ARMOR® MSP CHANNEL PARTNER SERVICE DESCRIPTIONS

SUMMARY

This document is the property of Armor Defense Inc. and Armor Defense Ltd ("Armor"). The information contained herein is proprietary and confidential to Armor and strictly restricted from disclosure. The dissemination, distribution, copying or use of this document, whether in whole or in part, is strictly prohibited without prior express written permission of Armor's executive leadership.

These Service Descriptions describe and define each of the service components for the Armor Anywhere™ 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™ 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

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.

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 are here. 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.
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. Technical details regarding the connectivity required to use the Armor Agent are available here.
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.

Dynamic Threat Blocking Service

Service Description	Dynamic Threat Blocking service leverages the IP Reputation Filtering service to provide a service that can be applied by a Customer account user to services within its network that are internal or external to the Services. The service delivers metadata related to malicious IP addresses known by Armor, allowing the Customer account user to query and block traffic from Armor's curated database.
Installation	Customer is responsible for the application or integration of the Dynamic Threat Blocking service.
Configuration	Armor is responsible for the configuration of the Dynamic Threat Blocking service and for ensuring vendor updates are provided and applied in a timely manner.
Administration	Armor is responsible for the administration of the Dynamic Threat Blocking service.
Remediation	Armor is responsible for remediating the Dynamic Threat Blocking service. Customer is responsible for deciding to allow or block IP traffic based on the results returned by the Dynamic Threat Blocking service as well as for the actual blocking of such IP traffic.
Disclaimer	Armor makes no warranties, whether express or implied, relating to the IP Reputation Filtering service. Armor further disclaims any implied or expressed warranties that traffic from bad IP addresses for which Armor has knowledge will always be blocked and remained blocked.

Two-Factor Authentication (2FA) Service

Service Description	Two-Factor Authentication (2FA) 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). 2FA 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 Two-Factor Authentication can be found here.
Installation	Customer is responsible for the configuration and installation of the 2FA service on its preferred secondary device.
Configuration	Armor is responsible for the configuration of the 2FA service.
Administration	Armor and Customer share responsibility for the administration of the 2FA service. Armor is responsible for the operation and availability of the 2FA 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 2FA 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	Armor is responsible for monitoring the Malware Protection service and for remediating issues with the operation of the Malware Protection service. In situations where malware protection data indicates a potential security event, Armor notifies the Customer in writing 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 and for Linux servers every Sunday and Thursday at 23:00 CST. 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	Armor is responsible for monitoring the FIM service and for remediating any issues with the operation of the FIM service. 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 Event Management Service

Service Description	The purpose of the Log and Event 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 event management services below. Upgraded retention is applied on an account basis and cannot be applied on a per server or virtual machine (VM) basis. Standard Log Sources: Armor collects specific logs from the server operating system (OS) and Armor Agent services (FIM, malware and IDS).
Installation	Installation of the Log and Event Management 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 Log and Event Management service.
Configuration	Armor is responsible for the configuration of the Log and Event Management 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 Log and Event 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 Event Management service and provides information about Customer logs, including aggregated log information for top sources through event ingestion and index size. Customer can search its 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 and event data are made available in the VM details and the log management pages in AMP.
Remediation	Armor is responsible for monitoring the Log and Event Management service and for remediating any issues with the operation of the Log and Event Management service. 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 data connectors, 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	Armor is responsible for monitoring the HIDS service and for remediating any issues with the operation of the service. 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 (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.

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. Customer 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.

Incident Response and Forensics (IRF) Service

Service Description	The Incident Response and Forensics (IRF) service provides for investigation with response and remediation options for certain reported events. The service consists of four (4) components: (a) event identification; (b) validation and initial triage with customer notification; (c) customer consultation; and (d) in-depth forensic investigations, reporting, and supporting remediation efforts. Components (a) – (c) are included with the Services and limited to a two (2) hour maximum duration per incident. Item (d) is available to Customer at an additional cost.
Event Identification	Armor's security analytics platform ingests and correlates data from Armor's security tools and other optional log sources and generates event notifications for potential indications of compromise (IOCs). These events are noticed to the Armor SOC for validation follow up. Customers may self-report potential security events.
Validation and Initial Triage with Customer Notification	The Armor Security Operations Center (SOC) opens a ticket with the Customer in the Armor Management Portal (AMP) and investigates the identified event as detailed above. The investigation may include access to the affected servers to review additional information. The SOC then provides information, to the extent practicable, on the type, nature and severity of the event, and may recommend steps to remediate the event. The SOC may request a Customer consultation based on the severity and/or complexity of the event.
Customer Consultation	At a time mutually convenient for Customer and the SOC, SOC personnel will discuss the event, gather additional information about the customer environment, and recommend additional actions. Once completed, Armor and Customer will agree upon any additional actions to be taken by the Armor SOC to further investigate, report on and support remediation efforts surrounding the event. All additional actions will require a retainer or the purchase of Incident Response time blocks to cover the time required to accomplish the agreed upon actions. A summary of the discussions and any agreed upon additional actions will be documented in the ticket.
Advanced Investigation, Remediation and Forensics	Armor Security Operations engineers will execute the agreed upon actions and record their findings in the ticket. Any additional direction, references, or referrals will be made to conclude the IRF Service.
Additional Incident Response and Forensics Hours	Customer may purchase additional IRF time blocks to address the assistance they may require from Armor to investigate and provide remediation assistance with security events. These time blocks are purchased in advance and expire twelve (12) months from the date of purchase. Unused IRF time blocks will not rollover into a new twelve (12) month term and will not be refunded to Customer.

Additional IRF Services	In the event a customer does not utilize all its purchased IRF time blocks within the twelve (12) month period, they may opt to use the remaining time on any of the following additional IRF services. They may also opt to purchase IRF time blocks to have these services provided by Armor. **Security Awareness Training** Description: Armor will remotely deliver a security awareness training session that can be used to fulfill compliance requirements. Armor will provide a standardized training session that will last approximately two (2) hours. Estimate time required – 4 hours **Advanced Security Reporting** Description: Reports can be of technical, management, or executive level and the details will be discussed and agreed upon during a consultation call. Estimate time required: • Weekly reports: 52 hours (1 hour per week per report) • Monthly reports: 12 hours (1 hour per month per report) **Industry Threat Report** Description: An industry specific report on the current state of the chosen industry to include current and expected trends and threats to the industry. Estimated time required - 10+ hours **Incident Response & Management Tabletop** Description: Armor will conduct an incident response tabletop exercise, to include tickets and real-time response to mimic and test the incident response capabilities and the interaction with Armor incident response services. Tabletops will start with Armor initiated response and will include escalation from Armor standard response and company runbooks. Estimated time required: 20+ hours (depending on scenario chosen).

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

Custom Policy Configuration Service

Service Description	The Custom Policy Configuration Service provides the design, development, and application of custom policies or rules for any Armor host or account. This includes changes to policies and configuration related to File Integrity Monitoring (FIM), Anti-Malware, and Host Intrusion Detection Service (HIDS) on each host. Custom configurations may modify the behavior or function of any associated service. Requests for custom rules or policies must be made in writing in the Armor Management Portal (AMP).
Installation	Installation of the custom policy is performed by the Armor.
Configuration	Armor is responsible for the configuration of the Custom Policy Configuration via remote access.
Administration	Armor is responsible for the administration of the Custom Policy Configuration service via the Armor Agent.
Reporting	Reporting is provided in AMP.
Remediation	Armor will apply custom rules upon Customer's reasonable written request. Customer acknowledges that custom rules may impact standard service terms and remediation.