ARMOR® SERVICE DESCRIPTIONS

SUMMARY

These Service Descriptions describe and define each of the service components for the Armor Anywhere™ and Armor Anywhere™ with secure hosting Services (the "Services"). Each Service Definition describes the services and defines the roles and responsibilities of Armor and you ("Customer"). Due to the modular nature of the Services, Armor may update or replace the service(s), or any component thereof, in whole or in part, as required to deliver the Services. Armor reserves the right to modify the Services, in whole or in part, at any time and without notice to you; provided, Armor does not materially decrease the overall security of the Services. Further, Armor reserves the right to combine or separate for purchase the Services defined herein and to change the combination of the Services at any time and without notice to you.

SCOPE OF SERVICES FOR THE ARMOR ANYWHERE™ WITH SECURE HOSTING SERVICES

The Armor Anywhere™ with secure hosting Services provides managed security services at the operating system (OS) level, including the application of critical security patches which require Customer reboot as identified in the Armor Management Portal (AMP). Customer will remain responsible for Customer applications and any associated data, and logical access control to the OS. Armor is responsible for the operation of the individual service components of the Armor Anywhere™ with secure hosting Services identified below.

SCOPE OF SERVICES FOR THE ARMOR ANYWHERE™ SERVICES

The Armor Anywhere™ Services provides managed security services at the operating system (OS) level. Customer will remain responsible for the underlying compute and third-party storage infrastructure, Customer applications and any associated data, and logical access control to the OS and all Customer applications. Armor is responsible for the operation of the individual service components of the Armor Anywhere™ Services identified below.

SERVICE AVAILABILITY

The Armor Anywhere™ with secure hosting Service is supported by all five (5) Armor datacenters located in Chicago (ORD01), Dallas (DFW01), London (LHX01), Frankfurt (FRA01), and Singapore (SIN01) for Armor Anywhere™ with secure hosting customers. A list of Armor Anywhere™ supported operating systems can be found here. The compatibility of an OS to the Services may change from time to time. Both Services are available to Armor Channel Partners.

APPLICABLE SERVICES TABLE

Below is a summary of products and services applicable to the Services:

Services	Anywhere with	Anywhere	Type of
Armor Management Portal	▪	▪	Default
Armor Agent	▪	▪	Default
Secure Virtual Machines and Storage	▪		Default
Operating System (OS) Software	▪		Default
Resource Availability Monitoring Service	▪		Default
IP Reputation Filtering Service	▪		Default
DoS/DDoS Mitigation Service	▪		Default
Core Web Application Firewall (WAF) Service	▪		Default
Virtual Network Firewall Service	▪		Default
SSL VPN (Secure Remote Access) Service	▪		Default
Multi-Factor Authentication (MFA) Service	▪	▪	Default
Malware Protection Service	▪	▪	Default
File Integrity Monitoring (FIM) Service	▪	▪	Default
Log and Data Management Service	▪	▪	Default
Host Intrusion Detection Service (HIDS)		▪	Default
Remote Support Service	▪	▪	Default
Vulnerability Scanning Service	▪	▪	Default
Vulnerability Monitoring (External/Internal Scanning) (Navis) Service	▪		Add-on
Advanced Web Application Firewall (WAF) Service	▪		Add-on
Data at Rest Encryption (Vormetric) Service	▪		Add-on
Disaster Recovery Service (Zerto) Service	▪		Add-on
Advanced Backup Service	▪		Add-on
Load Balancers	▪		Add-on
Colocation Service	▪		Add-on
Custom Policy Configuration Service		▪	Add-on
Cloud Security Posture Management	▪	▪	Add-on Services (Including Add-On Managed Services)
Endpoint Detection and Response	▪	▪	Add-on Services (Including Add-On Managed Services)

Support Services Matrix	▪	▪	Add-on
Managed & Enterprise Implementation Service	▪	▪	Add-on
Security Trends & Insights Report	▪	▪	Add-on

DEFAULT SERVICES

Armor Management Portal

Service Description	The Armor Management Portal (AMP) is a Software as a Service (SaaS) offering that combines Customer's account and instance specific information related to certain components of the Service. Features in AMP include without limitation billing and invoicing, user account management, service management and reporting. Specifics of portal functionality and features can be found in the Armor Knowledge Base. Armor reserves the right to add, remove, or modify features in AMP from time to time and without notice to Customer.
Accessibility	Armor is responsible for the availability of AMP. AMP is provided via the public Internet over encrypted transit channels. Customer's users are sent an invitation to their registered E-mail address which contains information for registering as a user and to activate the AMP account.
Administration	Customer is responsible for the activation and administration of its account in AMP, and for granting its employees, contractors, and agents with access to AMP. Customer will retain full access rights and permissions to its AMP account and is and will remain responsible for adding and removing users, managing user permissions and roles within its AMP account, and for keeping all user information (including billing contact) current and up-to-date.

