ARMOR ANYWHERE

TECHNICAL SOLUTIONS BRIEF

WE PROTECT YOUR APPLICATIONS AND DATA, ANYWHERE.

ARMOR

INTRODUCTION

Armor Anywhere integrates robust security capabilities with 24/7/365 monitoring to deliver unified threat detection and response as well as compliance for your applications and data wherever they reside.

ARMOR AWS

AZURE GCP

HYBRID PRIVATE

ARMOR ANYWHERE

24/7/365 Monitoring and Response

Security Capabilities	■ Host-based IDS/IPS ■ File Integrity Monitoring ■ Vulnerability Scanning ■ Malware Protection ■ Security Log Collector ■ Recommendation Scan
Log and Data Management (add-on)	■ Cloud-native Logs ■ Third-party Logs
Secure Hosting (add-on)	■ Compute ■ Storage ■ Web Application Firewall ■ IP Reputation Management ■ Redundant Infrastructure

Cloud Security Platform

Unified Visibility

Armor Anywhere addresses the following use cases:

Threat Detection and Response
Get advanced detection of threats in your applications and data. Go beyond alerting to receive a guided response from our cybersecurity experts.

Audit-Ready Compliance
Simplify compliance by meeting key controls in frameworks such as PCI DSS, HIPAA/HITRUST, and GDPR.

Protection for Mission-Critical Applications and Data
Offload the headaches of managing infrastructure while getting the industry's leading protection for your most sensitive workloads.

ARMOR ANYWHERE FOR ANY ENVIRONMENT

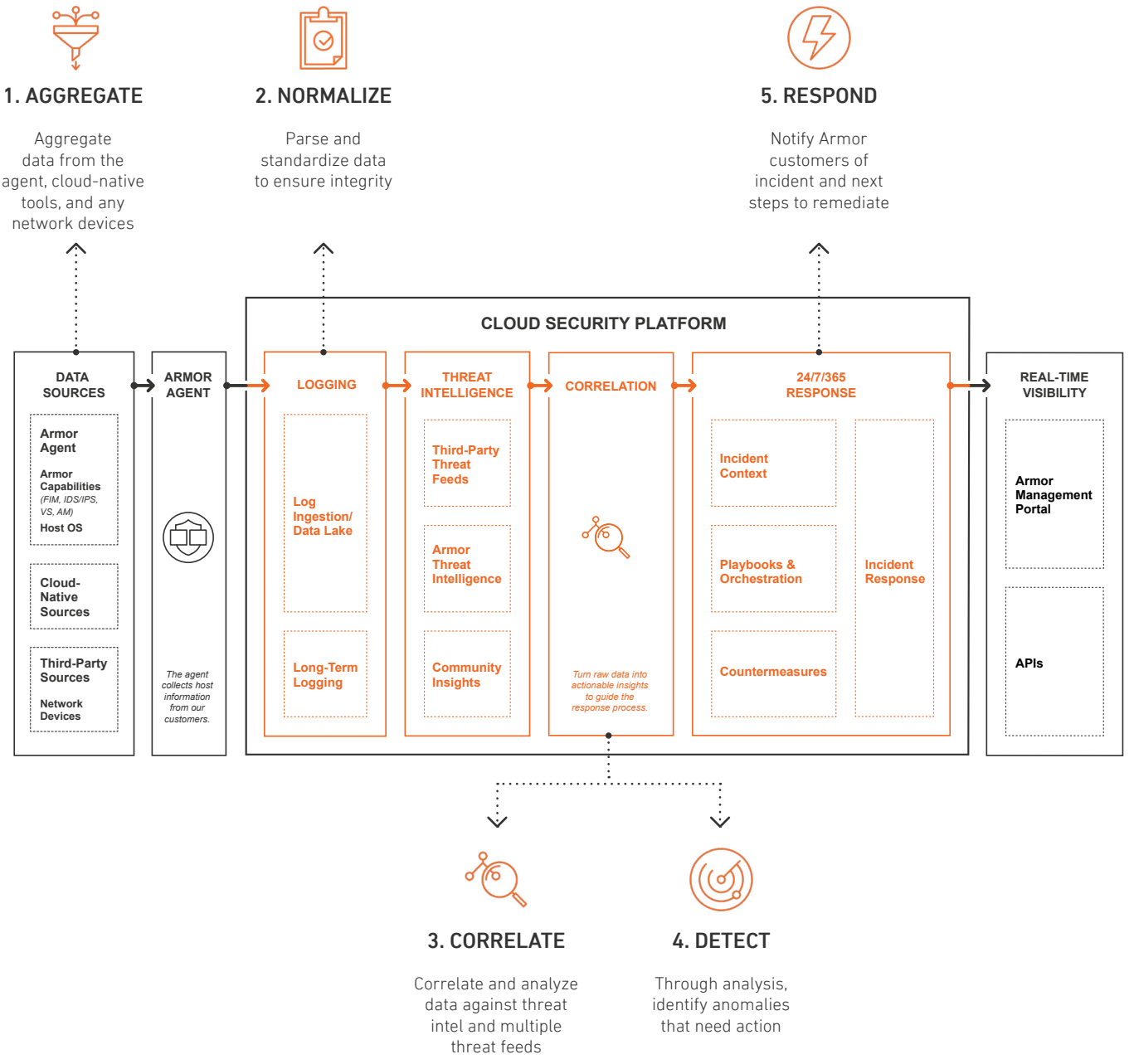
Armor Anywhere provides technology to protect customer workloads and has the ability to detect and respond to threats in any environment. Combined with our high-performance hosting infrastructure, Armor provides a secure and compliant virtual private cloud environment for customers who have mission-critical and sensitive applications.

