Used	Space used	Mounted on
devtmpfs	3.8 GiB	3.8 GiB	0 KiB	<div style="width: 0%; height: 10px; background-color: #ccc;"></div>	0% /dev
tmpfs	3.8 GiB	3.8 GiB	0 KiB	<div style="width: 0%; height: 10px; background-color: #ccc;"></div>	0% /sys/fs/cgroup
tmpfs	3.8 GiB	3.8 GiB	812 KiB	<div style="width: 2%; height: 10px; background-color: #ccc;"></div>	1% /tmp
tmpfs	3.8 GiB	3.8 GiB	236 KiB	<div style="width: 6%; height: 10px; background-color: #ccc;"></div>	1% /dev/shm
/dev/mapper/cachedev_0	27.9 TiB	9 TiB	18.9 TiB	<div style="width: 68%; height: 10px; background-color: #00aaff;"></div>	68% /volume1
tmpfs	3.8 GiB	3.8 GiB	19 MiB	<div style="width: 0.5%; height: 10px; background-color: #ccc;"></div>	1% /run
/dev/md0	2.3 GiB	527 MiB	1.6 GiB	<div style="width: 77%; height: 10px; background-color: #00aaff;"></div>	77% /
/dev/loop0	14.9 GiB	14.7 GiB	57 MiB	<div style="width: 0.4%; height: 10px; background-color: #ccc;"></div>	1% /volume

**Integrate Lansweeper with your IT operation management solutions** like PRTG, SenHub, and more to supply these tools with always-accurate device information that supplements monitoring of specific data points. This allows organizations to monitor and adjust the use of resources effectively, ensuring that capacity is managed in line with current and future requirements.

## Relevant Reports:

- [Windows Performance Counter Statistics](#)
- [Linux Performance Counter Statistics](#)
- [Windows & Linux Performance Counters Statistics](#)
- [Windows Disk Space Audit](#)

## 8.7 Protection Against Malware

**Control 8.7 mandates the implementation of anti-malware measures, coupled with user education to heighten awareness.** This approach not only involves deploying technical solutions to detect and block malware but also ensures that users understand their role in preventing malware infections, enhancing the organization’s overall defense against malicious software threats.

**Lansweeper’s Risk Insights** provide you with an overview of all at-risk assets in your IT environment as well as all known vulnerabilities threatening them. Lansweeper makes a comprehensive scan of your networked assets and compares them to vulnerability data drawn from the VulnCheck, VulDB, CISA, and MS databases. These vulnerability insights allow you to prioritize and respond to security threats promptly, strengthening your organization’s security posture against potential breaches.

RISK INSIGHTS ⓘ		Vulnerable assets				
Vulnerable assets 2,307		NAME	SEVERITY: CRITICAL ▼	SEVERITY: HIGH	SEVERITY: MEDIUM	TYPE
Ignored assets	2	<input type="checkbox"/> ZORLSRV01.zorin.local	166 vulnerabilities	915 vulnerabilities	814 vulnerabilities	Linux
Active vulnerabilit...	13,372	<input type="checkbox"/> UVMFRANK-SQL	120 vulnerabilities	1496 vulnerabilities	865 vulnerabilities	Windows
Ignored vulnerabilities	3	<input type="checkbox"/> 10.40.32.4	117 vulnerabilities	613 vulnerabilities	550 vulnerabilities	Linux
Insights	✚	<input type="checkbox"/> UVMMac-Esben	103 vulnerabilities	823 vulnerabilities	823 vulnerabilities	Apple Mac
Hardware lifecycle	31	<input type="checkbox"/> CONHQLWS02.contoso.local	101 vulnerabilities	398 vulnerabilities	488 vulnerabilities	Linux
OS lifecycle	52	<input type="checkbox"/> METLHYP01	92 vulnerabilities	232 vulnerabilities	186 vulnerabilities	Citrix XenServer
Custom views		<input type="checkbox"/> UVMW10BPTESTS	91 vulnerabilities	1103 vulnerabilities	654 vulnerabilities	Windows
Customize view	☰	<input type="checkbox"/> UVMW10CLIENTKDS	89 vulnerabilities	1174 vulnerabilities	690 vulnerabilities	Windows
Advanced filter view	☰	<input type="checkbox"/> UVMDEVTOOLS01	85 vulnerabilities	991 vulnerabilities	494 vulnerabilities	Windows
Export view	📄	<input type="checkbox"/> CONHQLWS01.contoso.local	81 vulnerabilities	337 vulnerabilities	420 vulnerabilities	Linux
		<input type="checkbox"/> UVMW10-ROOROO	76 vulnerabilities	746 vulnerabilities	480 vulnerabilities	Windows
		<input type="checkbox"/> UVMDEVTOOLS02	72 vulnerabilities	955 vulnerabilities	473 vulnerabilities	Windows
		<input type="checkbox"/> UVMTHIBO-TST3	72 vulnerabilities	867 vulnerabilities	447 vulnerabilities	Windows
		<input type="checkbox"/> UVMTHIBO-TST1	72 vulnerabilities	867 vulnerabilities	447 vulnerabilities	Windows
		<input type="checkbox"/> CONHQLWS03.contoso.local	72 vulnerabilities	474 vulnerabilities	415 vulnerabilities	Linux
		<input type="checkbox"/> UVM2019CORE2	66 vulnerabilities	1450 vulnerabilities	548 vulnerabilities	Windows
		<input type="checkbox"/> UVM2019CORE1	66 vulnerabilities	1450 vulnerabilities	548 vulnerabilities	Windows

**Create a compliance baseline**, using Lansweeper's powerful and granular reporting capabilities. By comparing your asset data against the established baseline, you can easily spot any deviations that could spell trouble. Lansweeper tracks your antivirus status, running services, required software and/or agents, registry key values and file versions, unapproved software, unauthorized local administrators, and more to help you ensure compliance with your baseline security standards.