Armor Agent

Service Description	The installation of the Armor Agent permits the functionality and management of the Services in the Customer's environment.
Installation	Installation of the Armor Agent is a Customer responsibility except in the case where Armor provides the Armor Anywhere™ with secure hosting Services to Customer.
Administration/ Configuration	Armor is responsible for the administration of the Armor Agent and for the configuration of the component parts of the Armor Agent that are installed using the Armor Agent.
Networking	Devices having an installed Armor Agent must be configured to enable Internet access. The configuration of firewall rules and network connectivity is a Customer responsibility except in the case where Armor provides the Armor Anywhere™ with secure hosting Services to Customer. Technical details regarding the connectivity required to use the Armor Agent are available in the Armor Knowledge Base.
Remediation	Customer maintains administrative control and domain over the operating system (OS) in which the Armor Agent is installed, potentially resulting in Customer directly or indirectly damaging or disabling the Armor Agent. In such cases, Armor will provide reasonable assistance to remediate operational issues with the installed Armor Agent.
Note:	At the time the Services are provisioned, Armor creates an account on the OS for each server in which the Armor Agent is installed ("Armor Account"). The Armor Account provides Armor administrative access to the OS and is solely used to provide Customer with the Services by Armor's Security Operations and Support personnel. The credentials for the Armor Account are maintained in confidence within the Armor Privileged Access Management (PAM) system, which provides Customer with auditing and visibility of Armor's access to Customer servers recording all actions taken by Armor during use of the Armor Account. Customer controls the availability of this account and can disable/enable it based on their own access policies. If disabled, Armor's ability to provide support will be disrupted until the account is enabled.

Secure Virtual Machines and Storage

Service Description	A Secure Virtual Machine is an emulated or non-physical computer system that can run an operating system (OS).
Installation	Armor is responsible for provisioning the Secure Virtual Machine and the associated OS's supported by the Armor platform.
Configuration	Armor is responsible for the configuration of the Secure Virtual Machine.
Administration	Armor is responsible for the administration of the Secure Virtual Machine.
Remediation	Armor is responsible for remediating issues for the Secure Virtual Machine.

Operating System (OS) Software

Service Description	Armor provides certain Operating System Software ("OS Software") and associated licenses. These include preconfigured versions of Windows and Linux operating systems (OS) to run on the Armor Secure Virtual Machines. A detailed list of Armor supported OS's are available in the Armor Knowledge Base. OS Software is provided in conjunction with a Secure Virtual Machine and cannot be purchased or used separate or independent of the Secure Virtual Machine.
Installation	Armor is responsible for the installation of the OS Software. Customer is responsible for any additional configuration and/or hardening.
Configuration	Each Secure Virtual Machine is provisioned by Armor with two local administrative accounts: ▪ Customer Admin Account - provided to Customer to access the Secure Virtual Machine. Customer is responsible for the logical access to its designated Secure Virtual Machine(s) and for managing access to the Customer Admin Account. • Armor Admin Account – provided for use by Armor's support staff to provide certain services as necessary or requested by Customer to access Customer's Secure Virtual Machine(s). The credentials for this account are maintained in the Armor Privileged Access Management (PAM) system. The PAM system records Armor's access to the Secure Virtual Machine and logs actions taken by Armor during the use of the account. This account cannot be disabled. Customer is responsible for the configuration of the OS Software after installation and deployment on the Secure Virtual Machine with the pre-installed OS, controlling subsequent configuration changes, and all applications that are installed.
Administration	Customer and Armor share responsibility for the administration of the OS Software. Armor is responsible for providing the initial base OS image and subsequent vendor provided patches and updates. Customer is responsible for all further hardening of the OS, any software installed by Customer, and for maintaining the configuration of the OS to meet Customer's requirements.
Remediation	Armor provides basic troubleshooting of the Secure Virtual Machine and OS.

Resource Availability Monitoring Service

Service Description	Armor provides Resource Availability Monitoring for specific components of the Secure Virtual Machine. As a default service, Armor may monitor: • IP Ping check – Armor attempts to ping the frontend of an IP every five minutes • SSH/RDP Response – Armor attempts a connection of either of these TCP ports (depending on the base operating system) every five minutes • URL/Service – Armor monitors one URL (with 1 case sensitive string check) or service every five minutes. • CPU, memory and disk space utilization.
Installation	Armor is responsible for the installation of the Resource Availability Monitoring.
Configuration	Armor is responsible for the configuration of the Resource Availability Monitoring.
Administration	Armor is responsible for the administration of the Resource Availability Monitoring.
Reporting	Armor will communicate with Customer for alerts in writing it receives from the Resource Availability Monitoring service.
Remediation	Armor is responsible for remediating issues with the infrastructure used to provide the Resource Availability Monitoring service. Customer is responsible for remediating any issues generated from alerts identified by Armor in writing.

.