	ARMOR ANYWHERE	ARMOR ANYWHERE WITH SECURE HOSTING
ENVIRONMENT	PRIVATE, PUBLIC, HYBRID, ON-PREM	ARMOR DATA CENTERS
WORKLOAD PROTECTION		
Host-based IDS/IPS	●	●
File Integrity Monitoring	●	●
Malware Protection	●	●
Vulnerability Scanning	●	●
Recommendation Scans	●	●
Log and Data Management	●	●
VISIBILITY		
Management Portal	●	●
NETWORK PROTECTION		
Web Application Firewall		●
IP Reputation Management		●
INFRASTRUCTURE		
Web		●
Load Balancers		●
Backup		●
Compute		●
Storage		●
Encryption (Optional)		●
Regions/Availability Zones/Edge Locations		●
SERVICES		
24/7/365 SOC Monitoring	●	●
Available Premium Support Options	●	●

CLOUD SECURITY PLATFORM

The Armor cloud security platform is the industry's leading threat detection and response platform. The platform integrates threat intelligence, advanced analytics, and incident response capabilities into a single platform that bolsters your defenses, uncovers threats, and prevents security breaches. Its modularity and interoperability allow Armor to deliver powerful security and compliance outcomes aligned to the unique use cases and consumption needs of our customers.

ARMOR CLOUD SECURITY PLATFORM IN ACTION



AGENT CAPABILITIES

The Armor Anywhere agent is lightweight and can be deployed in private, public, and hybrid clouds, as well as in on-premise environments. Armor Anywhere comes with the following capabilities:

HOST-BASED INTRUSION PREVENTION/INTRUSION DETECTION SYSTEM

With visibility to inbound and outbound activity at the host, Armor inspects anomalous traffic against predefined policies—detecting and blocking attacks such as generic SQL injections, generic XSS attacks, and generic web app effects. The host-based IDS/IPS has two modes—Detection and Prevention—allowing operators such as DevOps practitioners and security analysts to select their preferred setting.

IDS/IPS events are analyzed and correlated with event data from your other devices under management by our cloud security platform, delivering enhanced detection of potential threats across your cloud, on-premise, hosted, and hybrid environments.

FILE INTEGRITY MONITORING

File integrity monitoring examines critical system file locations on your hosts as well as critical OS files for changes that may allow threat actors to control your environment.

File integrity monitoring looks for:

- Changes to critical OS files and processes such as directories, registry keys, and values
- Changes to application files
- Rogue applications running on the host
- Unusual process and port activity
- System incompatibilities

MALWARE PROTECTION

Armor's malware protection safeguards your environment from harmful malware and botnets, including viruses, spyware, and rootkits.

Malware protection performs real-time continuous scanning of your instances against the latest definitions, heuristics, and honeypot discoveries. Armor's definition database is sourced by internal, public, and private resources. All instances report back to the AMP console, enabling us to manage and report on malware prevention and response. Detected threats are monitored and alerted on 24/7/365.

VULNERABILITY SCANNING

Armor's vulnerability scanning searches for application vulnerabilities that could be exploited by a threat actor and put your applications and data at risk.

RESPONSIBILITY BREAKDOWN	ARMOR	CUSTOMER
Provisioning and Management of Vulnerability Scanning Service	●	
Availability of Vulnerability Scanning Service Portal	●	
Initial Configuration of Customer Account Details	●	
Subsequent Configuration of Environment Scan: Scope and Scheduling	●	●
Ongoing Scan Modification	●	●
Remediation of Detected Vulnerabilities*	●	●
Review of Reports by Armor's Security Operations Team	Upon Request	
Application of Scan Reports to Customer Audit	●	●

*Applies to Armor Anywhere with secure hosting only. Remediation of vulnerabilities and patch management is considered a shared responsibility between Armor and the customer.

