

Establishing Secure Configuration Baselines

Best Practice Guide for Storage & Backup Systems



Four best practices to help you set secure configuration baselines for your storage & backup systems

Storage and backup systems are the backbone that support data integrity, availability, confidentiality, and recovery. However, these critical systems are often overlooked in security strategies – leaving them vulnerable to misconfigurations and cyber threats.

Establishing secure configuration baselines for storage and backup systems is essential to protect against unauthorized access, data breaches, and compliance violations.

A **secure configuration baseline** is a set of security settings that serve as a benchmark for configuring systems consistently and securely. It ensures that all systems adhere to an organization's security policies and industry best practices.

For storage and backup systems, which handle sensitive data and maintain critical operations, a secure configuration baseline mitigates risks associated with misconfigurations, weak encryption protocols, and unauthorized changes.

Breached Storage & Backup Systems

Misconfigurations and weak cryptographic settings are among the most common vulnerabilities exploited by attackers. According to the **Open Web Application Security Project (OWASP)**, security misconfigurations rank high in the **OWASP Top Ten** list of critical web application security risks. Similarly, the **Verizon Data Breach Investigations Report (DBIR)** consistently highlights how misconfigurations contribute to data breaches, emphasizing that even minor configuration errors can lead to significant security incidents.

Some of the recent examples involving storage and backup include the Russian cyberattack on Ukraine's largest mobile phone provider, Kyivstar and the [ransomware attack on UnitedHealth](#).



Alignment with Industry Standards and Regulations

So, it's no surprise that several industry standards and regulatory frameworks emphasize the importance of secure configurations. For example -

Source	Section	Requirement
NIST CSF Protect (PR)	PR.IP-1	"A baseline configuration of information technology/ industrial control systems is created and maintained."
NIST SP 800-53	CM-2: Baseline Configuration	Organizations are required to develop, document, and maintain a current baseline configuration of information systems.
NIST SP 800-53	CM-7: Least Functionality	"The organization configures the information system to provide only essential capabilities and limits unnecessary functionality."
NIST SP 800-53	CM-6: Configuration Settings	"Establish ... the most restrictive mode.... Identify and approve deviations ... Monitor and control changes to the configuration settings"
CIS Controls	Safeguard 4.1	"Establish and maintain a secure configuration process for all enterprise assets."
Digital Operational Resilience Act (DORA): Regulatory Technical Standards	Article 11: ICT Systems, Protocols and Tools	"Financial entities shall ensure the performance of automated vulnerability scanning and assessments, and the implementation of a secure configuration baseline of all network components and hardening the network and network devices according to vendor instructions... Identification of secure configuration baseline for ICT assets that will minimise their exposure to cyber threats and measures to verify regularly that these baselines are those that are effectively deployed. The secure configuration baseline shall take into account leading practices and appropriate techniques referred to in standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012."
Digital Operational Resilience Act (DORA): Regulatory Technical Standards	Article 13: ICT Security Tools and Policies	"Secure configuration baselines, network hardening, and session termination after inactivity limit potential attack vectors."
PCI DSS V4	Requirement 2	Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.... Implement secure configurations for all system components, addressing security vulnerabilities and considering industry best practices.
FFIEC	Configuration Management	Financial institutions must implement robust configuration management to ensure the security and integrity of systems

Challenges in Securing Storage and Backup Systems

Despite the clear mandates from industry standards and regulations, organizations face challenges in implementing secure configurations for storage and backup systems:

Complexity and Diversity	Insufficient Storage / Backup Security Expertise	Lack of Automation	Evolving Threat Landscape
Storage and backup environments often consist of heterogeneous systems with varying architectures, non-standard operating systems, command sets and configurations.	Often security personnel are not well familiar with storage and backup architectures, whereas storage and backup administrators are not focused on security and hardening.	Manual processes for establishing and maintaining baselines are time-consuming and prone to errors; developing home-grown scripts, keeping them operational and up to date, producing detailed finding reports and managing their lifecycle – equals to developing a product – that is, not a negligible one-time effort.	Cyber threats targeting storage and backup systems are becoming more sophisticated, requiring continuous monitoring and updates to configurations.

So, what can be done?

We'll explain how to build a **secure configuration baseline process**, which should have four steps.