IP Reputation Filtering Service

Service Description	IP Reputation Filtering blocks access to and from the Armor network by bad IP addresses for which Armor has knowledge. Armor curates lists of known malicious IP addresses used to manage ingress and egress at the routing layer of the infrastructure. These lists are managed by Armor's Threat Resistance Unit (TRU). Customers may request specific IP addresses be "whitelisted" in writing via Armor Management Portal (AMP). Armor, in its sole discretion, may deny Customers request to "whitelist" an IP address(es).
Installation	Armor is responsible for the installation of the IP Reputation Filtering on the Secure Virtual Machines.
Configuration	Armor is responsible for the configuration of the IP Reputation Filtering.
Administration	Armor is responsible for the administration of the IP Reputation Filtering.
Remediation	Armor is responsible for remediating issues for the IP Reputation Filtering.
Disclaimer	Armor makes no warranty, neither expressed nor implied, relating to the IP Reputation Filtering service. Furthermore, Armor expressly disclaims any implied or expressed warranty that traffic from bad IP addresses for which Armor has knowledge will always be blocked and remained blocked.

DoS/DDoS Mitigation Service

Service Description	The Dos/DDoS Mitigation service provides protection for denial and distributed denial of service attacks (DoS/DDoS). Armor deploys redundant, multi-stage DoS/DDoS mitigation systems within Armor's infrastructure that provide early detection and mitigation for DoS/DDoS attacks.
Installation	Armor is responsible for the installation of the Dos/DDoS service on Armor's infrastructure. Use of the DoS/DDoS service by Armor may negatively impact the performance and/or latency associated with Customer's Secure Virtual Machines.
Configuration	Armor is responsible for the configuration of the Dos/DDoS service.
Administration	Armor is responsible for the administration of the Dos/DDoS service.
Remediation	Armor is responsible for managing the DoS/DDoS service when utilized. Communication with Customer is required during this process.
Reporting	Armor reports instances of DoS/DDoS attacks to Customers.
Disclaimer	Armor makes no warranties, whether express or implied, related to the DoS/DDoS Mitigation service or that DoS/DDoS attacks will be successfully mitigated by the Dos/DDoS service. As required for some high-volume attacks, Armor may request that Customer cooperate in redirecting its traffic to a third-party mitigation service to assist with mitigation.

Core Web Application Firewall (WAF) Service

Service Description	The Web Application Firewall (WAF) service provides detection and protection against various types of malicious application layer attacks. The WAF service offers protection for applications on ports 80 and/or 443, only. A list of supported ciphers can be found in the Armor Knowledge Base.
Installation	Armor is responsible for the installation of the WAF service on its infrastructure. Customer must provide a copy of its SSL certificate to Armor Support Staff before HTTPS protection can be enabled.
Configuration	Armor is responsible for the configuration and certificate management of the WAF service in its infrastructure. Customer is responsible for ensuring its applications utilizing the WAF.
Administration	Armor is responsible for the administration of the WAF service in its infrastructure.
Remediation	Armor is responsible for remediating operational issues associated with the WAF service in its infrastructure. Customer may report false positive blocks and request certain types of custom rules in writing. Armor will make a best effort to accommodate requests, but Armor, in its sole discretion, may deny Customers requests.
Disclaimer	Armor makes no warranty, whether express or implied, that all application level attacks or exploits will be prevented by the WAF service. Customer is responsible for ensuring that the applications it deploys on the Secure Virtual Machine have been developed in accordance with industry standard best practices and that they are maintained and updated to maintain a secure posture.

Virtual Network Firewall Service

Service Description	Armor offers a self-managed Virtual Network Firewall.
Installation	Armor is responsible for the installation of the Virtual Network Firewall.
Configuration	Customer is responsible for the configuration of the Virtual Network Firewall
Administration	Armor is responsible for the administration of the Virtual Network Firewall.
Remediation	Customer is responsible for remediating any security issues that arise from the Customer's configuration of the Virtual Network Firewall.
Disclaimer	Armor makes no warranty, whether express or implied, for the services provided by the Virtual Network Firewall. Customer is responsible for defining the rules for each firewall instance. Armor cannot guarantee that the firewalls will protect Customer server from network-based attacks or exploits.

SSL VPN (Secure Remote Access) Service

Service Description	SSL VPN provides Customer the means to administer its Secure Virtual Machines via a secure remote access method. One SSL VPN account is provided with each Customer account. Additional SSL VPN accounts may be purchased for at an additional charge and configured via the Armor Management Portal (AMP).
Installation	Customer is responsible for enabling SSL VPN access through AMP.
Configuration	Customer is responsible for installing the Armor-provided VPN client. Armor is responsible for ensuring the SSL VPN services are configured correctly.
Administration	Customer is responsible for administering SSL VPN user accounts in AMP.
Remediation	Customer is responsible for remediating login and/or user information. Armor is responsible for remediating issues with the VPN service.

Multi-Factor Authentication (MFA) Service

Service Description	Multi-Factor Authentication (MFA) provides an additional layer of authentication for Customer's access to: • administration of its Secure Virtual Machines in conjunction with the SSL VPN access method provided by Armor and/or purchased by Customer; and • the Armor Management Portal (AMP). MFA operates by leveraging a second device, such as a smart phone or telephone, to authenticate a user prior to accessing the Services. Additional information on the configuration and requirements of Multi-Factor Authentication can be found in the Armor Knowledge Base.
Installation	Customer is responsible for the configuration and installation of the MFA service on its preferred secondary device.
Configuration	Armor is responsible for the configuration of the MFA service.
Administration	Armor and Customer share responsibility for the administration of the MFA service. Armor is responsible for the operation and availability of the MFA service to allow for Customer configuration. Customer is responsible for administering access to its users via AMP, resetting user's PIN numbers, and changing the registered telephone number as necessary. For mobile application-based authentication, Customer is required to install and configure a third-party application according to instructions provided by Armor.
Remediation	Armor is responsible for remediating any issues for the MFA service.

