ARMOR ANYWHERE

TECHNICAL SOLUTIONS BRIEF

WE PROTECT YOUR APPLICATIONS AND DATA, ANYWHERE.

ARMOR

INTRODUCTION

Armor Anywhere integrates enterprise-grade 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

REMOTE ENVIRONMENTS

ARMOR ANYWHERE

24/7/365 Monitoring and Response

Cloud Workload Protection	■ Host-Based IDS/IPS ■ File Integrity Monitoring ■ Vulnerability Scanning ■ Malware Protection ■ Recommendation Scan
Cloud Security Posture Management	■ Public Cloud Compliance Assessment
Endpoint Detection and Response	■ Next-Gen Antivirus ■ Behavioral Anomaly Detection ■ Containment
Log and Data Management	■ Cloud-Native Logs ■ Third-Party Logs

Cloud Security Platform

Unified Management and 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.

Streamlined 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.

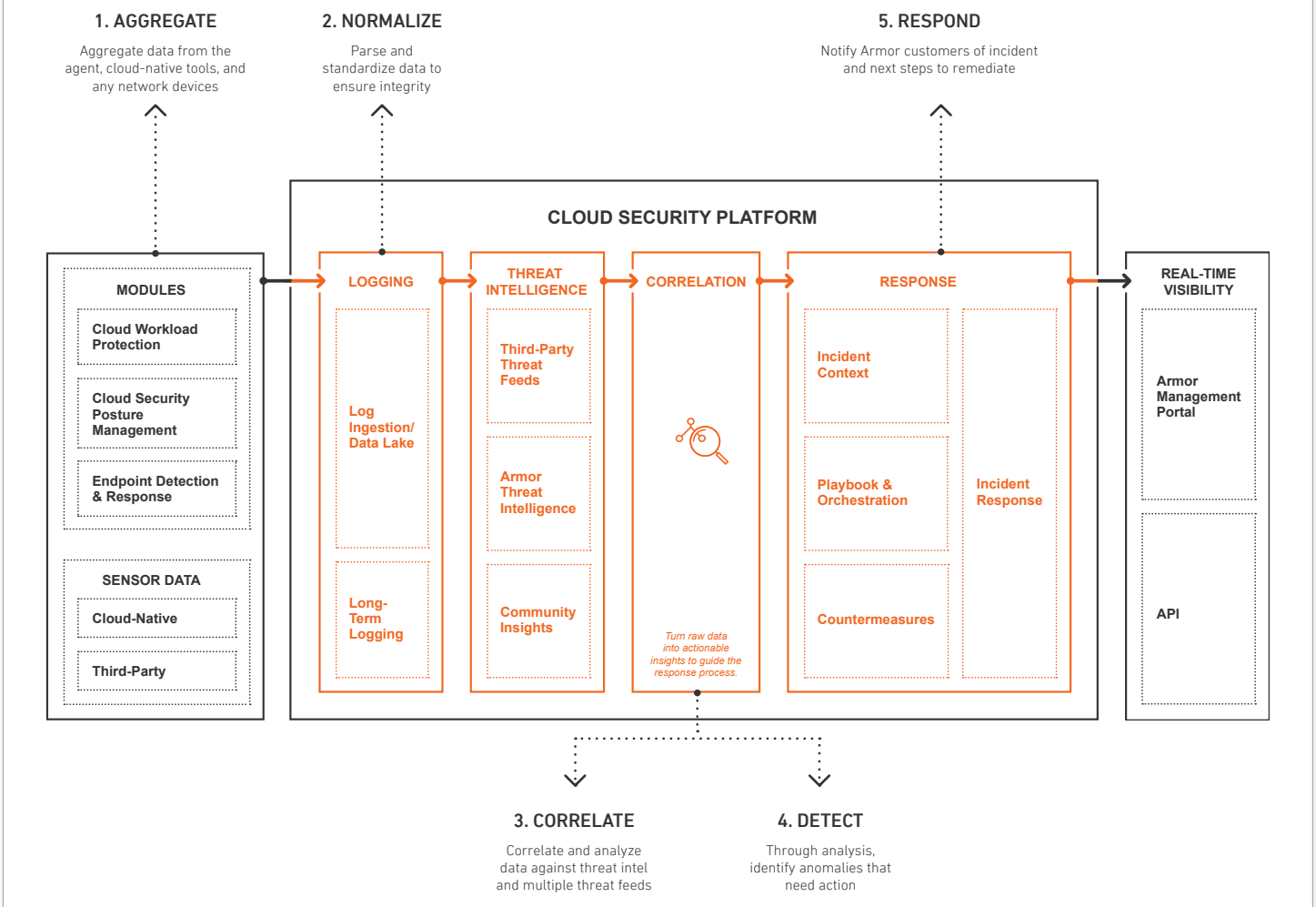
ARMOR ANYWHERE FOR ANY ENVIRONMENT

Armor Anywhere secures your application and data across your endpoint, server, network, and cloud environments. Combined with our high-performance hosting infrastructure, Armor also offers a secure and compliant, virtual private cloud environment for customers who have mission-critical and sensitive applications.