CONTINUOUS SECURITY IMPROVEMENT & VALIDATION

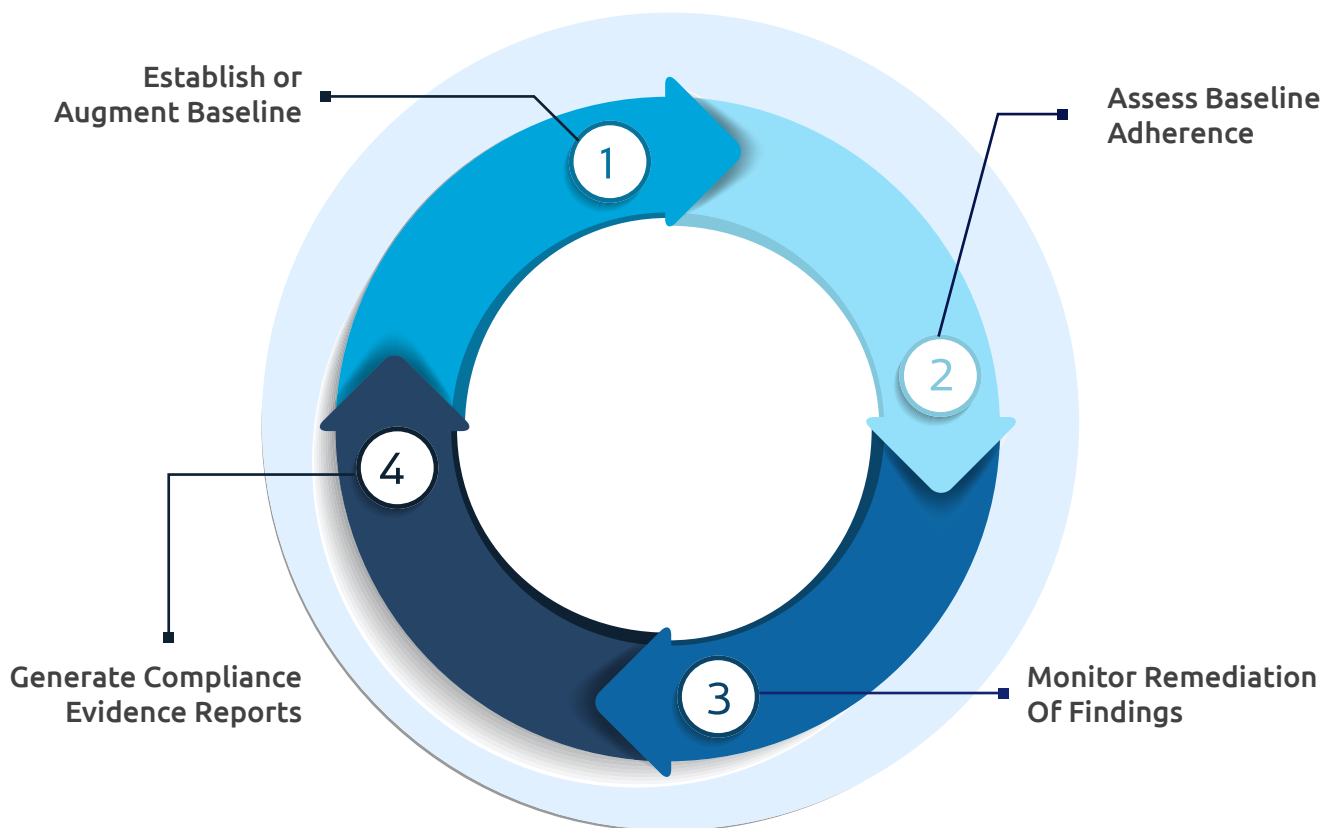


Image 1: Secure Configuration Baseline Process





STEP 1 Establish Or Augment The Baseline

As a starting point, you need to define the first version of the secure configuration baseline for each of its storage and backup solutions. This requires assembling a team of Storage Security SMEs for Block storage, NAS, Object, HCI and Backup. This team would need to work in two vectors:

- A.** Engage with your InfoSec department to learn about goals, policies and required controls for core IT infrastructure – and specifically for Storage and Backup systems.
- B.** Study Storage and Backup security. Understand the principles of securing the various storage technologies, review the vendor’s security configuration and hardening guides for the particular storage and backup system you use, review guidelines outlined in industry standards for information systems and specifically for Storage and Backup.

Now your team can start writing a Secure Configuration Baseline for each Storage and Backup solution used by your organization. This includes the technical implementation guide.