Malware Protection Service

Service Description	The Malware Protection services provide protection against malicious software ("malware"). Armor utilizes an enterprise-class malware protection application and deploys the application agent with the Armor Agent. The malware protection agent registers with an Armor management console that receives scan results and activity logs in real-time.
Installation	Installation of the malware protection services occurs simultaneously with the installation of the Armor Agent by Customer. Customer is responsible for the deployment, management, and confirmation of the installation of the malware protection agent.
Configuration	Armor is responsible for the configuration of the malware protection services via remote agent. Configuration includes the application and maintenance of the policies associated with the service. Configuration specific to the local Host or network/environment to enable the service is a Customer responsibility.
Administration	Armor is responsible for the administration of the Malware Protection service through the Armor Agent. For the purposes of this section, "administration" is defined as the management of licenses and the application used to provide the service and the administration of the underlying anti-malware platform.
Reporting	The Armor Management Portal (AMP) provides information related to the health status of the malware protection agent and provides information about malware scans. Malware name, path, category, action taken by the malware protection service, and date of such action, if available, are also displayed in AMP.
Remediation	In situations where malware protection data indicates a potential security event, Armor notifies the Customer via ticket and engages Customer via the Incident Response & Forensic Service. Customer will be notified and must authorize Armor to act before action is taken. Security event remediation is a shared responsibility between Armor and Customer.

File Integrity Monitoring (FIM) Service

Service Description	The File Integrity Monitoring (FIM) service provides collection, analysis, and notification of changes to critical operating system files, as defined by Armor's FIM policy. Armor utilizes an enterprise-class FIM application and deploys the application agent with the Armor Agent.
Installation	Installation of the FIM service occurs simultaneously with the installation of the Armor Agent by Customer. Customer is responsible for the deployment, management, and confirmation of the installation of the FIM agent.
Configuration	Armor is responsible for the configuration of the FIM services via remote agent. Configuration includes the application and maintenance of the policies associated with the service. Configuration specific to the local Host or network/environment to enable the service is a Customer responsibility.
Administration	Armor is responsible for the administration of the FIM service through the Armor Agent. For the purposes of this section, "administration" is defined as the management of licenses and the application used to provide the service and the administration of the underlying FIM platform.
Reporting	FIM event details are available in the Armor Management Portal (AMP). This service runs for Windows in real-time . Customer's services, applications, data and other files are excluded from the scope of the FIM service. Custom alerts, tuning, and FIM policies are available for Customer specific files at additional cost as outlined in the "Additional Services" section for the FIM services below. AMP provides information related to the health status of the FIM agent and provides information about file names and descriptions on each Host, and when and the types of changes that are detected on those files based on the most recent FIM scan.
Remediation	In situations where FIM data indicates a potential security event, Armor notifies the Customer through AMP and engages the Customer via the Incident Response & Forensic Service (as described below). Customer will be notified and must authorize Armor to act before action is taken. Security event remediation is a shared responsibility between Armor and the Customer.
Additional Services	Customer may purchase customized configurations, FIM policies, and FIM monitoring for Customer applications at an additional cost. To do so, Customer must contact its Armor Account Manager to define the scope of these additional services and to create a statement of work for the customizations.

Log and Data Management Service

Service Description	The purpose of the Log and Data Management service is to provide a centralized collection and analysis of the Standard Log Sources (described below). Customer's logs are indexed with a customer unique identifier and then analyzed and correlated for security events. As a default service, Armor retains Customer logs for a period up to thirty (30) calendar days. Custom log sources are excluded from the scope of the default Armor log management service. Customer may increase the retention period for logs by upgrading the log event management service to have logs retained for a period of thirteen (13) months, at an additional cost and in conformance with the "Additional Services" section for the Log and Data Management services below. Upgraded retention is applied on an account basis and cannot be applied on a per server or virtual machine (VM) basis except in the case where Armor provides the Armor Anywhere™ with secure hosting Services to Customer. Standard Log Sources: Armor collects specific logs from the server operating system (OS) and Armor Agent services (FIM, malware and IDS) and a number of additional log source devices outside of the Armor Agent (i.e. Cisco ASA firewalls). Link to the supported sources. Consult your Account Manager for support capability of your log source type.
Installation	Installation of the Log and Data Management service provided through the Armor Agent (FIM, Malware, and IDS) occurs simultaneously with the installation of the Armor Agent by Customer. Customer is responsible for the deployment, management, and confirmation of the installation of the Log and Data Management service. For additional log source implementation, the customer has responsibility to configure a log source, with available Armor documentation. Non-supported sources will require a scoping effort.
Configuration	Armor is responsible for the configuration of the Log and Data Management service from the Armor Agent via remote agent installation. Configuration includes the application and maintenance of the policies associated with the service. Customer is responsible for the configuration specific to the local Host or network/environment. Customer is responsible for configuring their other log source types outside of the Armor Agent, including the adding Log Relay capabilities to the Armor Agent.
Administration	Armor is responsible for the administration of the Log and Data Management service through the Armor Agent. For the purposes of this section, "administration" is defined as the management of licenses and the application used to provide the service and the administration of the underlying logging and analysis platform.
Reporting	The Armor Management Portal (AMP) provides information related to the health status of the Log and Data Management service and provides information about Customer logs from the Armor Agent, including aggregated log information for top sources through event ingestion and index size. Customer can search a pool of 30 days of log data via API and 10,000 events via AMP for 2 consecutive days at a time. The log data includes logs by date, message, and source, and will receive information such as last log received, retention policies, index size, and details related to log throughput and volume. Log data is made available in the VM details and the log management pages in AMP.

