COMPLIANCE MADE EASY

ARMOR ANYWHERE IN ARMOR'S PRIVATE CLOUD

Explore how Armor Anywhere in Armor's private cloud aligns with various compliance requirements and regulations.

Armor Cloud Security	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
PERIMETER CONTROLS						
IP Reputation Filtering	Security best practice	§164.308(a)(1)(ii)(a)	09.m	Article 32, Section 1(b)	500.02 (a), (b)(2)	Activity from known bad sources
DDoS Mitigation	Security best practice	Security best practice – implied control under §164.306(a)	09.m, 09.h[HT1]	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Loss of availability due to high volume of malicious activity
APPLICATION CONTROLS						
Web Application Firewall[1]	6.6	Security best practice – implied control under §164.306(a)	10.b[HT2]	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Application layer flaws and exploits
NETWORK CONTROLS						
Intrusion Detection/ Intrusion Prevention	11.4	Security best practice – implied control under §164.306(a)	09.m	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Malicious allowed traffic
Network Firewall[2] **(Hypervisor-based)**	1.1.5, 1.1.6, 1.1.7, 1.2.2, 1.2.3(2), 1.3.3, 1.3.5	Security best practice – implied control under §164.306(a)	01.m, 01.o, 01.w, 09.m	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Unwanted network connectivity
* **Internal Network Vulnerability Scanning**[3]	11.2.3	Included in §164.308(a)	10.m	Article 32, Section 1(d)	500.02 (a), (b)(2), (b)(3), 500.05 (b)	Exploits due to missing patches and updates; improper network firewall configuration
* **External Network Vulnerability Scanning**[3]	11.2.2	Security best practice – implied control under §164.306(a)	10.m	Article 32, Section 1(d)	500.02 (a), (b)(2), (b)(3), 500.05 (b)	Exploits due to missing patches and updates; improper network firewall configuration
Secure Remote Access (Two-factor authentication)[4]	8.3	§164.312(d), §164.312(a)(2)(iii)	01.j, 05.i, 09.s	Article 32, Section 1(b)	500.07, 500.12 (b)	Unauthorized use of administrative access
* **Encryption in Transit (SSL certificates resold by Armor only)**	4.1.c, 4.1.d	§164.312(e)(1)	09.m, 09.s	Article 32, Section 1(a)	500.02 (a), (b)(2), 500.15	Interception of sensitive data in transit

* Denotes optional services available for purchase from Armor.

COMPLIANCE MADE EASY

Armor Cloud Security	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
SERVER CONTROLS						
Hardened Operating System (OS)[5]	2.1.a, 2.1.b, 2.1.c, 2.2.a, 2.2.b, 2.2.c, 2.2.d	Security best practice – implied control under §164.306(a)	10.m	Article 32, Section 1(b)	500.02 (a)	OS configuration errors
File Integrity Monitoring[6]	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
Secure Remote Administrative Access[7]	2.3	§164.312(d)	01.j, 05.i, 09.m, 09.s	Article 32, Section 1(b)	500.07	Disclosure of administrative credentials
OS Patching[8]	6.1, 6.2	Security best practice – implied control under §164.306(a)	10.m	Article 32, Section 1(b)	500.02 (a), (b)(2)	OS weaknesses
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 or malware infection
Log and Data Management[9]	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)
* **Data at Rest Encryption**[10]	3.4	§164.312(d), §164.312(a)(2)(iii)	06.d, 10.g	Article 32, Section 1(a)	500.02 (a), (b)(2), 500.15	Unauthorized disclosure of sensitive information
Time Synchronization	10.4	Security best practice – implied control under §164.306(a)	09.af	Article 32, Section 1(b) and 1(d)	500.02 (a), 500.06 (a)(2)	Facilitates log and forensic analysis
Capacity Management[11]	Security best practice	Security best practice - implied control under §164.306(a)	09.h	Article 32, Section 1(b)	500.02 (a)	Ensures resource availability
END USER CONTROLS						
Endpoint Detection and Response[9]	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
PHYSICAL CONTROLS						
Rogue Wireless Scanning[12]	11.1	Security best practice – implied control under §164.306(a)	01.m, 09.m	Article 32, Section 1(b)	500.02 (a)(i), (b)(2)	Unauthorized network access
Physical Security	9.1, 9.2, 9.3, 9.4	§164.310(a)(2)(i), §164.310(a)(2)(ii), §164.310(a)(2)(iii), §164.310(a)(2)(iv)	08.b, 08.d, 08.j, 09.ab, 09.q	Article 32, Section 1(b)	500.02 (a)(ii)	Physical theft or compromise of data
Secure Data Deletion[13]	9.8.2	§164.310(d)(1), §164.310(d)(2)(i), §164.310(d)(2)(ii)	07.a, 08.l, 09.p	Security best practice	Security best practice	Data recovery from discarded systems

* Denotes optional services available for purchase from Armor.