This set of documents needs to be updated periodically to deal with changes to infoSec policies and controls, and to adapt to new vendor hardening instructions, security capabilities or limitations in latest storage/backup product versions, new industry guidelines, etc.

STEP 2 Assess Baseline Adherence

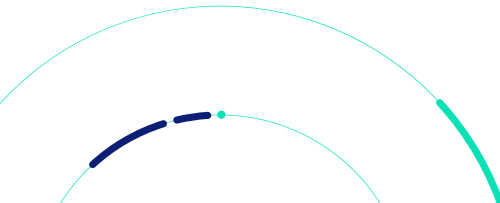
This step involves collecting up-to-date configurations & analyzing adherence to the baseline defined in step 1.

This can be done manually by an engineer, system by system. However, this isn’t very scalable, is very time-consuming and error-prone.

Another option is to automate the process – either by developing and maintaining in-house scripts, or by adopting a suitable commercial solution such as StorageGuard.

The configuration collection should be able to gather the security configuration of each of your storage and backup solutions, work for the different models and versions you use, and continue to work seamlessly as you deploy newer versions.

The analysis of baseline adherence should produce detailed, actionable baseline violation findings, including remediation guidelines, evidence from the scanned systems, detection timestamps, severity, affected systems, etc.



Data Domain ddsrsc: Secure NTP is disabled
 #1782 Opened: May-23-24 Verified on: Sep-29-24 Scan information: May-23-24 (Successfully scanned)

Medium	Error	Medium	Open	Authentication
Urgency	Severity	Ease of implementation	Status	Impact

Description

Data Domain Fortune 500 BL NIST SP800-53r5 Control IA-3 NIST SP800-53r5 Control IA-3(1) NIST SP800-53r5 Control IA-5 +3

The secure NTP option is disabled on the system. This option enables the system to authenticate an NTP server with a key or a certificate.

Secure NTP status

- Disabled

Impact

Neglecting to enable the secure Network Time Protocol (NTP) option exposes the system to significant security risks, including heightened vulnerability to inaccuracies in time synchronization. This can disrupt critical organizational processes such as backup schedules and data transfers, which rely on precise timekeeping. Furthermore, a compromised NTP server is susceptible to time spoofing attacks, where malicious actors manipulate NTP packet timestamps, potentially compromising data immutability by altering the sequence of events and undermining the integrity of records. Thus, enabling secure NTP is essential to mitigate these risks and uphold data integrity.

Image 2: StorageGuard Finding Example and Functionality



Ideally the finding lifecycle should be managed in such a way that a subsequent scan would close a previously detected baseline violation finding if it has been remediated.



In addition, for an effective process you should assign findings to an IT engineer for remediation with a due date and suppress certain findings with the ability to document the exception. Integrations with existing IT Service Management (ITSM) tools, like ServiceNow or Vulnerability Aggregators, like Kenna are recommended.



Overall, this step should ideally be repeatable and executed daily, weekly or monthly based on your risk flavor.

Integration for the nation

Integrates with your existing GRC and ITSM tools from ServiceNow, IBM and others, to automatically open tickets inside your service desk.

STEP 3

Monitor Remediation of Findings

Following the scan and analysis, findings are prioritized and assigned for remediation.

The inclusion of remedial steps (including commands) within each finding helps to accelerate the resolution of baseline violations. During this step, the ability to re-scan and determine if a finding has in fact been remediated is critical. If you're collecting statistics on open and resolved findings, it will allow your team leads and managers to track resolution progress and ensure the return the baseline adherence.

Resolution

The following command/script can be used to remediate the issue:

```
ntp secure add authentication-key {param1} SHA1
ntp secure add timeserver {param2} {param1}
ntp secure add trusted-key {param1}
ntp secure enable
ntp secure sync
# param1 Key-ID
# param2 Time server IP/FQDN
```