**Easily spot unauthorized software** thanks to Lansweeper's comprehensive software discovery. Lansweeper automatically scans all software within your network. Once your software has been scanned you can mark it as approved or unauthorized on-premises or use the custom report in Lansweeper Sites. Once you've set up your software authorization you can easily audit your network for unauthorized software and identify the exact devices they are on to start taking action.

OS Name	Publisher	Computer count	Approved
ms-resource/AppStoreName	Microsoft Corporation	59	●
Microsoft Visual C++ 2013 Redistributable (x86)	Microsoft Corporation	16	●
Google Chrome	Google LLC	14	●
Windows Internet Explorer 11	Microsoft Corporation	11	●
Microsoft Edge Update		10	●
Microsoft Visual C++ 2013 Redistributable (x64)	Microsoft Corporation	9	●
Microsoft Visual C++ 2015-2019 Redistributable (x86)	Microsoft Corporation	9	●
Microsoft Update Health Tools	Microsoft Corporation	9	●
Microsoft Edge	Microsoft Corporation	9	●
LsAgent	Lansweeper	9	●
Microsoft Edge WebView2 Runtime	Microsoft Corporation	8	●
Npcap OEM	Nmap Project	8	●
VMware Tools	VMware, Inc.	8	●
Microsoft Visual C++ 2015-2019 Redistributable (x64)	Microsoft Corporation	8	●
Xbox Game bar	Microsoft Corporation	8	●
Phone Link	Microsoft Corporation	7	●
Movies & TV	Microsoft Corporation	7	●
Microsoft Store	Microsoft Corporation	7	●
Microsoft Visual C++ 2015-2022 Redistributable (x64)	Microsoft Corporation	7	●
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	7	●
Wazuh Agent	Wazuh, Inc.	7	●

**Maintain reliable backups** to ensure data availability in case of a ransomware incident or system failures. By identifying and tracking backup solutions, Lansweeper enables you to verify whether critical systems are properly backed up, assess potential gaps in coverage, and ensure alignment with compliance standards. This visibility helps you mitigate the risk of data loss and strengthen your overall disaster recovery strategy.

**Tackle unapproved local administrators** to safeguard your critical system files and settings from unauthorized modifications that could lead to security breaches or data loss. Maintaining strict control over local administrator access is a critical strategy for protecting against malware. By limiting these privileges, you can significantly reduce the risk of malicious software gaining the necessary permissions to execute harmful actions. This approach ensures that only authorized and necessary applications or users can make significant changes to the system.

**Fuel your cybersecurity tools with rich Lansweeper data** to provide detailed insights into the asset environment. This leads to more effective management and remediation of malware through ticketing or automations based on data provided by Lansweeper. Lansweeper seamlessly integrates with cybersecurity solutions like Axonius, Armis and ITSM solutions like Jira Service Management, Servicenow and more.

### Relevant Reports:

- **Unauthorized Administrators**
- **Local Admin Accounts**
- **Unauthorized Software**

## 8.8 Management of Technical Vulnerabilities

**Control 8.8 focuses on the management of technical vulnerabilities.** It involves gathering information on system vulnerabilities, assessing the risks they pose to the organization, and implementing suitable measures to mitigate these risks. This control ensures that vulnerabilities are identified, evaluated, and addressed proactively, minimizing potential security threats to the organization's information systems.

**Lansweeper's Risk Insights** provide you with a clear view of all vulnerabilities threatening your network. By comparing the comprehensive IT asset data Lansweeper discovers to known vulnerability data drawn from the VulnCheck, VulDB, CISA, and MS databases, it compiles a list of all at-risk assets in your network. Each entry shows the affected asset and the vulnerabilities threatening it, as well as additional information, like a full description of the vulnerability, the CVSS score, patch availability, and additional resources. This allows you to quickly assess which issues are the greatest threat to your network and prioritize your remediation efforts.