COMPLIANCE MADE EASY

Armor Cloud Security	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
ADMINISTRATIVE CONTROLS						
Change Control[14]	6.4.5	Security best practice – implied control under §164.306(a)	09.g(10)	Security best practice	Security best practice	Unauthorized system changes
Formal Risk Assessment[15]	12.2	§164.308(a)(1)	03.a, 03.b, 03.c	Article 32, Section 1	500.02 (b)(1), 500.09	Identification of risks and threats
Incident Response[16]	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
* **Advanced Backup**	Security best practice	§164.308(a)(7)(ii)(A), §164.310(d)(1), §164.310(d)(2)(iv)	12.c	Article 32, Section 1(b) and 1(c)	500.02 (a), (b)(5)	Loss or corruption of data
* **Continuous Server Replication (DR)**	Security best practice	N/A	N/A	Article 32, Section 1(b) and 1(c)	500.02 (a), (b)(5)	Loss or corruption of data
Business Associate Contract	N/A	§164.308(b)(1)	05.k, 09.e	N/A	N/A	Legal liability for data loss/breach
Maintain Maintenance Records[17]	Security best practice	§164.310(a)(2)(iv)	08.j[HT2]	Security best practice	Security best practice	System failure
Access Control[18]	7.1.1, 7.1.2	§164.312(a)(1)(12)	01.a	Article 32, Section 1(b)	500.07	Unauthorized access
Security Audits[19]	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

* Denotes optional services available for purchase from Armor.

COMPLIANCE MADE EASY

1. Customers are responsible for ensuring that the applications they deploy on the Armor-provided servers have been developed in accordance with industry-standard best practices and are maintained and updated to sustain a secure posture.

2. For the 1.1.x and 1.3.x controls, other than definition and maintenance of the default global policy, customers are fully responsible for defining the rule set for each firewall instance.

3. Optional service provided via Navis, a third-party PCI-Approved Scanning Vendor (ASV). Armor provisions all customer IP addresses and the customer is responsible for scheduling their own internal and external scans.

4. Coverage for this control is limited to the default SSL VPN access provided by Armor for remote access to the customer environment, which allows customers to manage their virtual servers.

5. Armor supplies a pre-hardened OS (based on CIS benchmarks). The customer is responsible for all additional OS configuration after initial implementation and for maintaining the configuration in compliance with these controls.

6. This control is only applicable to OS files for the servers provided with Armor Complete. Customization to cover customer-specific files is available at an additional cost.

7. Coverage for this control covers OS layer access Secure Shell (SSH) and Remote Desktop Protocol (RDP) via the default SSL VPN access method provided by Armor.

8. Patching is a shared control. Armor is responsible for providing critical and security patches provided by the OS vendors only subject to the service description for this service. The customer is responsible for patching all other software/applications they install.

9. Armor provides automated log reviews and reports exceptions to the customer for further review. The reviews are limited to OS 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 other 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 the Armor Management Portal to meet this requirement.

10. This is an optional service that utilizes a solution from a third party, Vormetric. Armor provides the data security manager (DSM) appliance and sets up the initial customer administrative account. Armor also installs the required agents on the target servers and provides updates to both the DSM and agents. The customer has full control over defining their encryption policies and the creation and management of their encryption keys. Armor has no access to the DSM application, encryption policies, or encryption keys.

11. Armor monitors the resource capacity of all underlying infrastructure components and ensures adequate resources are available to support all customers. Armor also monitors CPU, RAM, and disk resources for all customer servers and this information is reported via the customer portal.

Armor also monitors Ping, SSH, RDP, and HTTP connectivity to all customer servers.

12. Armor does not maintain any in-scope or connected wireless networks within any of its cloud hosting locations.

13. Relates to the secure deletion of information from the Armor infrastructure upon decommissioning of customer's server(s).

14. Change control applies to OS patching process.

15. Applies to the underlying infrastructure up through the OS layer of the virtual servers and includes the security controls provided by Armor. Customers are responsible for conducting their own risk assessments for their entire solution that includes all customer-controlled systems outside of those deployed at Armor.

16. 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.

17. Applies only to the underlying Armor infrastructure and data center maintenance records.

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

19. 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. DDoS mitigation is included in Level 2 implementation of this control objective.

HT2. There are 19 domains that cover 135 system controls with 700+ potential requirements depending on individual scope for HITRUST.