Remediation	In situations where log data indicates a potential security event, Armor notifies the Customer via the Incident Response & Forensic Service. Customer will be notified and must authorize Armor to act before action is taken. Security event remediation is a shared responsibility between Armor and the Customer.
Additional Services	Customer may purchase customized configuration, custom log sources, and log exports at an additional cost. To do so, Customer must contact its Armor Account Manager to define the scope of these additional services and to create a statement of work for the customizations. Pricing will be defined in the statement of work.

Host Intrusion Detection Service (HIDS)

Service Description	The Host Intrusion Detection Service (HIDS) provides an agent-based system that is installed on a Host for network traffic analysis and reporting based on policies defined by Armor. Armor utilizes an enterprise-class HIDS application and deploys the application agent with the Armor Agent. The HIDS agent registers with an Armor management console, which receives HIDS events in real-time. HIDS event details are available in the Armor Management Portal (AMP). Armor's HIDS policies are designed to detect network-based events.
Installation	Installation of the HIDS service occurs simultaneously with the installation of the Armor Agent by Customer. Customer is responsible for the deployment, management, and confirmation of the installation of the HIDS agent.
Configuration	Armor is responsible for the configuration of the HIDS service via remote agent. Configuration includes the application and maintenance of the policies associated with the service. Configuration specific to the local Host or network/environment is a Customer responsibility.
Administration	Armor is responsible for the administration of the HIDS service through the Armor Agent. For the purposes of this section, "administration" is defined as the management of licenses and the application used to provide the HIDS service and the administration of the underlying HIDS platform.
Reporting	The Armor Management Portal (AMP) provides information related to the health status of the HIDS agent and the telemetry data coming from the HIDS system. AMP displays information from the HIDS service including the Host name, source IP/Port, destination IP/Port, event signature, and timestamp.
Remediation	In situations where HIDS reports indicate a potential security event, Armor notifies the Customer through AMP and engages Customer via the Incident Response & Forensic Service. Customer will be notified and must authorize Armor to act before action is taken. Security event remediation is a shared responsibility between Armor and the Customer.

Remote Support Service

Service Description	Remote support services provide Armor the ability to remotely access Customer's systems to provide ongoing Armor service support and Incident Response & Forensic Services. Remote support is facilitated by the local administrated account provisioned by Armor on each customer server. Please see the note included in the description of the Armor Agent above for additional detail on this account and its use.
Installation	Installation and removal of the remote support service is performed as needed via remote commands issued by Armor.
Configuration	Armor is responsible for the configuration of the remote support service. Customer is responsible for the configuration related to Customer's network and connectivity.
Administration	Armor is responsible for administration of the Remote Support service.
Reporting	Armor records all support activity taken via opening and/or updating service tickets viewable in the Armor Management Portal (AMP).
Remediation	Armor is responsible for the maintenance of and technical issues with the Remote Support service.

Vulnerability Scanning Service

Service Description	The Vulnerability Scanning service provides for continuous agent-based vulnerability scanning. The service is facilitated by a vulnerability scanning agent that is deployed with the Armor Agent (the "Scan Agent"). The Scan Agent collects information about the instance and includes basic asset identification information, Windows registry information (for Windows systems only), and file version and package information. This information is securely communicated to a scanning platform that assesses the data, determines the vulnerabilities that exist, and reports this data to Customer in the Armor Management Portal (AMP). The Scan Agent collects the information periodically throughout each day and reports the results to the platform. Armor posts vulnerability information in AMP on a weekly basis to represent the state of the instance as of the last scan report.
Installation	Installation of the Vulnerability Scanning service occurs simultaneously with the installation of the Armor Agent. Armor Anywhere Customer is responsible for the deployment, management, and confirmation of the installation of the Scan Agent. In the case of Armor Anywhere with secure hosting, Armor is responsible for the deployment, management, and confirmation of the installation of the Scan Agent.
Configuration	Armor is responsible for the configuration of the vulnerability scanning service via remote agent installation. Configuration includes the application and maintenance of the policies associated with the service. Customer is responsible for the configuration specific to the local Host or network/environment.
Administration	Armor is responsible for the administration of the Vulnerability Scanning service through the Armor Agent. For purposes of this section, "administration" is defined as the management of licenses and the applicable version of the Scan Agent deployed to provide the service.
Reporting	AMP provides information related to vulnerability information and includes vulnerability reports on a weekly basis. Each report contains details on the vulnerabilities identified, including the name and description of each vulnerability, the assets that are affected by each vulnerability, the CVSS score for the vulnerability, and the criticality rating (i.e., Critical, High, Medium, Low, or Informational). Customer can review the results by each vulnerability on a virtual machine basis and by the criticality rating of the identified vulnerabilities.
Remediation	Customer is responsible for the reviewing and implementing recommended remediation detected by the Scan Agent.