RISK INSIGHTS		Vulnerable assets				
Vulnerable assets 2,307		NAME	SEVERITY: CRITICAL	SEVERITY: HIGH	SEVERITY: MEDIUM	TYPE
Ignored assets	2	<input type="checkbox"/> ZORLSRV01.zorin.local	166 vulnerabilities	913 vulnerabilities	814 vulnerabilities	Linux
Active vulnerabilit...	13,372	<input type="checkbox"/> UVMFRANK-SQL	120 vulnerabilities	1496 vulnerabilities	865 vulnerabilities	Windows
Ignored vulnerabilities	3	<input type="checkbox"/> 10.40.32.4	117 vulnerabilities	613 vulnerabilities	550 vulnerabilities	Linux
Insights		<input type="checkbox"/> UVMMac-Esben	103 vulnerabilities	823 vulnerabilities	823 vulnerabilities	Apple Mac
Hardware lifecycle	31	<input type="checkbox"/> CONHQLWS02.contoso.local	101 vulnerabilities	398 vulnerabilities	468 vulnerabilities	Linux
OS lifecycle	52	<input type="checkbox"/> METLHYP01	92 vulnerabilities	232 vulnerabilities	186 vulnerabilities	Citrix XenServer
Custom views		<input type="checkbox"/> UVMW10BPTESTS	91 vulnerabilities	1103 vulnerabilities	654 vulnerabilities	Windows
		<input type="checkbox"/> UVMW10CLIENTKDS	89 vulnerabilities	1174 vulnerabilities	690 vulnerabilities	Windows
		<input type="checkbox"/> UVMDEVTOOLS01	85 vulnerabilities	991 vulnerabilities	494 vulnerabilities	Windows
Customize view		<input type="checkbox"/> CONHQLWS01.contoso.local	81 vulnerabilities	337 vulnerabilities	420 vulnerabilities	Linux
Advanced filter view		<input type="checkbox"/> UVMW10-ROOROO	76 vulnerabilities	746 vulnerabilities	480 vulnerabilities	Windows
Export view		<input type="checkbox"/> UVMDEVTOOLS02	72 vulnerabilities	955 vulnerabilities	473 vulnerabilities	Windows
		<input type="checkbox"/> UVMTHIBO-TST3	72 vulnerabilities	867 vulnerabilities	447 vulnerabilities	Windows
		<input type="checkbox"/> UVMTHIBO-TST1	72 vulnerabilities	867 vulnerabilities	447 vulnerabilities	Windows
		<input type="checkbox"/> CONHQLWS03.contoso.local	72 vulnerabilities	474 vulnerabilities	415 vulnerabilities	Linux
		<input type="checkbox"/> UVM2019CORE2	66 vulnerabilities	1450 vulnerabilities	548 vulnerabilities	Windows
		<input type="checkbox"/> UVM2019CORE1	66 vulnerabilities	1450 vulnerabilities	548 vulnerabilities	Windows

**Lansweeper also provides lifecycle information** for your assets where it is available. This includes end-of-Life and End-of-Support dates, as well as the status of your operating system or firmware. This allows you to retire or replace obsolete systems before they become a security risk, plan ahead for future purchases, and make sure that your systems are fully supported.

**Lansweeper can integrate with multiple cybersecurity applications** such as Splunk, Palo Alto Cortex XSOAR, ThreatAware, DeepSurface, Microsoft Sentinel, and more. These integrations enhance the tool by providing detailed asset data to improve their threat intelligence quality or provide additional context to threat intelligence already detected.

### Relevant Reports:

- [Hardware Lifecycle Overview](#)
- [OS Lifecycle Overview](#)

## 8.9 Configuration Management

**Control 8.9 mandates the thorough management of system configurations**, including their



**Lansweeper's Risk Insights** feature compiles a list of at-risk assets in your network and the vulnerabilities that are threatening them, based on vulnerability data from the VulnCheck, VulDB, CISA, and MS databases. This allows you to prioritize and address vulnerabilities promptly by applying the necessary patches and configuration changes.

**Achieve security baseline compliance** with Lansweeper's powerful and granular reporting capabilities. Create a configuration baseline to compare assets to and alert on any deviation. Lansweeper includes over 400 built-in and the option to create your own.

### Relevant Reports:

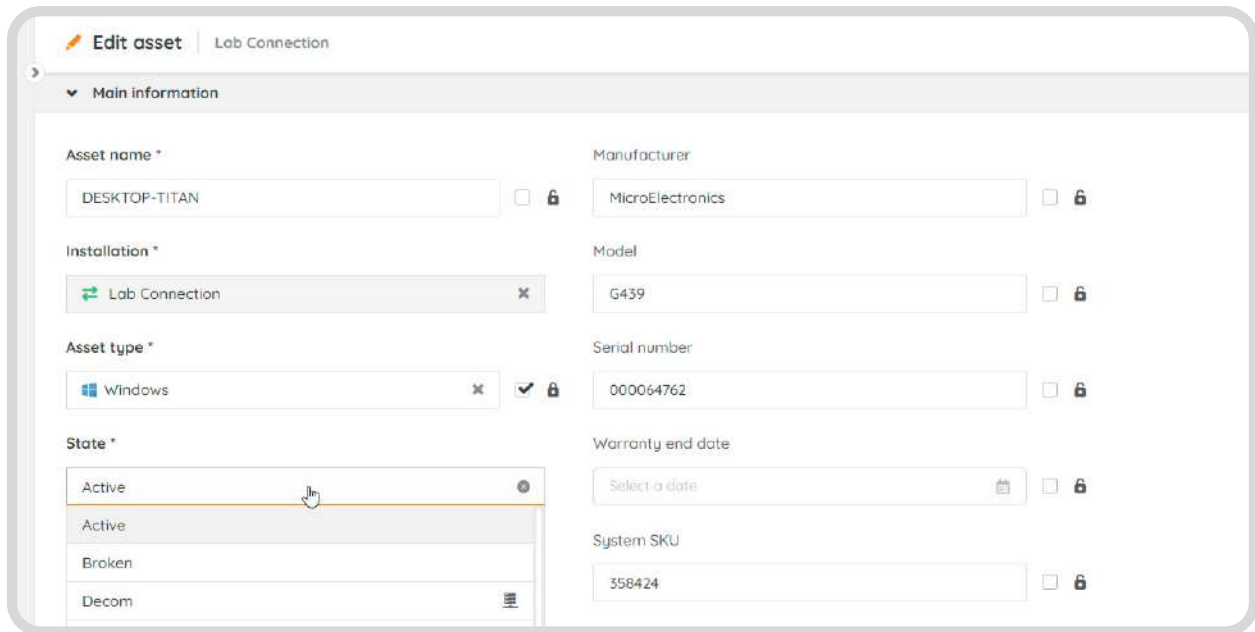
- **Software Changes in the Last 7 Days**
- **Newly Discovered Software in the Last 7 Days**