Image 3: StorageGuard Finding Remediation

STEP 4

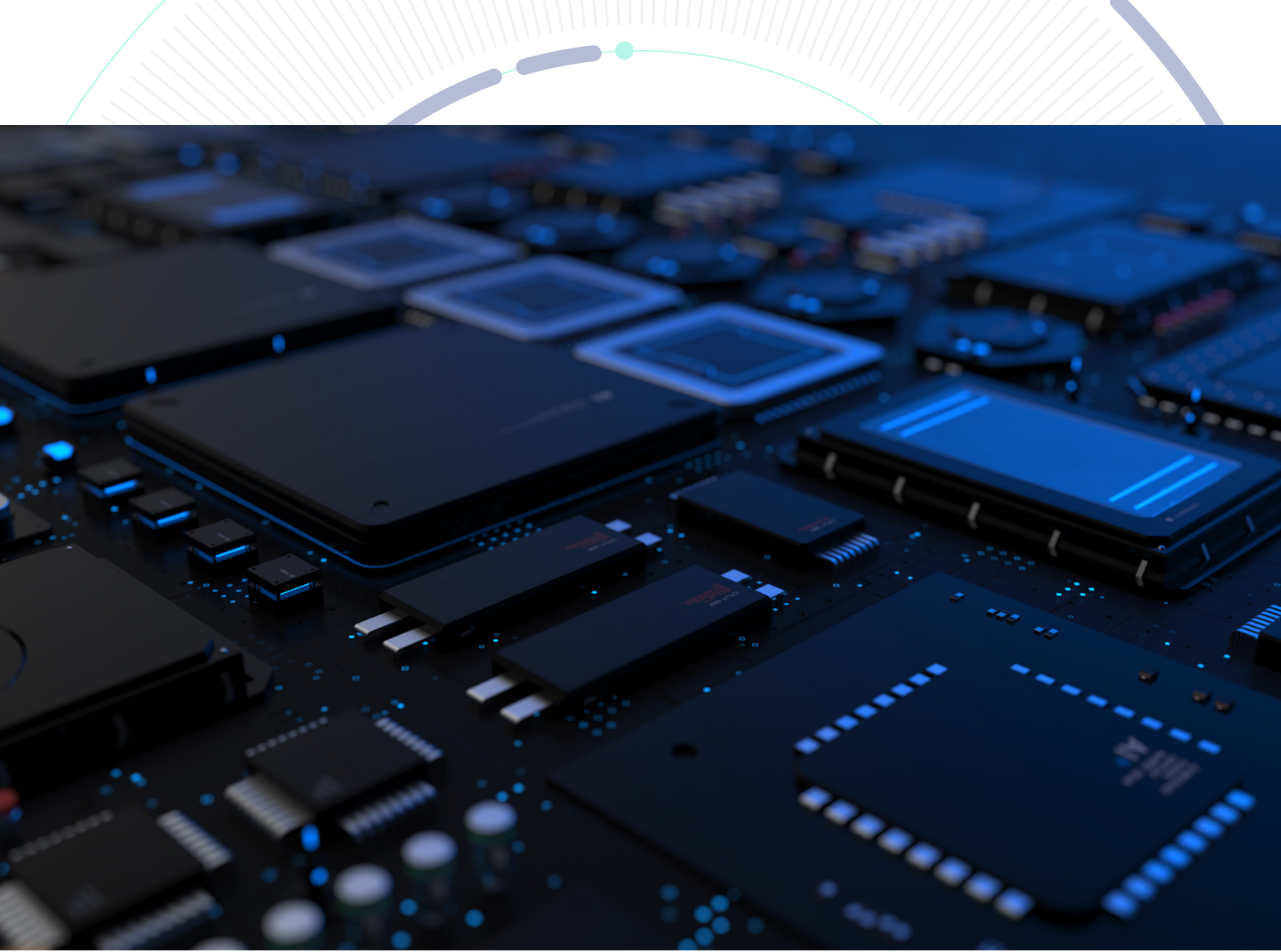
Generate Compliance Evidence Reports

Finally, you'd like to be able to produce baseline compliance reports. These reports include information about successfully passed and failed security principles, baseline checks.

For Infrastructure & Storage Managers, this should include statistics on open and resolved issues, trending, status by vendor, product and technology.

DETAILED ANALYSIS		
The following table presents the types of risks checked during the scan, and the status of the check		
Category	Principle	Data Domain ddbck6
Access Control	Disable unused interfaces	PASS
Access Control	Disable unused interfaces	PASS
Access Control	Idle sessions are terminated	FAIL
Access Control	Limit remote access to manufacturer	PASS
Access Control	System use notification is presented	PASS
Access Control	Vendor-supplied default passwords are not used	PASS
Access Control	Vendor-supplied default passwords are not used	PASS
Audit	Authorized (secure) time source servers are used	PASS
Audit	Authorized (secure) time source servers are used	FAIL
Audit	External (central) log servers are configured	PASS

Image 4: StorageGuard Pass/Fail Report



For Engineers and InfoSec teams, this should include detailed check result information including outputs as evidence for compliance or non-compliance.