CLOUD SECURITY PLATFORM WITH UNIFIED VISIBILITY

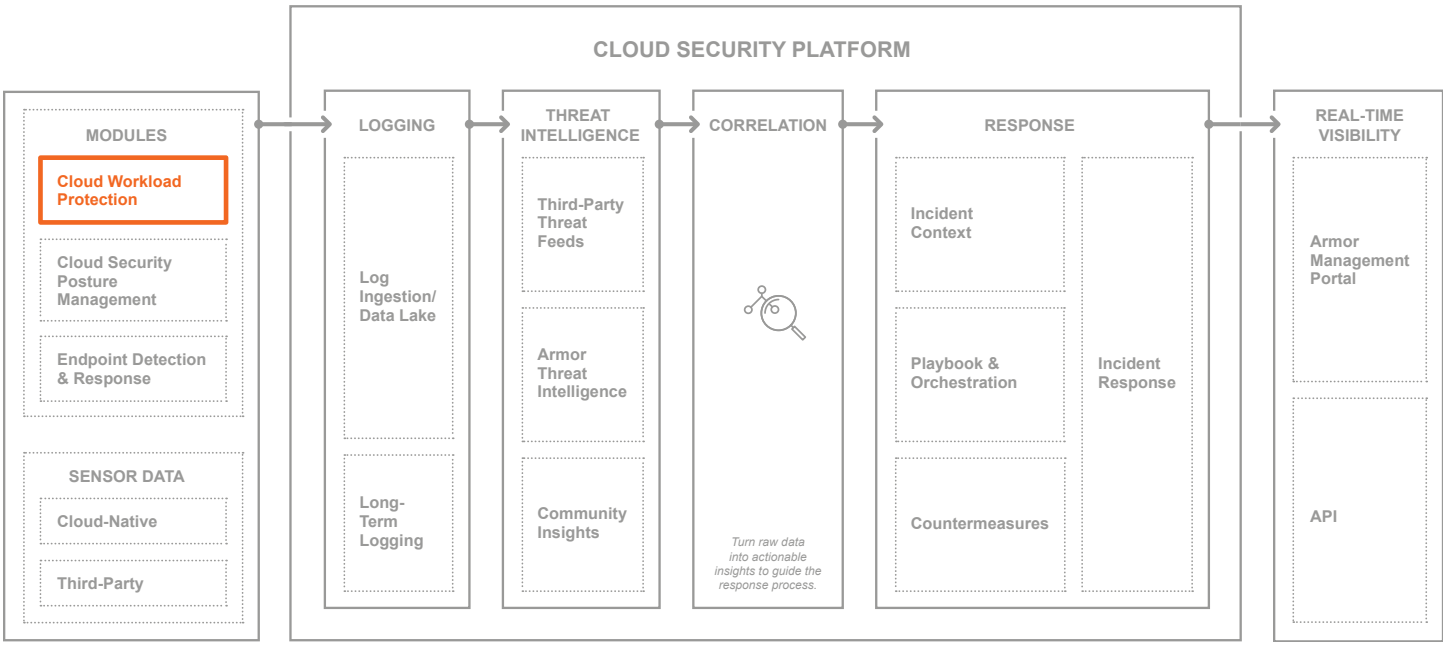
The Armor cloud security platform is the industry's leading threat detection and response platform. The platform integrates threat intelligence, advanced analytics, and incident response capabilities into a single platform that bolsters your defenses, uncovers threats, and prevents security breaches. 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



CLOUD WORKLOAD PROTECTION

Armor's cloud workload protection is delivered through the Armor Anywhere agent. The 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 cloud workload protection capabilities:

HOST-BASED INTRUSION DETECTION/INTRUSION PREVENTION SYSTEM (IDS/IPS)

Installed on a host, IDS/IPS analyzes network or host traffic and identifies if that traffic matches signatures of known attacks. 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 (FIM)

FIM 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.