## 8.10 Information Deletion

**Control 8.10 emphasizes the need for securely deleting information from systems, devices, or storage media when it is no longer necessary.** This control ensures that outdated or unnecessary data is removed to prevent unauthorized access and reduce the risk of data breaches, maintaining the confidentiality and integrity of information within the organization.

Lansweeper cannot delete your old data for you, but it can be used to track the lifecycle of the assets that are used to store and access your data.

**Lifecycle tracking** allows you to manage your assets from acquisition to disposal. It is an essential part of effective asset management, ensuring assets are maintained, upgraded, or disposed of in accordance with organizational policies and standards. Lansweeper can track the lifecycle of assets from acquisition through deployment, usage, and eventual decommissioning through customizable asset statuses and states.



**Through integrations** with multiple ITAM solutions Lansweeper can enhance the data quality in your favorite tools like Asset Panda, Setyl, Timly, and more. Additionally, by integrating with ITSM tools like Jira Service Management and ServiceNow, you can use ticketing and automations along with the Lansweeper data to ensure data is deleted on decommission.

## 8.12 Data Leakage Prevention

**Control 8.12 mandates implementing data leakage prevention measures for systems, networks, and devices handling sensitive information.** This control aims to prevent unauthorized disclosure of sensitive data by applying stringent security measures and monitoring mechanisms across all platforms where such information is processed, stored, or transmitted, ensuring the organization's data remains secure and private.

**Lansweeper offers visibility into the devices and systems that handle sensitive information,** aiding in the implementation of data leakage prevention measures. By identifying where sensitive data resides, Lansweeper helps ensure that appropriate security controls are in place across networks and devices, preventing unauthorized access or transmission of sensitive information, and contributing to a comprehensive data protection strategy.

**Lansweeper also integrates seamlessly with leading ITSM and CMDB solutions** like Jira Service Management, ServiceNow, HaloITSM and more. These tools can use Lansweeper's granular data as their foundation for managing user access, including reviewing and modifying access through ticketing and automations.

## 8.13 Information Backup

**Control 8.13 requires maintaining and periodically testing backup copies of information, software, and systems in line with a specific backup policy.** This ensures that critical data and system functionality can be restored after incidents like data loss or system failures, maintaining operational continuity and data integrity. Regular testing of backups confirms their effectiveness and reliability for emergency use.

Thanks to Lansweeper's comprehensive discovery capabilities, **you always have a complete view of all servers, assets, shares, and databases containing critical information that needs to be backed up** in order to ensure they are compliant with your backup policies. On top of your IT assets, Lansweeper also inventories your backup agents and versions. Track and report on your agents' status to ensure that your backups and disaster recovery services are always enabled and up-to-date.

**Integrate Lansweeper with your ITSM and CMDB tools** like Jira Service Management, ServiceNow, HaloITSM and more, for an accurate and up-to-date inventory of assets that need to be included in backup routines. This ensures that backup copies of information, software, and systems are maintained and regularly tested in line with the organization's backup policies through ticketing and automations.

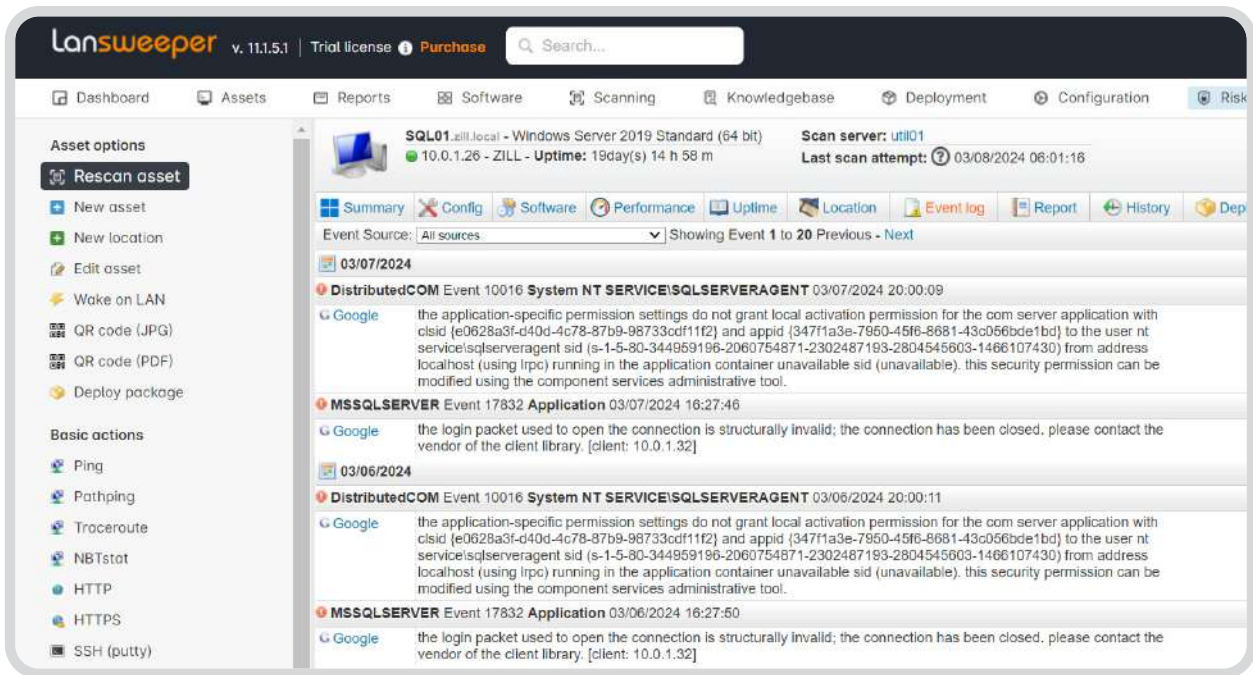
### Relevant Reports:

