

[3 STEPS]

3 steps for a hardened baseline for your storage & backup systems

Establish a hardened configuration baseline for multi-vendor storage and backup systems, then validate it autonomously. Deviations and drift are identified automatically.

- 01

Onboard & scan

Connect your storage and backup systems. Agentless and multi-vendor, so every layer is assessed.
- 02

Select policies

Built-in frameworks or your own baseline.
- 03

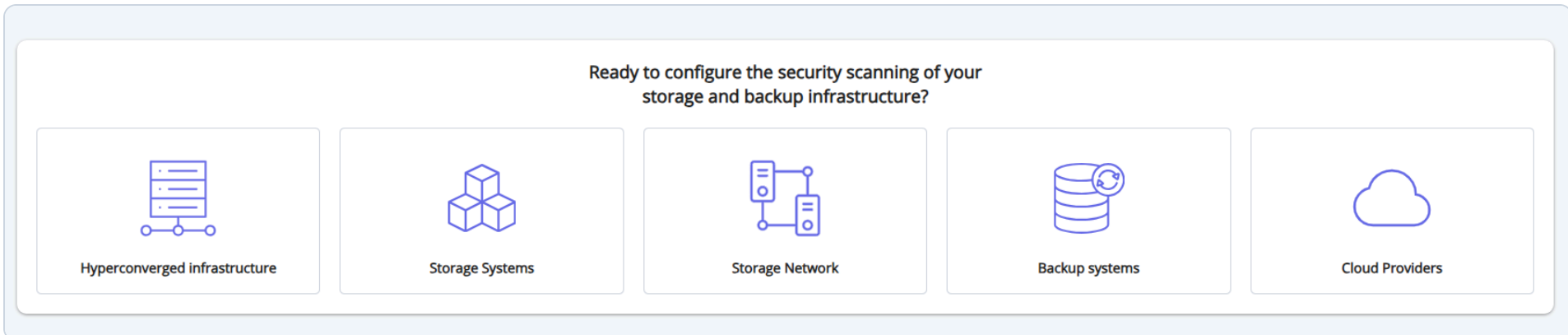
Review & remediate

Prioritized findings, validated before every fix.

01

Onboard & scan

Connect your storage and backup systems. Agentless and multi-vendor, so every layer is assessed.



/ Settings > Scan

02

Select your evaluation policies

Start from built-in policies. Or define your own baseline for each platform.

[BUILT-IN POLICIES]

CIS Controls

NIST SP800-209

DORA

NIS2

FFIEC

NERC CIP

Singapore MAS TRM

UK NCSC CAF

SG BL1 to BL5: Essentials to Fortified

[OR DEFINE YOUR OWN]

My ONTAP baseline

My Commvault baseline

My Hitachi VSP baseline

My Cisco/Brocade baseline

One baseline per platform, built to your standards.

03

Review & remediate

Every finding is prioritized and mapped to the frameworks you selected.
Two examples:

Configuration hardening example

Restrict storage administrative IP interface access

#3708 Data Domain **ddlab**: Client ACL is misconfigured

Check name | SG-C0197T061V01: Client IP ACL

Details

Activity

Description

Data Domain MyBaseline CIS Control v8 13.5 CIS Control v8 13.10 CIS v8 IG 2 +17

Client IP Access Control List (ACL) is incorrectly configured on the system. An Access Control List is essential for defining allowed client IP addresses.

Net filter configuration

- IPv4 admin-interface ethV0 22, 443 all clients, IPv6 admin-interface ethV0 22, 443 all clients

Baseline violation example

Two-person approval is not enabled for destructive backup changes

#4405 Storage Protect **ddlab**: Command approval is disabled

Check name | SG-C0166T169V01: Command approval is disabled

Details

Activity

Description

Storage Protect Fortune 500 BL NIST SP800-53rs Control AC-3(2) NIST SP800-53rs Control CM-5 NIST SP800-53rs Control CM-5(4) +5

Command feature approval is disabled.

Command approval incorrectly configured on the following server

- ddlab - Command approval is disabled

Then fix it, with full control

Remediation is proposed, reviewed and validated before it is carried out, so nothing changes in your storage and backup systems without you knowing.

Review

→

Validate

→

Execute

→

Rescan

Fix It

[AI-BASED REMEDIATION, WITH CONTROLS]
Review the proposed remediation, validate it, then execute it with **Fix it**. Rescan to confirm the result.

Everything is validated before any fix runs.
Full transparency. Full control.

[ONGOING]

Stay validated

Subscribe to dashboards to track your baseline compliance score and remediation progress over time.

/ Baseline compliance score

/ Remediation progress

/ Deviations and drift, identified automatically

core6
Storage & Backup Systems.
Autonomously Secured.

No breaches. No blind spots.
Just bulletproof storage & backup systems.

www.core6.com