FIM 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 Armor Management Portal (AMP), 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. Armor also provides an option to scan public cloud container images, allowing you to detect and address vulnerabilities early in the software development lifecycle. With Armor, organizations can adopt a Secure Left™ approach for early stages of development to strengthen overall security posture.

POLICY RECOMMENDATION SCANS

With recommendation 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, for example.

SUPPORTED OPERATING SYSTEMS

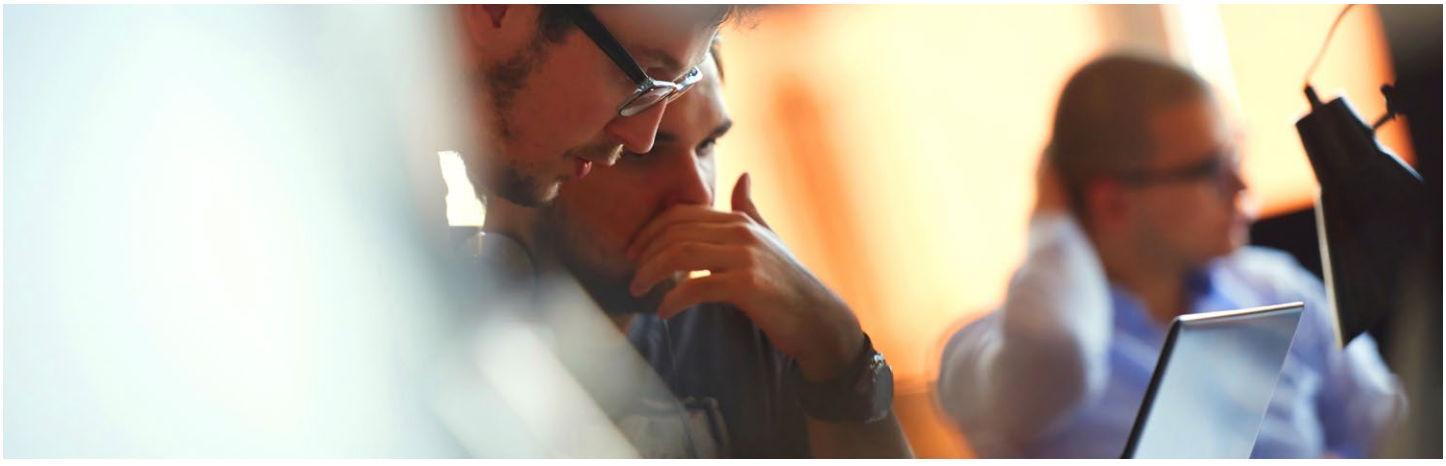
CENTOS	■ 6.X ■ 7.X
RED HAT ENTERPRISE LINUX (RHEL)[1]	■ 6.X ■ 7.X
UBUNTU	■ 16.04 ■ 18.04
AMAZON LINUX[1]	■ 2015.03 ■ 2015.09 ■ 2016.03 ■ 2016.09 ■ 2017.03 ■ 2017.09 ■ 2018.03 ■ Amazon Linux 2
ORACLE LINUX[1]	■ 6.X ■ 7.X

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.