- [Veeam End of Life](#)
- [Microsoft SQL Servers and Their Installed Databases](#)

## 8.15 Logging

**Control 8.15 requires the creation, storage, protection, and analysis of logs detailing activities, exceptions, faults, and other significant events.** This process is vital for tracking system behavior, identifying potential security incidents, and facilitating forensic investigations, ensuring that all pertinent events within the IT environment are appropriately documented and analyzed for security and operational integrity.

**Thanks to Lansweeper's event log monitoring** you can swiftly identify and assess security events. Event logs provide insight into the goings-on of your IT infrastructure. This facilitates early detection of potential incidents or suspicious behavior, so you can quickly respond to and mitigate risks, or investigate security incidents, protecting operational integrity and data security.



**Create event log alerts** to notify you as soon as a critical event is scanned. The combination of Windows event log scanning targets and email alerts, lets you know within minutes when vital assets are showing any suspicious activity. You can set email notifications for critical or non-critical event logs to stay updated on the state of your network.

**Track your asset change history** to keep meticulous records of any changes in hardware, software, configurations, and user permissions. This allows you can detect, track, and investigate unauthorized changes, ensuring that all modifications align with security policies. Lansweeper aids in accountability and forensic analysis by maintaining a comprehensive audit trail, crucial for mitigating risks and ensuring compliance with regulatory requirements and policies.

**Integrate Lansweeper with a wide range of cybersecurity** applications such as Splunk, Palo Alto Cortex XSOAR, ThreatAware, DeepSurface, Microsoft Sentinel, and more. Lansweeper can supports these products by providing detailed asset data that improves their threat intelligence quality or provides additional context to threat intelligence already detected.

## Relevant Reports:

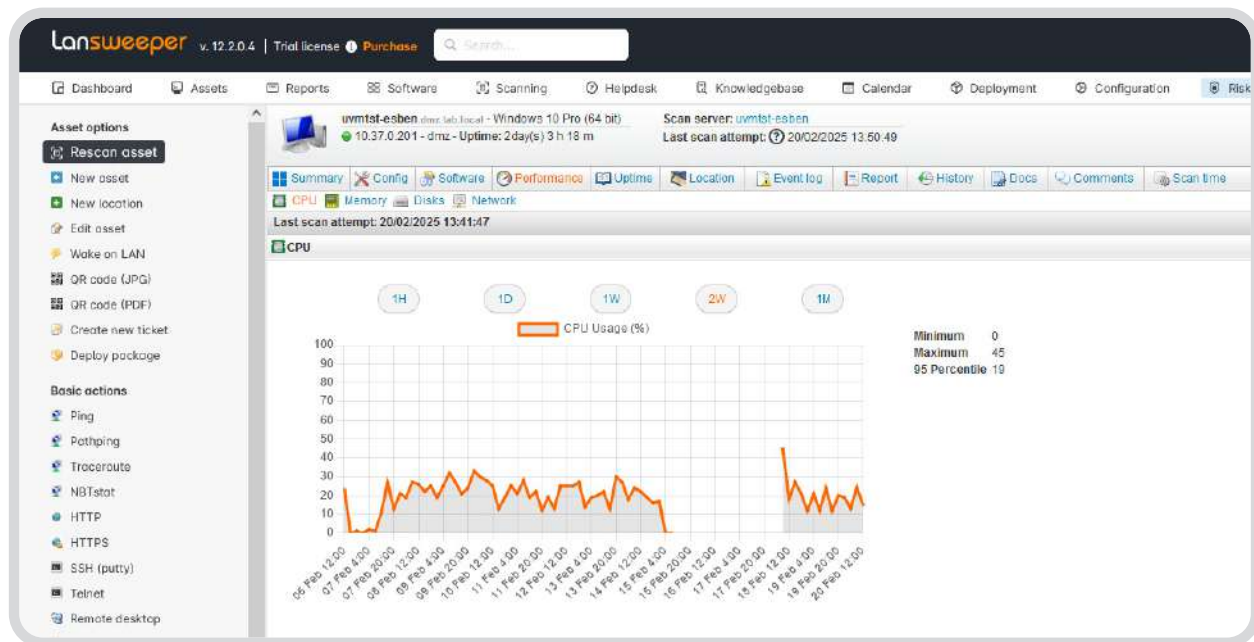
- **Windows Error events generated in last 7 days**

## 8.16 Monitoring Activities

**Control 8.16 mandates the continuous monitoring of networks, systems, and applications to detect unusual behavior, with necessary measures taken to assess potential security incidents.**

This proactive surveillance helps identify and respond to threats promptly, safeguarding information security.