ADD-ON SERVICES (INCLUDING ADD-ON MANAGED SERVICES)

Vulnerability Monitoring (External/Internal Scanning) (Navis) Service

Service Description	NAVIS is a third-party vulnerability monitoring tool provided by Coalfire. All NAVIS Vulnerability Monitoring Services are accessed via the NAVIS portal, a third-party portal (independent of Armor's Management Portal (AMP)), which is managed and maintained by Coalfire.
Installation	Armor is responsible for creating an account for Customer in the NAVIS portal and for providing the credentials to Customer. Customer is responsible for completing its enrollment in the NAVIS portal.
Configuration	Customer is responsible for maintaining the accuracy of configuration in the NAVIS portal.
Administration	Coalfire and the Customer share responsibility for the administration of the NAVIS Vulnerability Monitoring Service.
Remediation	Coalfire is responsible for remediating any issues with the NAVIS Vulnerability Monitoring Service including the NAVIS portal.
Disclaimer	Armor does not offer any service level commitments for the NAVIS Vulnerability Management Service. The service is provided "as-is."

Advanced Web Application Firewall (WAF) Service

Service Description	The Advanced Web Application Firewall (WAF), a third party appliance, provides detection and protection against various types of malicious application layer attacks. A list of supported ciphers can be found in the Armor Knowledge Base.
Installation	Armor is responsible for installing the Advanced Web Application Firewall appliance for the Customer.
Configuration	Customer is given administrative credentials and is responsible for configuring the Advanced Web Application Firewall. Customers are responsible for complying with any and all compliance regulations involving the Advanced WAF
Administration	Customer is responsible for administration of the Advanced Web Application Firewall.
Remediation	Customers are responsible for remediating issues found to be specific to their environments. Armor provides limited support for the Advanced Web Application Firewall. Limited support defined as: virtual server configuration, pool configuration, SSL certification installation/removal, WAF baseline protection (OWASP 10), WAF PCI-DSS protection (SSN masking), WAF logging configuration to Armor Log Relay.
Disclaimer	Armor makes no warranty, whether express or implied, that all application level attacks or exploits will be prevented by the WAF service. Customer is responsible for ensuring that the applications it deploys on the Secure Virtual Machine have been developed in accordance with industry standard best practices and that they are maintained and updated to maintain a secure posture. The Advanced Web Application Firewall appliances are provided "as-is."

Data at Rest Encryption (Vormetric) Service

Service Description	The Vormetric Data Security Platform, a third-party solution, protects Customer data with encryption, key management, appropriate security policies, and fine-grained data access controls. This service encompasses file and folder encryption as well as a centralized key management system.
Installation	Armor is responsible for deploying Vormetric on all subscribed Secure Virtual Machines.
Configuration	Customer maintains administrative domain and control for all encryption policies and keys. Customer is responsible for configuration of the Vormetric service.
Administration	Armor is responsible for applying vendor supplied updates. Customer has sole responsibility for administering all Vormetric services.
Remediation	Armor may provide general support for the Vormetric services.
Disclaimer	Armor does not offer any service level commitments for Vormetric Data Security Platform. The Vormetric Data Security Platform is provided "as-is."

Disaster Recovery Service (Zerto) Service

Service Description	Zerto offers a disaster recovery solution by providing Secure Virtual Machine replication at the virtual disk level with minimal impact on product workloads.
Installation	Armor is responsible for provisioning the recovery environment and configuring the Secure Virtual Machine for replication.
Configuration	Armor is responsible for the configuration of any firewall rules, LAN-to-LAN (L2L) IPSec tunnels, and/or SSL VPN access to the recovery environment conforms to the terms outlined in the respective descriptions of those services.
Administration	Armor is responsible for maintaining the Zerto infrastructure and applying vendor provided updates.
Remediation	Armor will provide general support for the remediation of the Disaster Recovery Service.
Disclaimer	Armor does not offer any service level commitments for Zerto. Zerto is provided "as-is."

Advanced Backup Service

Service Description	Advanced Backup provides Customer the ability to configure and restore file, folder, drive and Secure Virtual Machine level backups. This service is available to Armor Anywhere with secure hosting customers with workloads hosted in the Dallas (DFW) and Phoenix (PHX) data centers.
Installation	Armor is responsible for installing the Rubrik agent.
Configuration	Customer is responsible for the configuration of the Advanced Backup Service.
Administration	Armor is responsible for the administration of the Advanced Backup Service. Customer is responsible for maintaining backup policies and performing restores from the backups.
Remediation	Armor is responsible for remediating the Advanced Backup Service.
Reporting	The Armor Management Portal (AMP) provides visibility to Secure Virtual Machines subscribed to the backup service, configured backup policies, and the available successful backups.
Disclaimer	Armor does not offer any service level commitments for Advanced Backup. Advanced Backup is provided "as-is."