Principle name	P	F	Insu...	Labels
Dual authorization	2	0	0	NIST NIST SP800-172A NIST SP800-53 NIST SP800-53 AC-3 NIST SP800-53
In-flight data (client-server) is encrypted	0	2	0	NIST NIST SP800-53 NIST SP800-53 SC-8 NIST SP800-53v4 SC-8
Guest/Anonymous user access is limited	0	2	0	CIS Windows Server Benchmark
System use notification is presented	2	0	0	CIS RHEL Cisco Security Baseline NIST NIST SP800-209 AC-55-R23 NIST SP
Storage / Backup monitoring	2	0	0	CIS Control CIS Control 4.1 NIST NIST SP800-171 NIST SP800-53 NIST SP
Backup/Storage monitoring	0	0	2	CIS Control CIS Control 4.1 NIST NIST SP800-171 NIST SP800-171 3.5.8 N

Image 5: StorageGuard Compliance Report

So, what needs to be included in a secure Configuration baseline? The baseline defined in step 1 may include the following elements - and of course many other security control implementations:

<p>General</p>	<ul style="list-style-type: none"> ◆ MFA ◆ Min Password Length ◆ Account Lockout ◆ Authorized Certificates 	<ul style="list-style-type: none"> ◆ Terminate Idle sessions ◆ Change Default Passwords ◆ Encrypted communications
<p>Technology-specific (NAS, FC, Object, ...)</p>	<ul style="list-style-type: none"> ◆ NFS share ACL ◆ NFS root squash ◆ SMB version ◆ Default SAN Zone 	<ul style="list-style-type: none"> ◆ NFS root squash ◆ Bucket Delete MFA ◆ Bucket versioning
<p>Product-Specific (Dell, NetApp, Pure, Veritas, Rubrik, ...)</p>	<ul style="list-style-type: none"> ◆ DD Dual authorization ◆ Dell CR Cyber Sense 	<ul style="list-style-type: none"> ◆ Pure SafeMode ◆ ONTAP dynamic authorization
<p>Role-Specific (Primary Storage, Backup Storage)</p>	<ul style="list-style-type: none"> ◆ Separate credentials ◆ Retention Lock settings 	<ul style="list-style-type: none"> ◆ Off-site copy

Active	Custom labels	Principle	Check name	System type	Labels
✓	MyBaseline	Remove/Disable Default Accounts	SG-C0309T061V01: IPMI root user status	Data Domain / PowerProtect DD	CIS Control v8.8 CIS
✓	MyBaseline	Maximum Password Lifetime is Restricted	SG-C0234T061V01: Maximum password age	Data Domain / PowerProtect DD	#StopRansomware CIS
✓	MyBaseline	Password Policy - Minimum Password Length is Enforced	SG-C0264T061V01: Minimum password length	Data Domain / PowerProtect DD	#StopRansomware CIS
✓	MyBaseline	Storage and Backup Monitoring - Email Server is Configured	SG-C0395T061V01: SMTP server configuration	Data Domain / PowerProtect DD	Fortune 500 BL GLOB
✓	MyBaseline	Storage and Backup Monitoring - Enable Secure Remote Support and Call Home	SG-C0397T061V01: Remote support configuration	Data Domain / PowerProtect DD	Fortune 500 BL GLOB
✓	MyBaseline	Deprecated SMB Versions are Disabled	SG-C0122T061V01: CIFS SMB version enabled	Data Domain / PowerProtect DD	#StopRansomware CIS
✓	MyBaseline	Audit Logging Enabled	SG-C0001T061V01: Audit logging status	Data Domain / PowerProtect DD	CIS Control v8.8 CIS
✓	MyBaseline	Trusted Certificate Issuer	SG-C0447T061V01: Self-signed certificate	Data Domain / PowerProtect DD	#StopRansomware CIS
✓	MyBaseline	Strong Password Hashing Algorithm is Used	SG-C0417T061V01: Password hash strength	Data Domain / PowerProtect DD	CIS BH&L Benchmark 5
✓	MyBaseline	Idle Session Termination	SG-C0209T061V01: Idle session timeout	Data Domain / PowerProtect DD	CIS Control v7.16 CIS
✓	MyBaseline	Set Account Lockout Threshold	SG-C0393T061V01: Account lockout threshold	Data Domain / PowerProtect DD	#StopRansomware CIS

Image 6: StorageGuard Ready-Made Baseline Snippet

One approach to establishing a secure configuration baseline for Storage and Backup platforms is **Gradual Hardening**.

