ARMOR LOG MANAGEMENT

CORE CAPABILITY

Device logs are a valuable resource for insights on potential threats for security teams. Unfortunately, security personnel are often too busy to perform log reviews and analysis of log data due to the volume of logs and competing priorities. Security teams need to simplify the collection and long-term storage of logs for compliance while performing crucial analysis and correlation of log data to enhance their overall security posture.

CLOUD-DELIVERED LOG MANAGEMENT AND ANALYSIS

Armor Log Management simplifies the collection, storage and analysis of logs for potential threats, helping you meet compliance while enhancing your security posture. Effective log management is both a major compliance requirement as well as best practice in threat detection and remediation. With Armor Log Management, powered by our Spartan threat prevention and response platform, Armor helps your organization meet compliance while performing analysis and correlation of your log data to identify potential threats and eliminate risk to your organization.

ARMOR LOG MANAGEMENT:

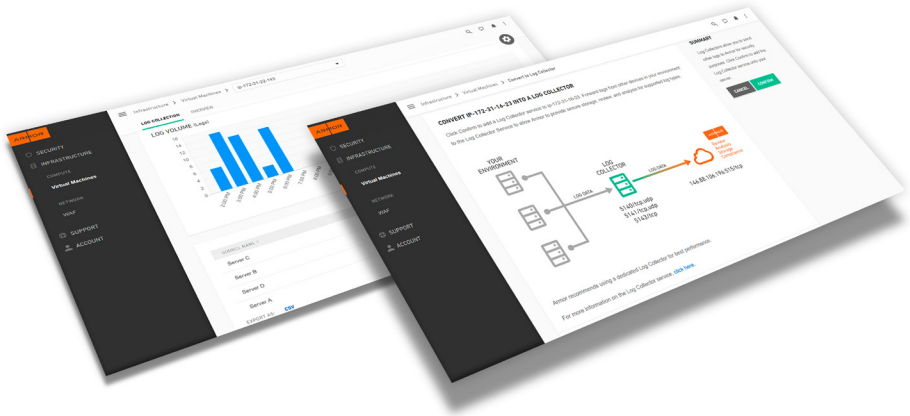
- Send Armor logs from any device from anywhere within your IT environment.
- Correlate and analyze log data to identify threats that may pose risk to your organization.
- Store log information for up to 13 months in compliance with applicable mandates.
- Get Audit-Ready Compliance Support for PCI, HIPAA, HITRUST, GLBA, GDPR and other compliance requirements.
- Access battle-tested security and compliance talent on-demand.
- Pay for what you use while avoiding the need for additional hardware.

HOW IT WORKS

Armor will ingest and store as many logs for you as you would like. Armor Log Management is usage-based allowing you to optimize your investment and pay only for how much you use.

Armor's Log Management natively supports logs coming from Armor's core security services (FIM, Malware Prevention, IDS, etc.), AWS CloudTrail logs and device logs such as from network appliances, web application firewalls, application logs and many more.

Armor Log Management, through our Spartan platform, delivers correlated events with additional flexible tuning options to minimize "noise" and increase fidelity of detection and alerting for your environment.



AUDIT-READY COMPLIANCE

Meet PCI, HIPAA, HITRUST, GLBA, GDPR and other compliance requirements related to storage and analysis of log information. Get audit-ready reporting capabilities through the Armor Management Portal.

POWERFUL ADVANCED ANALYTICS AND CORRELATION

Perform advanced analysis and correlation of logs to detect threats that may pose risk and be present in your environment. Enhance your security posture while offloading the burdens associated with log management and analysis.

UNIFIED PROTECTION AND VISIBILITY

Collect, manage and analyze logs from anywhere in your environment whether on-premise, cloud or hybrid. Correlate log information with other event data collected from your environment as an Armor customer.

SIMPLE AND FAST TURN-UP

Turn up Armor's Log Management service in just minutes through a simple 3-step process within the Armor Management Portal.

FEATURES

RAPID TURN-UP

- Easy turn-up of log collection in minutes
- DevOps supported/DevOps approved

LOG STORAGE AND RETENTION

- Up to 13 months of log storage available
- Storage of incident-related analysis and data

ADVANCED ANALYTICS AND CORRELATION

- Performed by Armor Spartan threat prevention and response platform
- Advanced analytics and correlation capabilities applied to log and other collected data
- Detection of malicious activity
- Rule-based automatic alerting
- Available onboarding for parser and custom rules development

CLOUD-DELIVERED MANAGED SECURITY SERVICES

- 24x7 Security Operations Center staffed by expert security analysts
- Continuous and automated response to eliminate threats
- Continuous threat hunting to uncover hidden threats

VISIBILITY AND REPORTING

- Visibility and access to logs via the Armor Management Portal (AMP)
- View of daily log volume by hour, sources, events per source and top sources by index size and EPS calculations
- Robust search and filtering capabilities

COMPLIANCE

- Support for PCI, HIPAA, HITRUST, GLBA, GDPR and other compliance requirements
- Audit-ready reporting
- Storage for incident-related analysis and data

POWERED BY SPARTAN

Advanced analysis and correlation of logs are powered by Spartan, the industry's leading threat prevention and response platform that outthinks and outpaces threats at the speed of cloud. Spartan integrates advanced analytics, global threat intelligence, and continuous response capabilities into a single solution that bolsters your defenses, uncovers hidden threats, and prevents security breaches. Customers can tap into the power and value of Spartan through the Armor Management Portal.

ARMOR

ARMOR HOLDS THE FOLLOWING CERTIFICATIONS AND DESIGNATIONS:

- PCI DSS Level 1-Certified (Highest attainable)
- HITRUST CSF-Certified (Certified for HIPAA Compliance)
- ISO/IEC 27001 (2013) Certified
- SSAE16 Certification
- Privacy Shield Framework

HIPAA COMPLIANCE | HITRUST | PCI Security Standards Council

PROTECT ANY ON-PREMISE, CLOUD OR HYBRID ENVIRONMENT, ANYTIME, ANYWHERE.

Securing your company and getting complete visibility across your IT ecosystem shouldn't be so hard. Collect, store and analyze logs from virtual appliances, applications, PaaS solutions, containers and other devices in the environment (on-premise, cloud and hybrid IT).

ARMOR