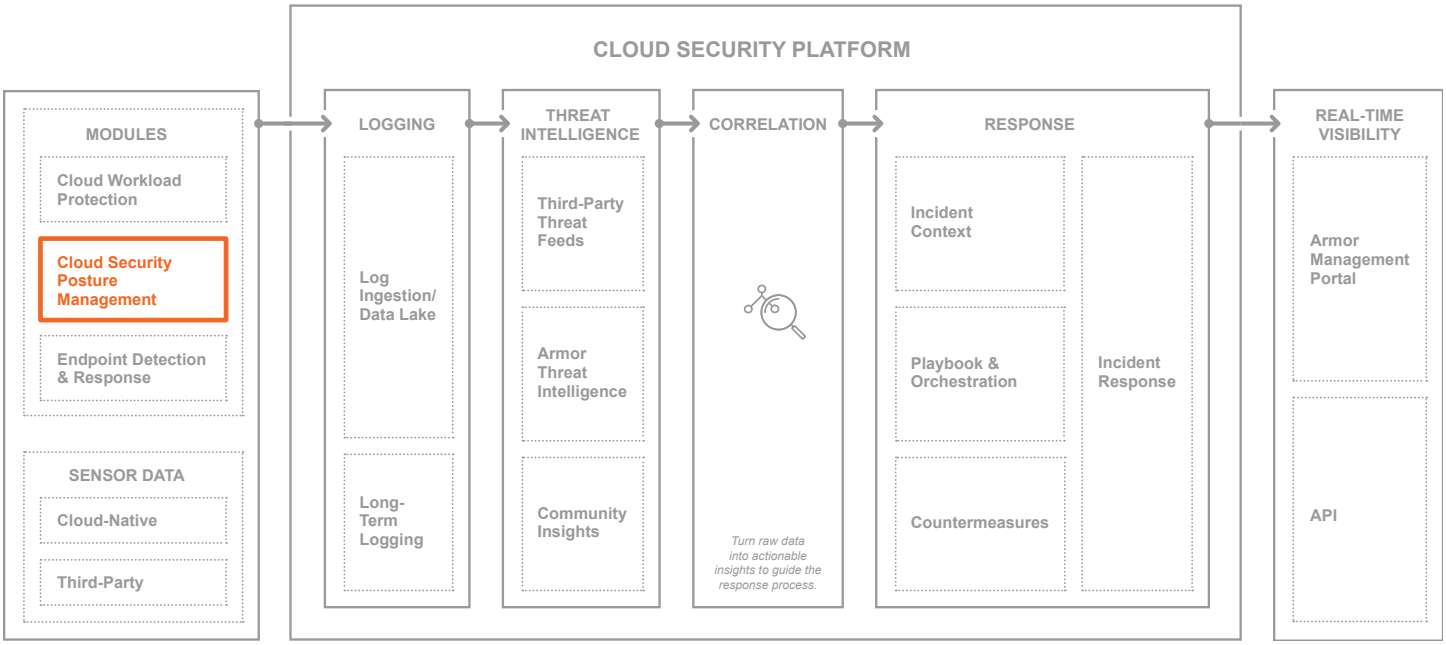
DEVOPS SUPPORT

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



CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

The cloud security posture management (CSPM) module of Armor Anywhere enables you to monitor the security posture of your public cloud infrastructure and helps you remain compliant against major mandates such as PCI, HIPAA, and CIS Benchmarks. Quickly identify and receive direction to remediate accidental risks through the Armor Management Portal.



CSPM uses cloud connectors to establish connection with your public cloud account. Cloud connectors use application programming interfaces (APIs) to aggregate data from your accounts without interfering with your public cloud service. It builds an inventory of the cloud account with detailed metadata and relationship mapping used for subsequent analysis. It discovers and aggregates your assets and resources from one or multiple cloud providers.

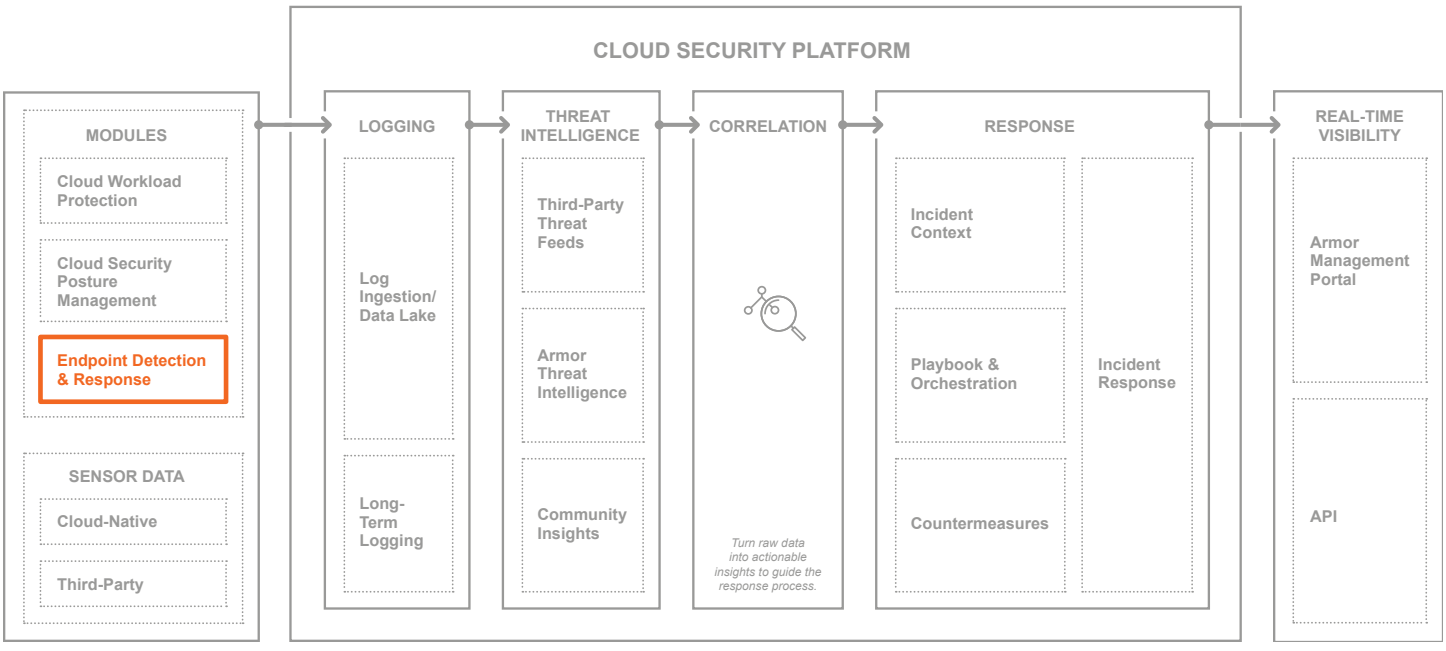
CSPM supports the following cloud environments: AWS, Microsoft Azure, and GCP.