Load Balancers

Service Description	Virtual load balancer appliances are provided by a third party and allow Customer to distribute traffic loads across multiple Secure Virtual Machines.
Installation	Armor is responsible for installing the Load Balancer appliance in the Customer.
Configuration	Customer is given administrative credentials and is responsible for configuring the load balancer.
Administration	Customer is responsible for administration of the load balancer.
Remediation	Armor provides limited support for the Load Balancers.
Disclaimer	Armor does not offer any service level commitments for the load balancer appliances. The load balance appliances are provided "as-is."

Colocation Service

Service Description	Colocation Services allow Customer to locate certain equipment that is required to interface directly with its Secure Virtual Servers in Armor' datacenter locations for an additional fee. Armor will provide connectivity, power, UPS and physical security for Customer's co-located equipment.
Installation	Customer and Armor are responsible to coordinating the installation of Customer equipment.
Configuration	Customer is responsible for the configuration of Customer's co-located equipment.
Administration	The customer is responsible for the administration, maintenance, service, and functionality of co-located equipment.
Remediation	Armor is responsible for remediating issues with Armor's network connectivity and power issues. Customer is responsible for remediating all issues with the co-located equipment, including maintenance and support. Armor may assist Customer on a best efforts basis with issues that may arise with the co-located equipment at an additional charge upon Customer's reasonable written request.
Disclaimer	Customer must provide its own property insurance to cover co-located equipment.

Cloud Security Posture Management (CSPM)

Service Description	Armor's Cloud Security Posture Management (CSPM) helps customers identify policy and security violations in their public cloud environment and provides remediation steps to address those policy and security violations.
Installation	CSPM is available to all Armor Anywhere customers with an AMP account. CSPM is installed by giving Armor's platform read-only access to one or more of your public cloud accounts to monitor assets and their configurations. .
Configuration	Customer is responsible for the configuration of connectors to the CSPM service via the Armor Management Portal (AMP). Creation and configuration of third-party cloud sources is a Customer responsibility.
Administration	Armor is responsible for the administration of the cloud security posture management service.
Remediation	Customer is responsible for applying remediation recommended by CSPM service.
Disclaimer	CSPM does not provide automated reporting or remediation. Customer is responsible for running cloud posture reports and managing remediation when recommended.

Endpoint Detection and Response (EDR)

Service Description	Endpoint Detection and Response (EDR) is an advanced security detection and incident response solution delivering continuous visibility to Security Operations and Incident Response teams across an organization's end user IT estate. EDR can be installed on laptops, desktops, and servers, giving Customers a 360-degree detailed overview of endpoint activity. EDR provides next-generation endpoint protection, identifying suspicious activities and events, and performing validation on detected threats, along with identifying anomalies and suspicious behavior patterns. The EDR product also provides next-gen anti-virus technologies to prevent malicious executables from firing in your environment. And, because EDR is a Software as a Service (SaaS) solution, there is no hardware that needs to be deployed on the customer's premise or within their data center.
Installation	Customer is responsible for the deployment, management, and confirmation of the installation of the EDR sub-agent. Customer will be responsible for installing the Armor Anywhere Agent and the EDR sub-agent on each endpoint device. Provisioning is done through the Armor Management Portal (AMP). The EDR agent will serve as a sub-agent to the Armor Anywhere (AA) agent, allowing for logssecurity telemetry from the EDR agent to be ingested and threat analytics to be performed. Armor recommends the customer disconnects uninstalls any existing anti-virus program prior to installing EDR due to next-gen AV being an included component of the EDR install. Customers will be able to install the EDR sub-agent one-by-one at the machine level, or go to the Armor Toolbox and choose to install all machines in scope for this service through a batch process.
Configuration	Armor is responsible for the administration of the Armor Agent and for the configuration of the component parts of the Armor Agent that are installed using the Armor Agent. Once Armor Engineering completes configuration of the EDR sub-agent, the Customer is responsible for customization and deployment of this service to their endpoint devices. Armor is responsible for patches and updates to the EDR sub-agent. Armor will provide a baseline security policy configuration that can be used across all devices supported. Armor recommends that this policy is never touched by the customer and any custom policies are stored in a separate policy configuration by the Customer. After configuration is completed, the sensor will perform an initial, one-time inventory scan in the background to identify malware files that were pre-existing on the endpoint. Once the baseline configuration is provided, the customer can install or uninstall the subagent, either using a Command Line Interface (CLI) or a toolbox provided through the AMP portal.
Administration	Armor is responsible for the administration of the EDR service through the Armor Agent. For the purposes of this section, "administration" is defined as the management of licenses and the application used to provide the service and the administration of the underlying logging and analysis platform.

