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 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 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 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 Complete™ 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	Armor is responsible for monitoring the Log and Data Management service and for remediating any issues with the operation of the Log and Data 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 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. 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 Complete, 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 here ***<Matthew/Rahul will point to KB for supported ciphers>***.
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 Complete 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."

SSL Certificates

Service Description	SSL Certificates may be purchased in the Armor Management Portal (AMP).
Configuration	Armor will provide certificate information to Customer in writing
Remediation	Armor will provide assistance in troubleshooting and remediating issues with installed certificates per the Support Services Matrix.
Disclaimer	The certificates are provided by GlobalSign, a third-party commercial Certificate Authority (CA). Armor cannot ensure that GlobalSign will maintain its standing as a CA or that the certificates purchased will be honored through their expiration date.

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.

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 Experience Manager	--	Named Customer Experience Manager	Named Customer Experience 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.

Armor Automated Compliance – Prisma Public Cloud™

Service Description	The Armor Automated Compliance – Prisma Public Cloud offering provides monitoring on AWS, Azure and GCP environments for cloud security and compliance risks due to account misconfigurations against master security policies.
Installation	Armor is responsible for creating the customer instance within Armor's master tenant and assigning the initial compliance policy to the customer's tenant.
Configuration	Armor will work with the customer to configure the settings for the customer tenant. Customer will provide the set-up details and credentials in order to access the customer cloud environment and provide an IAM role for Armor so they can setup access into the visibility controls necessary to apply appropriate posture management capabilities. Customer specific integrations will not be available.
Administration	Armor is responsible for the overall administration of the customer tenant within Armor's master tenant. Customer is responsible for the administration of users.
Remediation	The Prisma Public Cloud Portal provides both manual and auto-remediation steps to many common misconfiguration violations. Remediation beyond what is provided within the portal is the customer's responsibility.
Disclaimer	Armor makes no warranty, whether express or implied, that all malicious or anomalous cloud activity will be detected.
Professional Services	Armor does not offer professional services regarding the Prisma Public Cloud product. The product is offered as is. Armor will not build custom policies for customers. Customers will receive access to the Prisma Public Cloud (formerly known as RedLock) portal. Armor will not deliver incident management in relation to this service. Customers will receive front-line support for the service through the Armor Ticketing Platform.