It can be rather overwhelming to attempt to implement all security controls at once. Thus, we recommend doing it in multiple phases, each time taking on a group of additional security guidelines to further protect storage and backup systems.

For example, as an initial step you may want to change default passwords, disable telnet & check RBAC.

In more advanced phases, consider looking into encrypted communications & backup immutability.

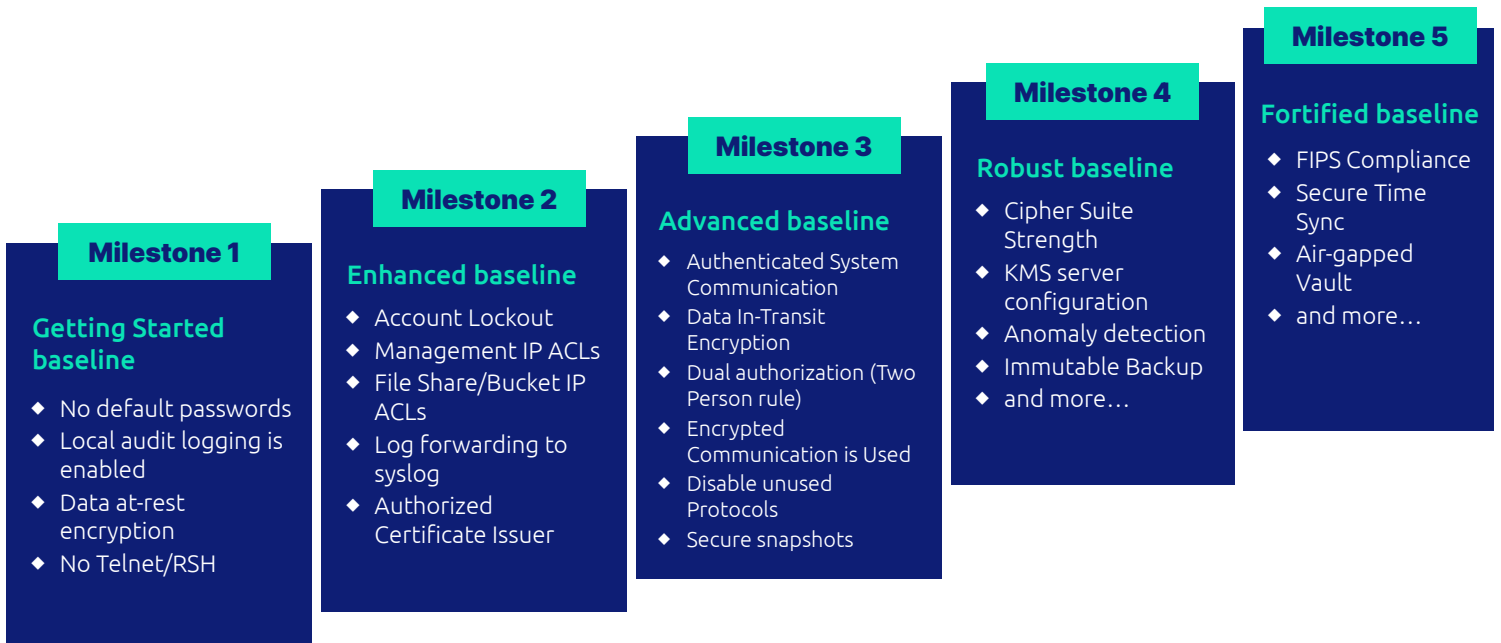


Image 7: StorageGuard built-in gradual hardening baselines

Implementing a secure configuration baseline for storage and backup systems is not a one-time task but a continuous process that evolves with emerging threats, changing IT landscapes, and organizational priorities.

By following the four steps outlined in this guide – establishing the baseline, assessing adherence, monitoring remediation, and generating compliance evidence – you’ll create a repeatable framework that ensures the resilience of critical infrastructure.

Leveraging automation tools and gradual hardening strategies can simplify this journey, making it manageable and scalable over time.

The ultimate goal is to embed security and compliance into the DNA of your IT operations, protecting your organization’s most valuable data assets, while enabling operational continuity and trust.