Lansweeper helps by providing a comprehensive view of your networks, systems, and applications so that you can **monitor for any anomalies indicative of potential security incidents**. It extends its functionality by identifying and classifying devices for a **seamless integration** with monitoring tools like PRTG and SolarWinds, ensuring a wide-ranging surveillance of all critical assets. Additionally, Lansweeper monitors key performance metrics, including CPU, memory, and network utilization, offering insights into performance-related issues that could highlight security concerns, thus bolstering the organization's monitoring and incident response capabilities.



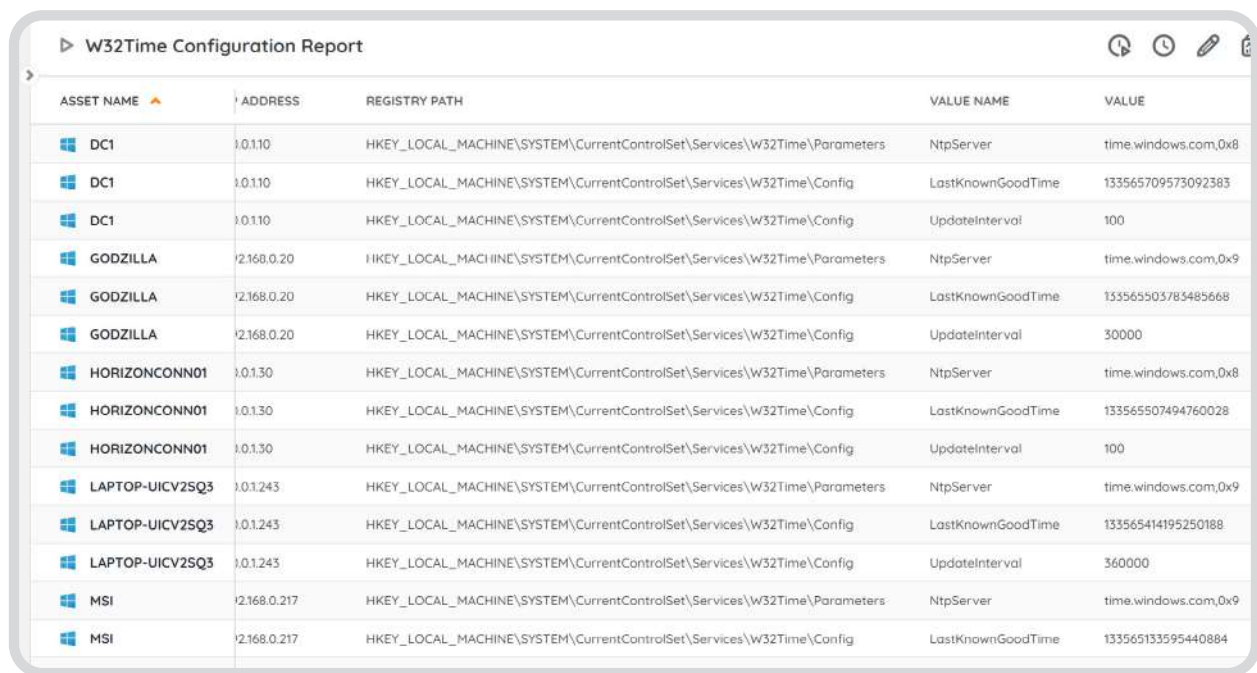
### Relevant Reports:

- [Windows Performance Counter Statistics](#)
- [Linux Performance Counter Statistics](#)
- [Windows & Linux Performance Counters Statistics](#)
- [Windows Disk Space Audit](#)

## 8.17 Clock Synchronization

**Control 8.17 stipulates that the clocks of all information processing systems within an organization should be synchronized to a reliable and approved time source.** This synchronization ensures consistency in timekeeping across systems, which is crucial for accurate log management, security incident tracking, and the coordination of time-sensitive operations, thereby enhancing the reliability and integrity of data processes.

**Lansweeper scans Windows registry keys to gather configuration data, helping administrators track and manage settings across their network.** By querying the registry, Lansweeper collects valuable information on software configurations, system settings, and other key data points. To ensure proper time settings on Windows systems, you can check registry keys related to the Windows Time Service.



