ARMOR ANYWHERE | TECHNICAL SOLUTION BRIEF

ARMOR ANYWHERE—SECURITY AS A SERVICE

With new demands placed upon IT from business leaders, security teams must be able to accelerate go-to-market for their efforts to secure IT initiatives and the future of their businesses. A new security approach is required, one that accelerates security teams’ ability to deploy new protections quickly and effectively across a fluid IT environment, accelerates compliance, and greatly reduces the common challenges associated with siloed IT environments and data.

Introducing Armor Anywhere. Armor Anywhere delivers protection in minutes, audit-ready compliance, unifying visibility, and control across your entire IT landscape. Armor Anywhere fortifies and unifies your on-premise, cloud, and hybrid IT security defenses to enable you to detect and respond to cyberthreats in real-time and at a fraction of the cost of traditional solutions.

**Armor Anywhere boosts your security by providing:**

1. **Unified Protection & Visibility**
   Get a consolidated view into the security health of your on-premise, cloud, and hybrid IT infrastructure, as Armor collects and analyzes logs and events from firewalls, servers, operating systems (OS), and other applications throughout your environment.

2. **Audit-Ready Compliance**
   With security controls mapped to compliance mandates such as PCI DSS, HIPAA, HITRUST, and GDPR, Armor Anywhere accelerates compliance for customers.

3. **Continuous Detection & Response**
   Combine best-of-breed security tools and threat intelligence with the expertise of our Threat Resistance Unit (TRU) and security operations center (SOC) to speed threat detection and incident response.

4. **Swift & Scalable Deployment**
   Deploy 24/7/365 security in minutes with our lightweight agent (no hardware needed).

**HOW IT WORKS**

**ARMOR ANYWHERE AGENT**

The Armor Anywhere service uses a powerful agent installed across your on-premise, cloud, or hybrid environments. The Armor Anywhere agent uses best-of-breed security capabilities to secure your environment. Once installed, the Armor Anywhere agent defends your environment at the host level, monitoring inbound and outbound traffic, gathering logs, monitoring changes to critical files, and providing customers with security status and updates. The Armor Anywhere agent is lightweight and can be deployed in minutes.

Security results from the Armor Anywhere agent provide valuable data to Armor's SOC, where our experts manage and secure your systems and workloads—monitoring both inbound and outbound traffic at the host—and identify malicious threats in real-time to enable quick response and containment before larger issues occur.

The Armor Anywhere agent is lightweight and can be deployed in the following, but not limited to, on-premise cloud, and hybrid IT environments:
SECURITY CAPABILITIES

INTRUSION DETECTION
With visibility to inbound and outbound activity at the host, Armor inspects anomalous traffic against predefined policies—detecting attacks like generic SQL injections, generic XSS attacks, DoS, and generic web app attacks. This service provides an agent-based IDS on the installed host for network traffic analysis and reporting based on policies defined by Armor.

FILE INTEGRITY MONITORING
FIM is designed to monitor critical system file locations and alert you when your files have changed. It monitors critical operating system (OS) files for changes that may allow threat actors to control your environment. FIM uses OS-specific policies and provides Armor log visibility to assist in reviewing security events.

MALWARE PROTECTION
Armor protects your environment from harmful malware and botnets deployed to capture your data, monitor your activity, or use your servers for illicit activity. In the event an alert is created, Armor’s threat analysts begin an in-depth investigation. Armor uses an enterprise-class malware protection application and deploys the application agent within the Armor agent.

LOG & DATA MANAGEMENT
Log & Data Management captures agent logs and stores them for 30 days. Additionally, customers can ingest, analyze, and store additional logs from cloud native and other third party sources for up to 13 months.

VULNERABILITY SCANNING
Armor scans for potential points of risk to help reduce the surface area of attack. Weekly scheduled scans provide you a visible audit report to identify the vulnerabilities that attackers could use to penetrate your network, so you can develop your remediation plan.
THE SHARED RESPONSIBILITY MODEL & ARMOR ANYWHERE

Public clouds like Amazon Web Services (AWS) and Microsoft Azure are effective for raw infrastructure, but public cloud customers are still tasked with managing and securing data workloads. Armor reduces the burden of these challenges for your organization by sharing both risk and responsibility. Purpose-built to achieve a secure and compliant posture for your data, Armor Anywhere makes it easy to balance security, cost-effectiveness, and cloud agility. The shared responsibility model means that you too are responsible for securing your IT environment, supplementing your cloud provider and its security controls. Security is a shared responsibility between client and cloud provider.

COMPLIANCE WITH PCI DSS, HIPAA, HITRUST CSF, AND GDPR

Armor Anywhere creates a turnkey security program designed with compliance requirements in mind to include PCI DSS, HIPAA, HITRUST CSF, and GDPR. We help you accelerate your compliance processes and help you meet your compliance requirements whether you have payment data, ePHI, or PII while reducing the burden of expensive audits.

Explore how Armor Anywhere security solutions and services aligns with various compliance requirements and regulations.

