CONTINUITY

Summary of Risk Types

The following table lists the types of risks detected by StorageGuard:

System Type	Check ID	Check Name	Security Principle	Category	Impact Level	Ease of Implementation
NetApp cluster	K0502I0MP908	Ransomware protection Policy	Malware scanning is enabled	Malware Protection	1-High	2-Medium
Infinidat Infinibox	Infinidat vulnerability	INFINIBOX-45631 (CVE-2021-44228)	Vulnerability identification for Infinidat	Vulnerabilities (CVE)	1-High	2-Medium
Pure Storage FlashArray	K022E000P160	Default administrative passwords	Vendor-supplied default passwords are not used	Access Control	1-High	1-High (Easy)
Brocade SAN Switch	K0719I0M0800	SAN Fabric - zone member identification	Secure SAN (FC) zoning	Access Control	2-Medium	2-Medium
Dell EMC PowerProtect DD (Data Domain)	K080CI00P183	Protected recovery copies	Immutable data copies	Malware Protection	1-High	3-Low (Difficult)
Dell EMC PowerScale (Isilon)	K140D00MP345	File share client access list	Access rights granted to authorized users/hosts only	Authorization	1-High	1-High (Easy)
NetApp cluster	K2102I000965	Snapshot autodelete configuration	Immutable data copies	Malware Protection	2-Medium	2-Medium
Dell EMC PowerProtect DD (Data Domain)	K020CI0MP298	IPFilter configuration	Management access is restricted	Access Control	1-High	1-High (Easy)
Hitachi Virtual Storage Platform (VSP)	K0110I0MP0734	Command Device (CLI) Authentication	Strong storage management host identification	Access Control	1-High	2-Medium
IBM V7000/SVC	IBM vulnerability	IBM V7000/SVC vulnerability: 872456	Vulnerability identification for IBM	Vulnerabilities (CVE)	1-High	2-Medium
Dell EMC Unity	K030CIVM0365	CIFS SMBv1 status	Unsecure SMB versions are disabled	Services and Protocols	1-High	1-High (Easy)
NetApp cluster	K022A00M0250	Two-factor authentication configuration	Multifactor authentication is used	Services and Protocols	1-High	2-Medium
IBM FlashSystem	K0513I0MP600	NTP configuration	Synchronization with authoritative time source is enabled	Audit	1-High	1-High (Easy)
Hitachi Content Platform (HCP)	K011CI0MP344	Idle session timeout	Idle sessions are terminated	Access Control	2-Medium	1-High (Easy)

System Type	Check ID	Check Name	Security Principle	Category	Impact Level	Ease of Implementation
Cohesity DataPlatform	K132BI0MP983	Hardening status	Hardening (STIG)	Information Security	2-Medium	2-Medium
Dell EMC Elastic Cloud Storage (ECS)	K0228I0MP120	Non-default (unapproved) local user accounts	Local user accounts should not be used	Access Control	2-Medium	1-High (Easy)
Brocade	K070400M0907	Firmware integrity check	Approved OS release	Configuration Management	1-High	1-High (Easy)
NetApp cluster	K0502I0MP909	Anti-ransomware status	Antivirus scanning is enabled	Malware Protection	1-High	2-Medium
…						
…						
… (and more)						