	EDR collects and analyzes comprehensive information about endpoint events, giving Customers near-real time visibility into their environment. EDR delivers threat intelligence, automated watchlists, and integration with other security tools within the Customer's environment for unparalleled visibility. Customers can define which team member will have credentials into the portal and choose the RBAC and privilege level assigned to them. The customer is responsible for all administration of the technology within the EDR console themselves.
Reporting	The EDR agent will send logs to the Armor Security Information Event Manager (SIEM) which will examine log data for patters that could indicate a cyberattack, and then correlates event information to identify anomalies and generate alerts. Events are indexed, stored and made available through the Armor web portal with the data lake and can be accessed via log search. The Security Orchestration and Automation (SOAR) moves data to the next level, where it looks at workflow and analysis. Rules are applied to create a risk profile in order to determine risk severity and whether to open on an incident ticket. Reporting through AMP shows: • Sub-Agent Health • Detections/Incidents • Events/Alerts
Remediation	Validation and threat remediation for EDR is the Customer's responsibility. Armor will not automatically quarantine or block access to any endpoint device where suspicious activity is detected, unless otherwise directed by the customer or if it represents a significant security threat indicative of a breach or active compromise. Customers have access to a complete and detailed overview of endpoint activity. This empowers teams to proactively hunt for threats, review risk and incidents, and take immediate remediation action. EDR records and stores endpoint activity data so that threat hunting can take place in near-real time. EDR gives Customers the ability to visualize the entire attack kill chain cycle and remediate at any step of the process flow.

ARMOR SUPPORT SERVICES MATRIX

	Basic Support (included, no cost)	**Advanced Support (Add-on, MRC, annual)**	**Enterprise Support (Add-on, MRC, annual)**

Self-service support	Full product documentation and support/troubleshooting available through http://Docs.armor.com	Full product documentation and support/troubleshooting available through http://Docs.armor.com	Full product documentation and support/troubleshooting available through http://Docs.armor.com
Included Infrastructure Management Services	VM configuration and deployment, Add/Remove services including backup and disaster recovery configuration, 24/7 server monitoring, troubleshooting, Patching support, OS support, Network configuration support	VM configuration and deployment, Add/Remove services including backup and disaster recovery configuration, 24/7 server monitoring, Troubleshooting, Patching support, OS support, Network configuration support	VM configuration and deployment, Add/Remove services including backup and disaster recovery configuration, 24/7 server monitoring, Troubleshooting Patching support, OS support, Network configuration support, Architecture analysis and guidance
API Services access	Full access, unlimited use.	Full access, unlimited use.	Full access, unlimited use.
Ticketing	24/7/365	24/7/365	24/7/365
Phone support	Available as an add-on service enabling 8am-5pm CST & GMT, M-F	8am-5pm CST & GMT, M-F	24/7/365
Security Operations Center	24/7/365 operations	24/7/365 operations	24/7/365 operations
Customer Success Manager	--	Named Customer Success Manager	Named Customer Success Manager
Business Reviews	--	--	Up to a Quarterly Executive Business Reviews
Support Response SLO	48 hours	--	--
Support Response SLA	--	Priority ticket handling. 6 hours for acknowledgement during coverage hours, eligible for up to 3% credit on support service for impacted month. Request for credit must be made in writing (via ticket) within 72 hours of incident.	Priority ticket handling. 30 minutes to acknowledgement. Eligible for to 5% credit on support service for impacted month. Request for credit must be in writing (via ticket) within 120 hours of incident.

Managed & Enterprise Implementation Service

Service Description	These services will be unique to each customer and tailored to their environment and needs, the individuals assigned to support your organization will begin by establishing the customer objectives in writing at the time of initiation of this service. The scope of services does not extend beyond Armor furnished products.		
Service Level		**Managed**	**Enterprise**
Eligibility	$100,000.00 (USD) in Total Contract Value at the time of service initiation.		$250,000.00 (USD) in Total Contract Value at the time of service initiation.
Service Matrix	Duration	Not to exceed 4 weeks.	Not to exceed 8 weeks.
	Personnel	Named project staff	Named project staff
	Response & Training	• 24 Hour general support response objective. • Up to 2 hours of product training, remote.	• 2 Hour general support response objective. • Up to 5 hours of product training, remote.
Initiation	An onboarding coordinator may be named as the primary contact point for the client as a part of this service offering. This individual will act as the primary liaison for all services, including the definition of objectives, scheduling, and follow up.		
Reporting	Reporting is provided on an ongoing basis throughout the duration of the project and tailored to each engagement.		
Remediation	These services carry no guarantees or SLA/SLO's. Each engagement will be a best effort to ensure the objectives established in the initial scoping discussion are met.		

Security Trends & Insights Report

Service Description	The Security Trends and Insights Reports is a standardized report which summarizes security data from the client environment and presents it in a scheduled report to the customer for review. This service delivers a digital report to analyze trends, security analytics of note, and any prioritized protection methods the customer might need to take within their environment.
Delivery	Armor is responsible for the development and delivery of the report on the subscribed cadence by the customer. The customer can subscribe to this report in weekly, bi-weekly and monthly delivery schedules.
Disclaimer	This service carries no guarantees on the data or report briefing delivered. This report cannot be customized.