ASSETS & RESOURCES		
AWS	**AZURE**	**GCP**
■ Auto Scaling Group ■ EBS Volume ■ IAM User ■ Instance ■ Internet Gateway ■ Lambda Function ■ Load Balancer ■ Network ACL ■ RDS ■ Route Table ■ S3 Bucket ■ Security Group ■ Subnet ■ VPC	■ Function App ■ Network Security Group ■ Resource Group ■ SQL Server ■ SQL Server Database ■ Virtual Machine (Virtual Machines created using Resource Manager only) ■ Virtual NetworkWeb App (App Service)	■ Cloud Functions ■ Firewall Rules ■ Networks ■ Subnetworks ■ VM Instances

MANDATES ADDRESSED BY CSPM				
■ PCI DSS ■ HIPAA	■ FedRAMP ■ CIS Benchmark	■ ISO 27001 ■ NIST	■ GDPR ■ NERC CIP	■ ASD 8 ■ And more

ENDPOINT DETECTION & RESPONSE (EDR)

The endpoint detection and response (EDR) module helps you quickly detect and stop advanced threats across your distributed endpoint. Armor has integrated VMware Carbon Black into its solution. EDR is agent-based and is installed through the Armor Anywhere agent on laptops, desktops, and servers, giving you a detailed view of your endpoint activities.



SUPPORTED OPERATING SYSTEMS

WINDOWS

CARBON BLACK CLOUD	OPERATING SYSTEM (x86, x64)	OS VERSION
3.5+	Windows 10 20H1	v19041.208
3.4+	Windows 10 19H2	v1909
3.4+	Windows 10 19H1	v1903
3.2.1 — 3.5.0	Windows 10 October 2018 Update	v1809
	Windows Server 2019	
2.1.0 — 3.5.0	Windows 10 April 2018 Update	v1803
	Windows 8.1	SP0, Update 1, Update 2
	Windows 8	SP0
	Windows Server 2016	SP0
	Windows Server 2012 R2	SP0
	Windows Server 2012	SP1
	Windows Server 2008 R2	SP0, SP1
2.1.0 and 3.1.0	Windows Server 2008	SP2

LINUX

CARBON BLACK CLOUD	OPERATING SYSTEM (x86, x64)
2.7.0 - 2.8.0	RHEL/CentOS 7.0 - 7.8
	RHEL/CentOS 6.6 - 6.10
2.5.0 - 2.8.0	Ubuntu 16 & 18
	SUSE SLES 12 & 15
	Amazon Linux 2

MACOS

CARBON BLACK CLOUD	OPERATING SYSTEM
3.5.1	10.13 (High Sierra)
	10.14 (Mojave)
	10.15 (Catalina)
	11 (Big Sur)

- macOS 10.15 (Catalina) devices installed with macOS sensors 3.3.3+ may require a reboot.
- macOS 10.13+ devices installed with macOS sensors 3.1+ require new Apple KEXT approval. Unapproved sensors will enter bypass mode.