POLICY RECOMMENDATION SCANS

With recommendations scans, you can scan your hosts to identify vulnerabilities and the state of controls on the host.

It scans the operating system, installed applications, Windows registry, open ports, directory listings, the file system, running processes and services, and users.

The scans provide recommendations and can be set to automatically apply new rules and changes such as the addition of any new rules to intrusion prevention or file integrity monitoring, as examples.

SECURITY LOG COLLECTOR

Log and data management allows organizations to enhance threat detection, expand context for effective response, and satisfy compliance requirements for the storage of logs. Armor's security log collector ingests logs from the following sources into the cloud security platform:

LOG TYPES		
AGENT LOGS	**CLOUD-NATIVE SOURCES**	**THIRD-PARTY SOURCES**
The capability natively supports logs coming from Armor's core security capabilities including IDS, file integrity monitoring, malware protection, vulnerability scanning, and operating system logs.	Armor can ingest, analyze, and correlate logs from AWS CloudTrail, AWS GuardDuty, AWS WAF, VPC flow logs, Azure Application Gateway logs, and Azure NSG flow logs. Contact Armor for additional log management options for Google Cloud Platform.	Third-party sources include network appliances, web application firewalls, application logs, and others. Armor can ingest more than 250 log types. Additional configuration and tuning may be necessary.

Log and data management delivers correlated events with additional flexible tuning options to minimize "noise" and increase fidelity of detection and alerting for your environment. For organizations subject to compliance requirements, log and data management provides additional value through storage of logs for up to 13 months. Log and data management is usage-based, allowing you to optimize your investment and pay only for how much you use.

SETUP

OPERATING SYSTEM SUPPORT

The Armor Anywhere agent is packaged to make it easy to install on major Window and Linux platforms. The following OS environments are supported:

CENTOS	■ 6.X ■ 7.X
RED HAT ENTERPRISE LINUX (RHEL)[1]	■ 6.X ■ 7.X
UBUNTU	■ 16.04 ■ 18.04
AMAZON LINUX[1]	■ 2015.03 ■ 2015.09 ■ 2016.03 ■ 2016.09 ■ 2017.03 ■ 2017.09 ■ 2018.03 ■ Amazon Linux 2
ORACLE LINUX[1]	■ 6.X ■ 7.X

WINDOWS SERVER[2]	■ Microsoft Windows Server 2012 Standard[3] ■ Microsoft Windows Server 2012 Datacenter[3] ■ Microsoft Windows Server 2012 Enterprise[3] ■ Microsoft Windows Server 2012 R2 Standard[3] ■ Microsoft Windows Server 2012 R2 Datacenter[3] ■ Microsoft Windows Server 2012 R2 Enterprise[3] ■ Microsoft Windows Server 2012 R2 Foundation[3] ■ Microsoft Windows Server 2016 Standard ■ Microsoft Windows Server 2016 Datacenter ■ Microsoft Windows Server 2016 Essentials ■ Microsoft Windows Server 2019 Standard ■ Microsoft Windows Server 2019 Datacenter ■ Microsoft Windows Server 2019 Enterprise

1. To use a Linux-based Armor Anywhere agent, you must have Python 2.7 installed. 2. For Windows users, PowerShell 3 must be installed. 3. For Windows 2012 users, when you install the Armor Agent, the corresponding Trend Micro agent will require a reboot.

DEVOPS SUPPORT

Armor provides install scripts for the Armor Anywhere agent to integrate into your DevOps toolchains.

ONBOARDING & INSTALLATION

Armor provides step-by-step guidance on installing the Armor Anywhere agent in your environment through AMP. Once the quick-and-easy installation is complete, the Armor Anywhere agent registers with Armor's API service endpoints via open outbound network ports or port-forwarding services. All data in transit is encrypted using TLS 1.2. With a secure connection established, the security scan results and activity logs are sent to AMP.

INSTALLATION OF THE ARMOR ANYWHERE AGENT

Installation of Armor Anywhere includes two components—the agent and the supervisor. Both of these components ensure a more robust process. The Armor agent is intended to be the primary mechanism with which the user interacts. This is the component downloaded by the user that controls registration and performs service setup/orchestration during install.

- The Armor Anywhere agent runs as a service while the supervisor runs as a task or cron.
- Both the Armor Anywhere agent and the supervisor require connectivity to the Armor API.
- Armor manages/updates both components.

