COMPLIANCE MADE EASY

ARMOR ANYWHERE - COMPLIANCE MATRIX

The Armor Compliance Matrix is intended to help IT, IT security, and compliance teams understand how Armor accelerates adherence to major compliance mandates to which their organizations are subject.

Armor Security Services	PCI DSS 3.2.1 Controls	HIPAA/HITECH Controls	HITRUST CSF v9.3 (66 Controls Required for Certification)	GDPR	DFS 500 (23 NYCRR 500)	Risk Mitigation
NETWORK CONTROLS						
Intrusion Detection and Prevention	11.4	Security best practice - implied control under §164.306(a)	09.m[HT1]	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Malicious allowed traffic
Internal Network Vulnerability Scanning[1]	11.2.3	Included in §164.308(a)(1)	10.m	Article 32, Section 1(d)	500.02 (a), (b)(2), (b)(3), 500.05 (b)	Exploits due to missing patches/updates; improper network firewall configuration
SERVER CONTROLS						
File Integrity Monitoring[2]	11.5	§164.312(e)	09.ab, 10.h	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Monitoring unauthorized changes to critical files
Malware Protection	5.1, 5.2, 5.3	§164.308(a)(5)(ii)(B)	09.ab, 10.h	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Compromise due to virus/malware infection
Log Management[3]	10.1, 10.2.2-10.2.7, 10.3, 10.5, 10.6, 10.7	§164.308(a)(1)(ii)(D), §164.308(a)(5)(ii)(C), §164.312(b)	09.aa, 09.ab, 09.ac	Article 32, Section 1(b) and 1(d)	500.02 (3), (4), 500.06 (a) (2) - see special note	Detection of malicious activity (security incidents)
Operating System (OS) Patching[4]	6.1, 6.2	Security best practice - implied control under §164.306(a)	10.m	Article 32, Section 1(b)	500.02 (a)	OS and COTS software weaknesses
END USER CONTROLS						
Endpoint Detection and Response[4]	5.1, 5.2, 5.3, 10.6, 10.8	§164.308(a)(1)(ii)(D) §164.308(a)(5)(ii)(B) §164.312(b)	Endpoint Protection Domain Vulnerability Management Domain Audit Logging Monitoring Domain	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Antivirus protection and detection of malicious activity on user endpoints
ADMINISTRATIVE CONTROLS						
Incident Response[5]	12.10	§164.308(a)(6)	05.b, 11.a, 11.c	Article 32, Section 1(b)	500.16 - see special note, 500.10 (a), (b), 500.17	Response to security incidents
Multi-factor Authentication for AMP Access[6]	N/A	N/A	N/A	N/A	500.12 (b)	Unauthorized remote use of administrative access
Business Associate Contract	N/A	§164.308(b)(1)	05.k, 09.e[HT1]	N/A	N/A	Legal liability for data loss/ breach
Access Control[7]	7.1.1, 7.1.2	§164.312(a)(1)(12)	01.a	Article 32, Section 1(b)	500.07	Unauthorized access
Security Audits[8]	Security best practice	§164.308(a)(8)	06.g	Article 32, Section 1(d)	500.02 (b)(1), 500.11 - see special note	Validation of security controls program

COMPLIANCE MADE EASY

1. The service collects basic asset identification information, Windows registry information (for Windows systems only) and file version and package information periodically throughout each day and reports the results to the scan platform that assesses the data and determines the vulnerabilities that exist.

   Armor posts vulnerability information in Armor Management Portal (AMP) weekly that represents the state of the instance as of the last report.

   Note: Armor does not provide any patches or updates.

2. This control is only applicable to OS files for the servers protected by Armor Anywhere. Customization to cover customer-specific files is available at an additional cost.

3. Armor provides automated log reviews and reports exceptions to the customer for further review. The reviews are limited to operating system logs for customer virtual servers, malware protection, file integrity monitoring, intrusion detection services, and endpoint detection and response. Collection and review of customer application and other logs are the responsibility of the customer. Application logs as well as the device and cloud-specific logs can be collected and analyzed at an additional cost. Default retention for all logs is 30 days with an option for 13-month retention available at an additional cost.

   Special note for DFS 500: Customers are required to retain logs for three years and will therefore need to export their logs from AMP to meet this requirement.

4. Armor provides a report highlighting any missing critical/security patches against the vendor-supplied OS and other commercial-off-the-shelf software (COTS) installed on the server. Customer is responsible for the installation of all patches for both the OS and all applications they install.

5. Customers should document and maintain their own incident response policies. Armor's services assist in the detection, communication, and mitigation of security breaches.

   Special note for DFS 500: Armor's security operations center (SOC) fulfills these requirements for the services provided and for our incident response service.

6. Coverage for this control is limited to access to the AMP.

7. Relates to the provisioning and use of the Armor administrative account included with each secure server.

8. Applies to Armor's third-party attestations that include PCI DSS validation, HITRUST certification, ISO 27001:2013 certification, and SOC 2 Type II reports.

   Special note for DFS 500: Armor's third-party audit attestations assist covered entities (CEs) with their third-party vendor management requirements.

HT1. There are 19 domains that cover 135 system controls with 700+ potential requirements depending on your individual scope for HITRUST.