



Starhive + Lansweeper for compliance

Reduce your risk and make GRC hassle-free with instant insight into which assets each control applies to.

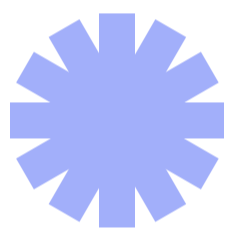
CIS compliance / CIS safeguard / 4.4 Implement and Manage a Firewall on Servers

TITLE ID
4.4 Implement and Manage a Firewall on Servers
14/11/25 1 min Charlotte Nicolaou

Owner: Charlotte Nicolaou
Priority: High
CIS Control: 4. Secure Configuration of Enterprise Assets and Software
Asset Type: Devices
Security Function: Protect
Implementation: IG2, IG3, IG1
Description: Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.
Technology Association: Servers

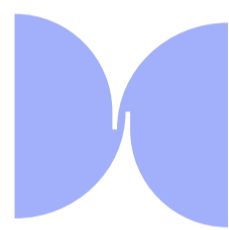
Relationships: Graph, Tree
Inbound relationships: [checked]
Comments: [unchecked]

How to get started



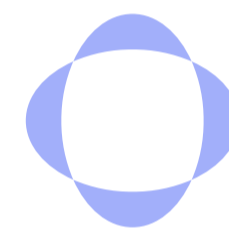
Import assets to Starhive

Configure Starhive for your Lansweeper assets and set up the import to run manually or on a schedule.



Document your frameworks

Bring your GRC frameworks, controls, and safeguards into Starhive ready for mapping to underlying technology.



Link assets to controls

Create the relationships between controls and asset groups. When new assets are added, automations can include them too.

[Documentation](#)

Supported GRC frameworks

- Tablets (56)
- MacBooks (18)
 - MB-816
 - MB-817
 - MB-818
 - MB-819
- Load more
- CIS safeguard
 - 3.6 Encrypt Data on End-User Devices
 - 4.11 Enforce Remote Wipe Capability on Portable End-User Devices
 - 4.5 Implement and Manage a Firewall on End-User Devices

Any framework is supported in Starhive due to our flexible data structure. This includes SOC 2, ISO, NIST, and DORA.

We have a template for CIS that can be adapted to other frameworks. Or get in touch with us and we'll help you import your GRC frameworks.

[Get in touch](#)