SYSTEM REQUIREMENTS

HARDWARE

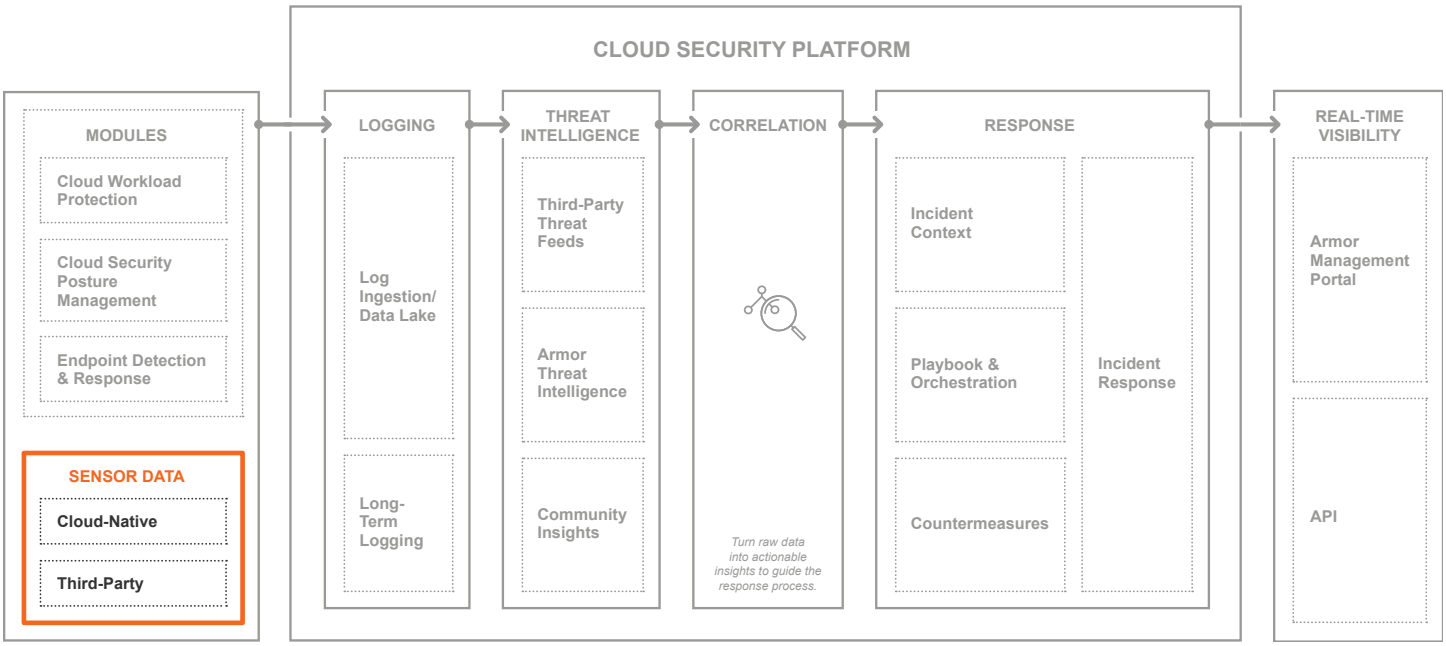
- CPU: 2GHz multi-core
- RAM: 2GB
- Disk Space: 500MB
- +600MB if local scanning is enabled or using ThreatHunter
- Network Card: 100/1000 mbps
- Additionally, Linux systems need 100 MB free space on the /opt partition and 4.1 GB free on the /var partition.

NETWORK

- TLS: 1.2 or later
- Minimum Network used during light usage is 1k bytes/sec read/writes each
- Primary port 443 and fail over port 54443
- Firewall or proxy should be configured with a bypass rule to allow outgoing connections over TCP/443 as well as Carbon Black Cloud's alternate port TCP/54443.

LOG & DATA MANAGEMENT

The log and data management module delivers correlated events 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.



Armor collects logs from the following sources:

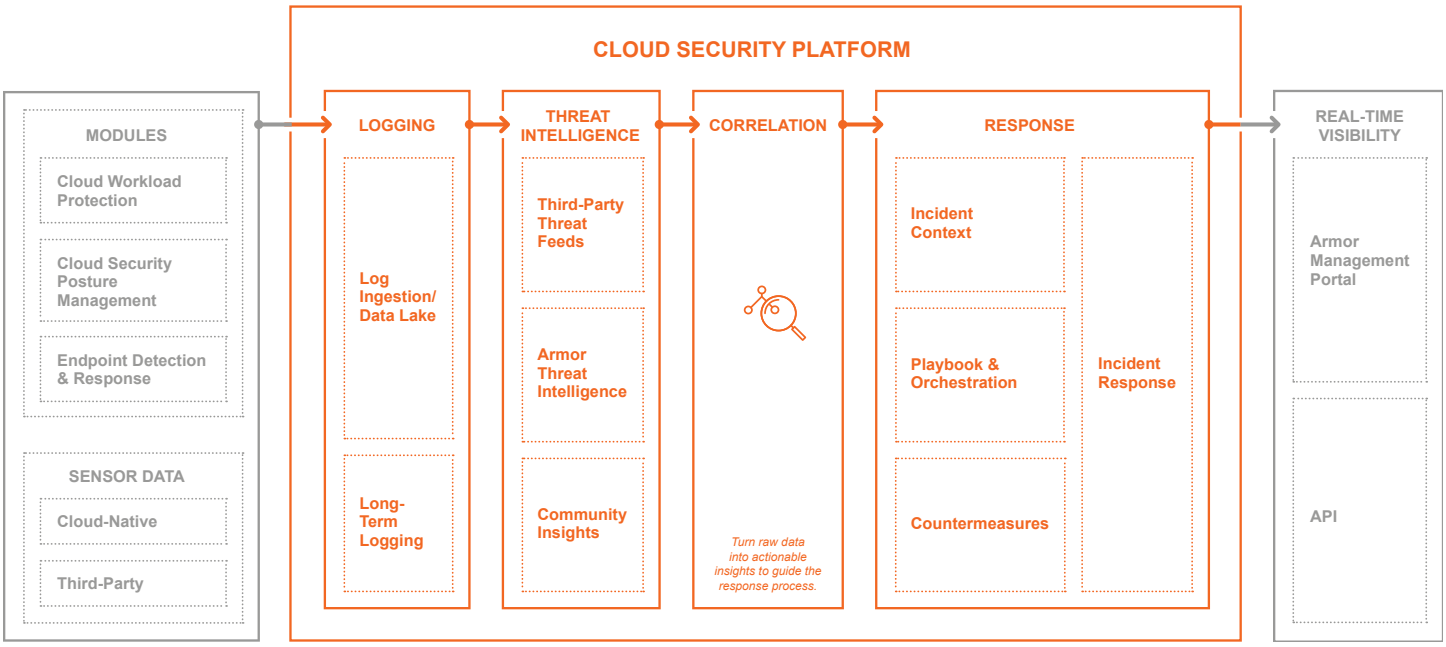
LOG TYPES		
AGENT LOGS	**CLOUD-NATIVE SOURCES**	**THIRD-PARTY SOURCES**
The capability natively supports logs coming from Armor's core security capabilities including IDS, file integrity monitoring, malware protection, vulnerability scanning, and operating system logs.	Armor can ingest, analyze, and 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.

SECURITY LOG COLLECTOR

Logs are collected either through API or through the security log collector into the cloud security platform. Log sources utilizing the security log collector will need to be configured and uploaded via syslog (TCP/UDP), and then sent through a device-specific port.

CLOUD SECURITY PLATFORM

Armor's cloud security platform integrates a robust data lake; security information and event management (SIEM); threat intelligence; logging and storage; and security orchestration, automation, and response (SOAR). The cloud security platform takes in syslogs, cloud-native logs, and other raw log forms, and then parses and normalizes them to ensure integrity. Once these logs are normalized, the platform automatically correlates the logs against Armor's threat intelligence and subscribed third-party feeds through the SIEM. With this process, Armor can identify any indicators of compromise (IOC) in your environment. With Armor's SOAR, we have created custom playbooks to more quickly respond to events identified. The SOAR streamlines the security operations with data aggregation, highly automated incident workflow, and response playbooks. All your data in the data lake are made available to you for further analysis and storage.



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 Anywhere 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