MINIMUM REQUIREMENTS	
WINDOWS ■ 2 CPU Cores ■ 2 GB RAM ■ 3 GB Disk Space	**LINUX** ■ 1 CPU Cores ■ 1 GB RAM ■ 3 GB Disk Space
Bandwidth: Estimated 50-100Kb per minute, based on the logs generated in your system.	

ARMOR ANYWHERE WITH SECURE HOSTING COMPONENTS

COMPONENTS

CLOUD SERVERS
Wide range of configurations, instant provisioning, and 99.99% availability SLA

Virtual Processors
1 | 2 | 4 | 8 | 12 | 16 vCPUs

Virtual Memory
2 | 4 | 6 | 8 | 12 | 16 | 24 | 36 | 48 | 64 |72 | 96 GB

OS
Ubuntu | RedHat | Windows | CentOS

STORAGE
Flexible storage options

Tier 1—Top Performance
All-SSD 10 to 500 GB

Tier 2—Top Value
Hybrid SSD 50 GB to 2 TB

Tier 3—High Value
Fast Disk 250 GB to 2 TB

NETWORK
Built-in networking options available as part of offer

- Native Firewall
- Private IP Addresses
- VPN Services-SLL and L2L/IPSec

OPERATING SYSTEM SUPPORT — WINDOWS SERVER

WINDOWS
- 2012 Datacenter
- 2012 R2 Standard
- 2012 Standard
- 2016 Standard (Desktop Experience)

Note: Windows servers require a minimum of 2 CPU and 2GB of memory.

LINUX
- CentOS – Versions 6,7
- RHEL – Versions 6,7
- Ubuntu – Versions 16.04, 18.04

Note: Windows servers require a minimum of 2 CPU and 2GB of memory.

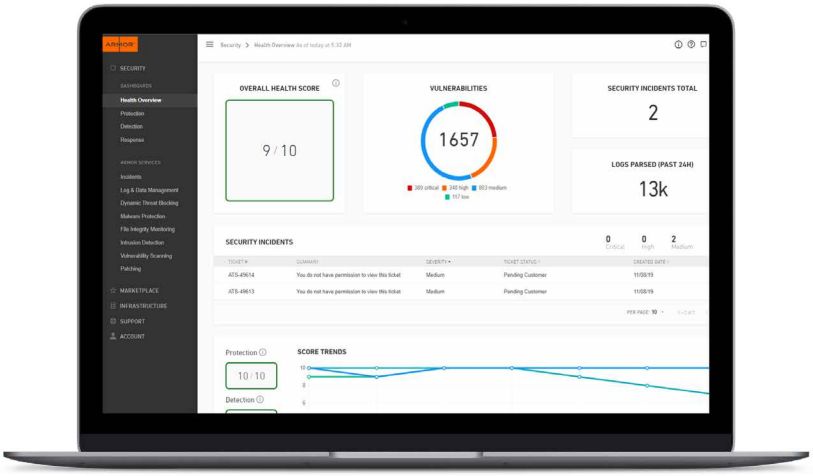
AVAILABLE CONFIGURATION OPTIONS

NUMBER OF CPUs				
2	4	8	12	16
MEMORY GB OPTIONS				
2	4	8	12	16
3	8	16	24	32
6	12	24	36	48
8	16	32	48	64
12	24	48	72	96
16	32	64	96	
	64			

AVAILABLE CONFIGURATION OPTIONS

NUMBER OF CPUs					
1	2	4	8	12	16
MEMORY GB OPTIONS					
2	2	4	8	12	16
4	4	8	16	24	32
6	6	12	24	36	48
8	8	16	32	48	64
	12	24	48	72	96
	16	32	64	96	
		64			

ARMOR MANAGEMENT PORTAL



The Armor Management Portal (AMP) supports:

Chrome Firefox Internet Explorer Safari

ARMOR API

Armor offers a RESTful HTTP service called the Armor API. This API system allows you to fully access the Armor Management Portal (AMP) via JSON data formats, which allows you to programmatically manage elements of your AMP account. For more information on the Armor API, visit developer.armor.com

COMPLIANCE

Armor Anywhere simplifies adherence to major compliance such as PCI DSS, HIPAA/HITRUST, and ISO 27001 by addressing several key controls for each framework. For information on specific compliance controls addressed by Armor Anywhere, read Armor Anywhere Compliance Matrix or Armor Anywhere with Secure Hosting Compliance Matrix.

Armor holds the following certifications and designations:

- PCI DSS Level 1-Certified
  (Highest attainable)
- HITRUST CSF-Certified
  (to demonstrate HIPAA compliance)
- ISO/IEC 27001-Certified
- SSAE 18 Certification
- Privacy Shield Framework

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167