Learn More>
POWERED BY ARMOR CLOUD SECURITY PLATFORM

Armor Anywhere is powered by Armor cloud security platform—the IT security industry’s leading threat prevention and response platform. Armor integrates advanced analytics, global threat intelligence, and continuous response capabilities into a single platform that bolsters your defenses, uncovers hidden threats, and prevents security breaches. Whether your sensitive data and workloads are stored in a private, public, or hybrid cloud—or in an on-premise IT environment—cloud security platform provides a proactive approach to cyberthreats.

Our solutions are designed from the ground up to be scalable, deployable, and manageable in diverse environments, providing unparalleled monitoring, protection, detection, and response capabilities to boost security and reduce the dwell times of attackers.

One major component of Innovum’s security posture is Armor Anywhere. Innovum needs to provide the active, around-the-clock monitoring that is required when storing sensitive personal data in a database, it needs to react quickly to any suspicious activity.

— Innovum

Armor Anywhere takes risk off our plate, especially when it comes to maintaining PCI compliance. The shared responsibility between BraveSoft and Armor minimizes the time and energy I have to spend to remain compliant. And that’s what we love about it.

— Thomas Wood | CTO, BraveSoft
WHAT CLOUD SECURITY PLATFORM DOES

5 BILLION + EVENTS PER MONTH

- Tool-based detection & prevention
- Application of threat intelligence
- Advanced analytics & correlation
- Qualified security outcomes

Countermeasures

Armor averages 1/100th of industry dwell time

Armor Threat Resistance Unit (TRU)

Security Operations Center (SOC)

Suspicious
Requires human interaction for further investigation

Known Bad

Known Good
Whitelisted IP addresses

Client Portal
SECURITY OPERATIONS CENTER COMPONENTS

Our Security Operations Center experts monitor your environment 24/7/365 for potential risk to your applications and data. Should we see something of concern, we go beyond alerting to help you respond to an incident.

Our Support options allow your teams to get the right level of engagement and value from Armor that your organization needs.

Armor security experts continually develop new countermeasures, analytics tools, and playbooks. They work to improve Armor’s threat detection as well as provide greater context for how to respond to threats to your private, public and hybrid cloud environments.

SECURITY ENGINEERING

Change to Armor’s security engineering team collaborates closely with Threat Resistance and Security Operations teams for the identification, prioritization and development of enhancements to the cloud security platform’s threat detection and response capabilities, as well as plays a pivotal role in countermeasure development.

SECURITY OPERATIONS CENTER EXPERTS

Change to Security Operations Center experts provide 24/7/365 threat monitoring for Armor customers. Going beyond simple alerting, Armor SOC experts provide expert guidance to customers on how best to respond to potential incidents.

THREAT RESISTANCE UNIT

The Threat Resistance Unit is Armor’s threat research arm focused on identifying new threat actor tactics, techniques and procedures and emerging threats, and turning that intelligence into real protections for Armor customers.
OVERALL HEALTH, PROTECTION, DETECTION, & RESPONSE SCORES

AMP is a single-pane-of-glass view into your security program, providing real-time visibility and management of your security controls. Through AMP, your organization gains access to powerful capabilities that speed threat detection and response, and provide critical insights that your security analysts need to make their jobs easier.

- **Security Analytics Dashboard:**
  With the security analytics dashboard, you have instant access to critical incidents requiring investigation and rapid response. You also can view a prioritized list of vulnerabilities based on severity and recommended actions.

- **Intrusion Detection:**
  AMP provides our users with a look at the telemetry data coming off our IDS.

- **Malware Protection Service Health:**
  View state of malware service engine and review previously detected malware items.

- **File Integrity Monitoring Status View:**
  AMP provides users with a look at the file names and descriptions of files on each host—and when and what types of changes are detected on those files based on our latest FIM scan.

- **Log & Data Management:**
  View up to 30 days of log events or select an option to access 13 months for regulatory requirements. Aggregating log information, including top sources by event ingestion and index size, are reported within AMP.

- **Vulnerability Scanning:**
  View vulnerability scanning results to identify risks and determine appropriate next steps for updating and patching.
SET UP

Operating System Support

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

![Supported Operating Systems](image)

DevOps Support

Armor provides install scripts for the Armor agent so you can integrate into your DevOps toolchains.

ONBOARDING & INSTALLATION

Armor provides step-by-step guidance on installing the Armor 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. The security results and logs also feed into Armor’s cloud security platform and data is translated into security policies applied to your environment. This crowd-sourced intelligence loop, combined with multiple channels of threat intelligence, blends to enhance the overall security protecting you from the latest threats.

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

API

Armor provides an API for organizations that prefer to directly integrate with their own systems and environment.

Learn More>

MINIMUM REQUIREMENTS

**Windows**

- 2GB RAM
- 2 CPU
- 3GB of free disk space

**Amazon Web Services (AWS)**

- 1GB RAM
- 1 CPU
- 3GB of free disk space