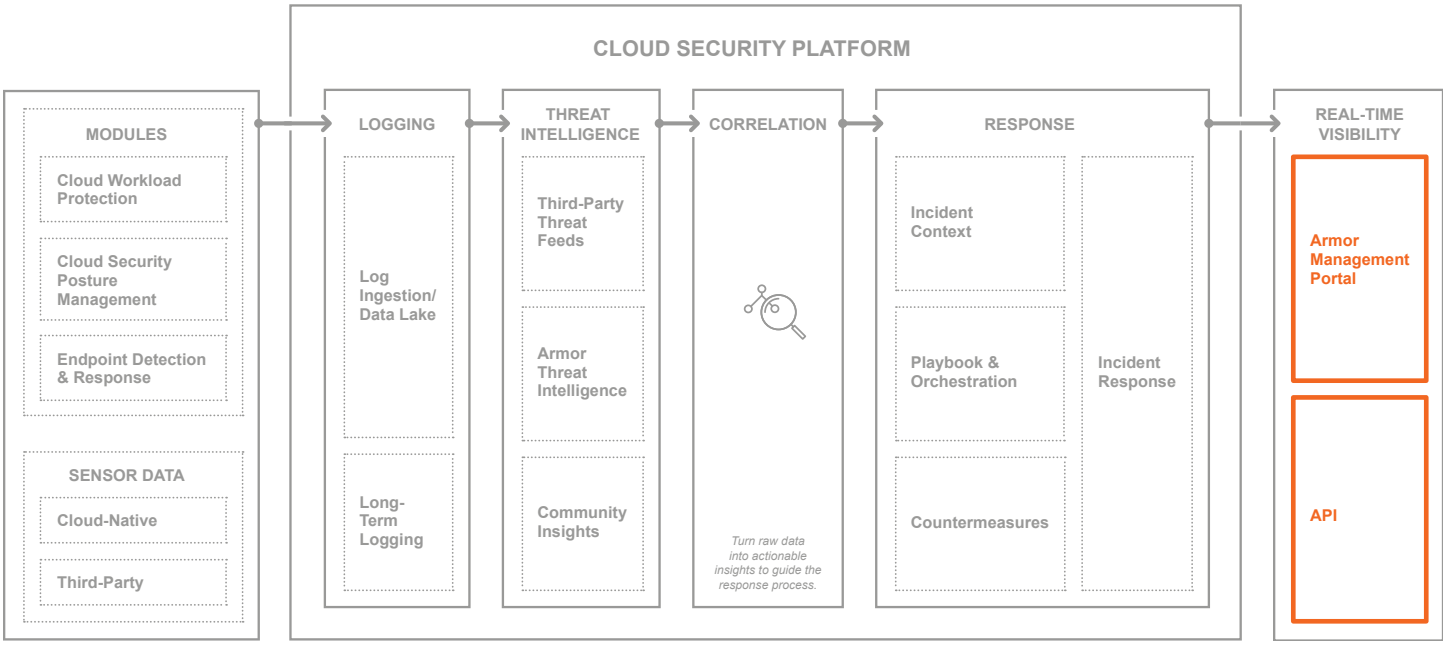
- 2 CPU Cores
- 2 GB RAM
- 3 GB Disk Space

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 MANAGEMENT PORTAL (AMP) & API



ARMOR MANAGEMENT PORTAL (AMP)

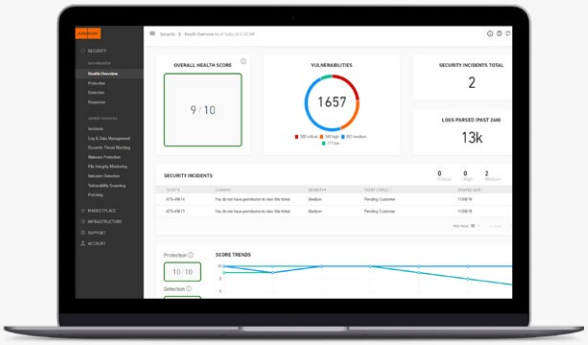
AMP supports:

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 AMP via JSON data formats, which enables you to programmatically manage elements of your AMP account. Armor uses ADFS and OAUTH workflow for the portal and API authentication. By presenting a retrieved Bearer id_token to the API, you can leverage the API documentation to access all API endpoints. For more information on the Armor API, visit developer.armor.com

ARMOR'S PRIVATE CLOUD

For compliance-conscious organizations that don't want to maintain infrastructure but have sensitive data and applications, Armor has a fully managed and monitored, high-performance private cloud secured with Armor Anywhere.

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

- 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: Linux servers require a minimum of 1 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			

NETWORK PROTECTION

WEB APPLICATION FIREWALL (WAF)

A WAF provides protection from layer 7 attacks targeted at a customer's applications such as cross-site scripting, directory traversal, and SQL injection. WAFs filter and monitor HTTP traffic between a web application and the internet.

INTERNET PROTOCOL REPUTATION MANAGEMENT (IPRM)

IPRM utilizes threat intelligence from Armor's Threat Resistance Unit (TRU) to filter and block traffic from malicious or suspicious IP addresses. Armor maintains a database of blacklisted IPs collected from Armor's TRU team and other third-party security partners. Customers can look up IPs within Armor's Management Portal and either whitelist or blacklist those IPs.

ADDITIONAL CONFIGURATIONS

BACKUP SERVICE

Flexible backup solution with simple recovery options is fully supported by Armor.

DISASTER RECOVERY

Ensure business continuity by enabling continuous data replication between two physical Armor locations.

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, see compliance matrix for Armor Anywhere or compliance matrix for Armor's private cloud.

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