ARMOR

THE FIRST TOTALLY SECURE CLOUD COMPANY™

Armor Complete - Secure Hosting

ACHIEVING COMPLIANCE THROUGH SECURITY

Explore how Armor Complete security solutions and services align with various compliance requirements and regulations.

Armor Security Services	PCI DSS 3.2 Controls	HIPAA/HITECH Controls	HITRUST CSF v8 66 Controls Required for Certification	Risk Mitigation
PERIMETER LAYER				
IP Reputation Filtering	Security best practice	§164.308(a)(1)(ii)(A)	09.m[HT1]	Activity from known bad sources
DDoS Mitigation	Security best practice	Security best practice - implied control under 164.306(A)	09.m[HT1], 09.h[HT2] (included in Level 2 implementation)	Loss of availability due to high volume of malicious activity
APPLICATION LAYER				
Web Application Firewall	6.6[1]	Security best practice - implied control under 164.306(A)	09.m[HT1]	Application layer flaws and exploits
NETWORK LAYER				
Intrusion Detection	11.4	Security best practice - implied control under 164.306(A)	09.m[HT1]	Malicious allowed traffic
Network Firewall [3] (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[HT1]	Unwanted network connectivity
Internal Network Vulnerability Scanning	11.2.3	Included in §164.308(a)[1]	10.m	Exploits due to missing patches and updates; improper network firewall configuration
External Network Vulnerability Scanning[4]	11.2.2	Security best practice - implied control under 164.306(A)	10.m	Exploits due to missing patches and updates; improper network firewall configuration
Secure Remote Access (Two-factor authentication)	8.3	§164.312(d), §164.312(a)(2)(iii)	01.j, 05.i[HT3], 09.s[HT3]	Unauthorized remote use of administrative access
Encryption in Transit (Armor SSL certificates only)	4.1.c, 4.1.d	§164.312(e)(1)	09.m[HT1], 09.s[HT3]	Interception of sensitive data in transit

Armor Security Services	PCI DSS 3.2 Controls	HIPAA/HITECH Controls	HITRUST CSF v8 66 Controls Required for Certification	Risk Mitigation
SERVER LAYER				
Hardened Operating System (OS)	2.1.a, 2.1.b, 2.1.c, 2.2.a, 2.2.b, 2.2.c, 2.2.d [5]	Security best practice - implied control under 164.306(A)	10.m[HT4]	Configuration errors
File Integrity Monitoring	11.5[6]	§164.312(e)	09.ab[HT5], 10.h	Monitoring unauthorized changes to critical files
Secure Remote Administrative Access	2.3	§164.312(d)	01.j, 05.i[HT1], 09.m[HT1], 09.s[HT1]	Disclosure of administrative credentials
OS Patching/Updating	6.1, 6.2[7]	Security best practice - implied control under 164.306(A)	10.m[HT4]	OS weaknesses Malware Protection
Malware Protection	5.1, 5.2, 5.3	§164.308(a)(5)(ii)(B)	09.ab[HT5], 10.h	Compromise due to virus or malware infection
Log Management[8]	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[8], 09.ab[HT5], 09.ac[8]	Detection of malicious activity
Data At Rest Encryption[9]	3.4	§164.312(d), §164.312(a)(2)(iii)	06.d[HT1], 10.g	Unauthorized disclosure of sensitive information
Time Synchronization	10.4	Security best practice - implied control under 164.306(A)	09.af	Facilitates log and forensic analysis
Capacity Management	Security best practice	Security best practice - implied control under 164.306(A)	09.h[HT6]	Ensures resource availability
PHYSICAL LAYER				
Rogue Wireless Scanning	11.1[2]	Security best practice - implied control under 164.306(A)	01.m[HT1], 09.m[HT1]	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[HT4], 09.q[HT1]	Physical theft or compromise of data
Secure Data Deletion[15]	9.8.2	§164.310(d)(1), §164.310(d)(2)(ii), §164.310(d)(2)(ii)	07.a[HT1], 08.l[15] 09.p[15]	Data recovery from discarded systems

Armor Security Services	PCI DSS 3.2 Controls	HIPAA/HITECH Controls	HITRUST CSF v8 66 Controls Required for Certification	Risk Mitigation
ADMINISTRATIVE CONTROLS				
Change Control	6.4.5[10]	Security best practice - implied control under 164.306(A)	09.g(10)	Unauthorized network access
Formal Risk Assessment[11]	12.2	§164.308(a)(1)	03.a, 03.b, 03.c	Identification of risks and threats
Incident Response [12]	12.10	§164.308(a)(6)	05.b, 11.a, 11.c	Response to security incidents
Array Snapshots	Security best practice	§164.308(a)(7)(ii)(A)[13], §164.310(d)(1), §164.310(d)(2)(iv)	12.c[13]	Loss or corruption of data
Business Associate Contract	N/A	§164.308(b)(1)	05.k[HT1], 09.e[HT1]	Legal liability for data loss/breach
Maintain Maintenance Records	Security best practice	§164.310(a)(2)(iv)	08.j[HT7]	System failure
Access Control[14]	7.1.1, 7.1.2	§164.312(a)(1)(12)	01.a	Unauthorized access
Security Audits	Security best practice	§164.308(a)(8)	06.g[HT8]	Validation of controls program

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 maintain a secure posture.
2. Armor does not maintain any in-scope or connected wireless networks within any of its cloud hosting locations.
3. 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.
4. 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 scans.
5. While Armor supplies the original OS in a hardened configuration, 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 and is validated for the Gen4 platform and was included in the Gen3 platform after its May, 2016 validation.
7. These are shared controls - Armor is responsible for OS patches supplied by Armor only. Customer is responsible for patching all other software/applications they install.
8. 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, and the malware protection, file integrity monitoring and intrusion detection services. All review of application layer logs are the responsibility of the customer.
9. This is an optional service that utilizes a solution from a third party - Vormetric. Armor provides the DSM (data security manager) 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.
10. Change control applies to OS-patching process and implementation of firewall rule change requests from customers.
11. Applies to the underlying infrastructure up through the OS layer of the virtual servers. 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.
12. Applies to incidents discovered or reported by Armor security services related to the underlying infrastructure only. If a customer requests assistance with a breach they discovered, Armor may provide assistance to the extent it is able.
13. Array snapshots provided consists of daily volume-level snapshots that are each kept for fourteen (14) days. These snap[shots are not file based data backups and customer remain responsible for all data backup.
14. Relates to the provisioning and use of the Armor administrative account included with each secure server.
15. Relates to the secure deletion of information from the Armor infrastructure upon decommissioning of customer's server(s).

HT1. These controls assist in meeting the control objective.

HT2. DDoS mitigation is included in Level 2 implementation of this control objective.

HT3. These controls assist in meeting the control objective.

HT4. These controls are included in Level 2 implementation of this control objective.

HT5. These controls are included in Level 3 implementation of this control objective.

HT6. 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, 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.

HT7. Applies only to the underlying Armor infrastructure and data center maintenance records.

HT8. Applies to Armor's third party attestations that include PCI DSS validation, HITRUST certification, ISO 27001:2013 certification and SSAE 16 SOC 1 and SOC 2 Type II reports.