ASSET NAME	ADDRESS	REGISTRY PATH	VALUE NAME	VALUE
DC1	10.0.1.10	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters	NtpServer	time.windows.com,0x8
DC1	10.0.1.10	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	LastKnownGoodTime	133565709573092383
DC1	10.0.1.10	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	UpdateInterval	100
GODZILLA	172.168.0.20	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters	NtpServer	time.windows.com,0x9
GODZILLA	172.168.0.20	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	LastKnownGoodTime	133565503783485668
GODZILLA	172.168.0.20	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	UpdateInterval	30000
HORIZONCONN01	10.0.1.30	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters	NtpServer	time.windows.com,0x8
HORIZONCONN01	10.0.1.30	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	LastKnownGoodTime	133565507494760028
HORIZONCONN01	10.0.1.30	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	UpdateInterval	100
LAPTOP-UICV2SQ3	10.0.1.243	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters	NtpServer	time.windows.com,0x9
LAPTOP-UICV2SQ3	10.0.1.243	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	LastKnownGoodTime	133565414195250188
LAPTOP-UICV2SQ3	10.0.1.243	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	UpdateInterval	360000
MSI	172.168.0.217	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters	NtpServer	time.windows.com,0x9
MSI	172.168.0.217	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	LastKnownGoodTime	133565133595440884

### Relevant Reports:

- [Scanned Registry Keys](#)
- [W32Time Configuration Report](#)

## 8.18 Use of Privileged Utility Programs

Control 8.18 focuses on the strict regulation of privileged utility programs that have the potential to bypass system and application controls. These powerful tools must be used sparingly and under strict oversight to prevent unauthorized or harmful alterations to system configurations and operations, ensuring that only authorized personnel have access to such utilities under controlled conditions.

Lansweeper can help monitor and manage the use of privileged utility programs by identifying and monitoring these programs on the network, ensuring they are only available to authorized personnel. By tightly controlling access to these tools, Lansweeper helps maintain system and application security, preventing unauthorized actions that could bypass critical controls.

## 8.19 Installation of Software on Operational Systems

**Control 8.19 mandates the establishment of secure processes for installing software on operational systems, ensuring that installations do not compromise system integrity or security.** This involves setting up strict procedures and safeguards to manage how software is added to systems, verifying the software's legitimacy, and assessing its impact on the existing security posture to prevent unauthorized or harmful installations.

**Use Lansweeper's deployment and SCCM integrations to manage software installations on operational systems securely.** Through integrations with your deployment tools, you can leverage Lansweeper's data to ensure that only approved software is installed, in line with organizational policies. This approach helps maintain system security and integrity, effectively preventing unauthorized software installations and aligning with secure management practices for operational systems.

### Relevant Reports:

- [Unauthorized Software](#)
- [Assets with Unauthorized Software](#)

## 8.20 Networks Security, 8.21 Security of Network Services, and 8.22 Segregation of Networks

We are grouping together controls 8.20, 8.21, and 8.22 since they are closely related, and the way Lansweeper can support these controls is the same.

**Control 8.20 emphasizes the need to secure and manage networks and network devices to protect the information within systems and applications.** This control requires implementing measures to safeguard network infrastructure against unauthorized access, threats, and vulnerabilities, ensuring that data transmitted across networks is protected consistently and effectively.

**Control 8.21 mandates the identification, implementation, and monitoring of security mechanisms and service levels for network services.** It requires that network services have clearly defined security measures and service requirements to ensure the protection and reliability of network operations, facilitating ongoing monitoring and management to safeguard against security risks.

**Finally, control 8.22 calls for network segregation within an organization, ensuring that different groups of information services, users, and systems are separated within the network.** This segregation is critical for minimizing potential cross-system security threats and ensuring that sensitive information and critical services are compartmentalized to enhance overall security.

Lansweeper helps you achieve all three of these controls by identifying and mapping out devices, subnets, and VLANs across networks. **The comprehensive view of your devices and systems as well as their status, configurations, and dependencies allows you to safeguard their security.** It also facilitates the organization of assets into categories based on their functions, application stacks, or user access levels, supporting effective network segregation.

This capability allows for refined control over access and network segmentation, enhancing security by ensuring that users and systems have access only to the networks and information necessary for their roles. In case of a security incident, **detailed network diagrams** can immediately tell you what parts of your network are at risk.

**The Risk Insights feature** also gives you a comprehensive overview of all vulnerabilities threatening your network, as drawn from the VulnCheck, CISA, and MS databases. The list provides additional detail for each vulnerability like CVSS scores, patch availability, and additional resources. This way you can prioritize and address vulnerabilities before they can become an issue.



## Relevant Reports:

- [Bitlocker Drive Encryption](#)
- [Active Directory BitLocker Recovery Keys](#)
- [Trusted Platform Modules](#)
- [Windows Certificate Overview](#)
- [Windows Certificates With Expired Key](#)
- [Windows Self-Signed Certificates](#)

## 8.27 Secure System Architecture and Engineering Principles

**Control 8.27 mandates the establishment, documentation, maintenance, and application of secure system architecture and engineering principles.** This control ensures that security is integrated into the fabric of information system development, applying robust security standards and practices throughout all phases of system design and engineering to mitigate risks and enhance system resilience.

By tracking software and hardware specifications, firmware, services, and group memberships, **Lansweeper ensures that security measures like appropriate group implementations are in place.** This comprehensive oversight aids in the secure development and maintenance of information systems. It helps you adhere to secure system architecture and engineering principles by ensuring that administration procedures and principles are properly implemented.

## 8.31 Separation of Development, Test and Production Environments

**Control 8.31 dictates that development, testing, and production environments must be kept separate and secure to prevent unauthorized access and data breaches.** This separation helps ensure that developmental changes do not unintentionally affect the live environment, safeguarding the production system's integrity and stability.

There are several ways in which you can classify your assets within Lansweeper to identify and classify them as belonging to either your development, test, or production environment.

- **Use custom fields to label your assets.** These fields can be used to add any information to your assets that you may find useful. That includes their environment. Custom reports also let you locate these assets based on the custom fields you set.

- **Use existing asset naming conventions** to quickly document details. Servers can be deployed with naming conventions to describe the environment. This then allows you to filter on the naming convention in the multi-edit asset menu, and quickly edit diagram. For example, you could filter Windows servers with names containing 'PRD' - if your organization names production servers with that abbreviation - and update the appropriate custom field for tracking environment, to 'Production.'

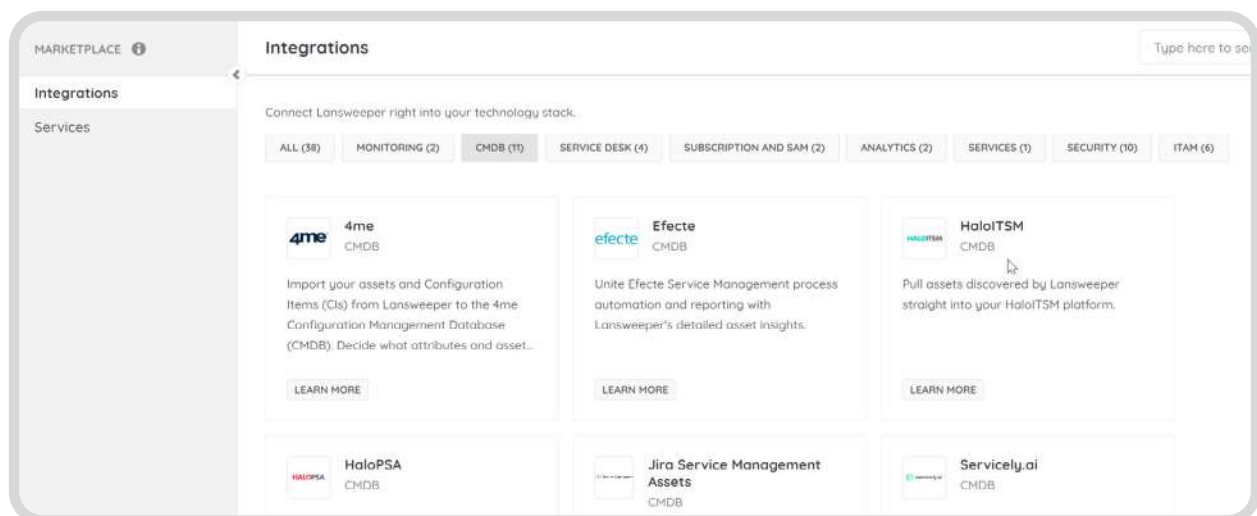
Once you have a reliable way of identifying these assets as part of a certain environment, you can then use this info, in combination with Lansweeper's network insights and **diagrams**, to make sure that your environments are properly separated and secured.

## 8.32 Change Management

**Control 8.32 necessitates that all modifications to information processing facilities and systems go through established change management procedures.** This ensures that changes are assessed, authorized, implemented, and reviewed in a controlled manner, minimizing the risk of disruptions or security vulnerabilities introduced by the changes, thereby maintaining system integrity and reliability.

**Lansweeper's comprehensive asset inventory can serve as a robust foundation for a Configuration Management Database (CMDB),** facilitating effective change management. By maintaining an up-to-date and detailed overview of information processing facilities and systems, you can make an informed assessment of the impact of proposed changes, ensuring that all modifications are accurately recorded, analyzed, and implemented within a structured framework. This approach minimizes risks associated with changes, promoting stability and security in information systems.

Lansweeper also **seamlessly integrates with leading ITSM/CMDB platforms**, significantly enhancing change management processes. These integrations let you sync Lansweeper's detailed asset inventory directly into ITSM solutions, providing a unified view of assets and facilitating effective tracking, analysis, and management of changes across the IT landscape.



## Discover What Lansweeper Can Do for Your ISO 27001 Certification

ISO27001 provides a coherent and comprehensive framework for establishing, implementing, maintaining, and improving an Information Security Management System (ISMS) to safeguard your information assets. By simply adhering to the standards it sets, you can systematically manage your information security risks, ensuring the confidentiality, integrity, and availability of data. ISO 27001 certification is a great way to demonstrate a commitment to robust security practices, build trust with stakeholders, and help your organization meet regulatory and business requirements.

Ultimately, achieving ISO 27001 certification is not just about compliance but also about establishing a culture of continuous improvement in information security management. It is an ongoing effort to strengthen resilience against cyber threats, foster trust, and ensure business continuity in an increasingly digital and interconnected world.

Lansweeper helps to streamline the implementation of many of ISO 27001's controls. From inventory management to compliance auditing, Lansweeper supports your organization in identifying vulnerabilities, managing assets, and enforcing security policies. Seamless integrations allow you to further leverage Lansweeper's technology asset data throughout your tech stack. These capabilities help you prepare for ISO 27001 certification by providing the visibility and insights you need to address both technical and operational controls.

[Try Lansweeper Today](#)

[Request a Demo](#)