ARMOR

Armor | Anywhere

TECHNICAL SOLUTIONS BRIEF

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 under 2 minutes, audit-ready compliance, unifying visibility, and control across your entire IT landscape. Armor Anywhere is a managed security service that fortifies and unifies your on-premise, cloud, and hybrid IT security defenses to enable you to prevent, 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.

3 Audit-Ready Compliance

With security controls mapped to compliance mandates such as PCI DSS, HIPAA, HITRUST, and GDPR, Armor Anywhere accelerates compliance for customers.

2 Continuous Detection & Response

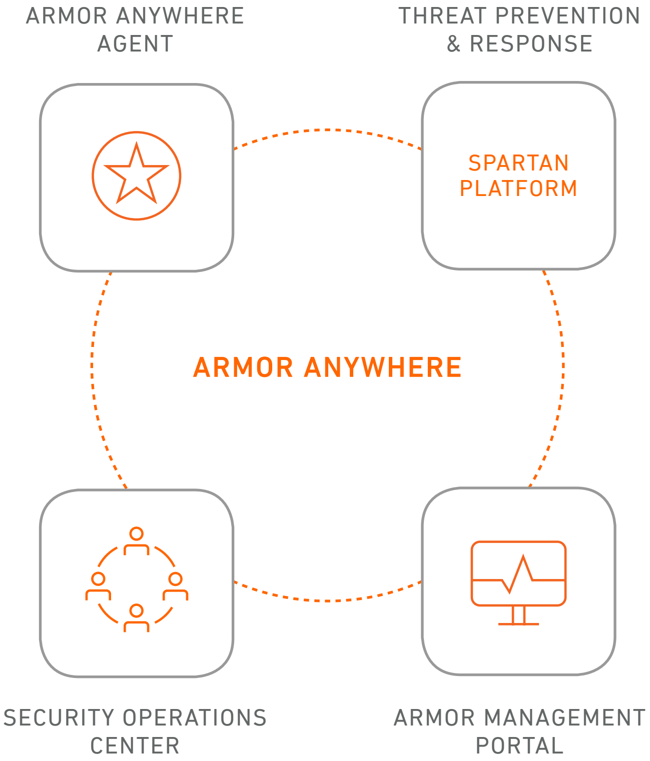
Combine best-of-breed security tools and threat intelligence with the expertise of our Threat Resistance Unit (TRU) and security operations center (SOC) to speed threat detection and incident response.

4 Swift & Scalable Deployment

Deploy 24/7/365 security in under 2 minutes with our lightweight agent (no hardware needed).

HOW IT WORKS

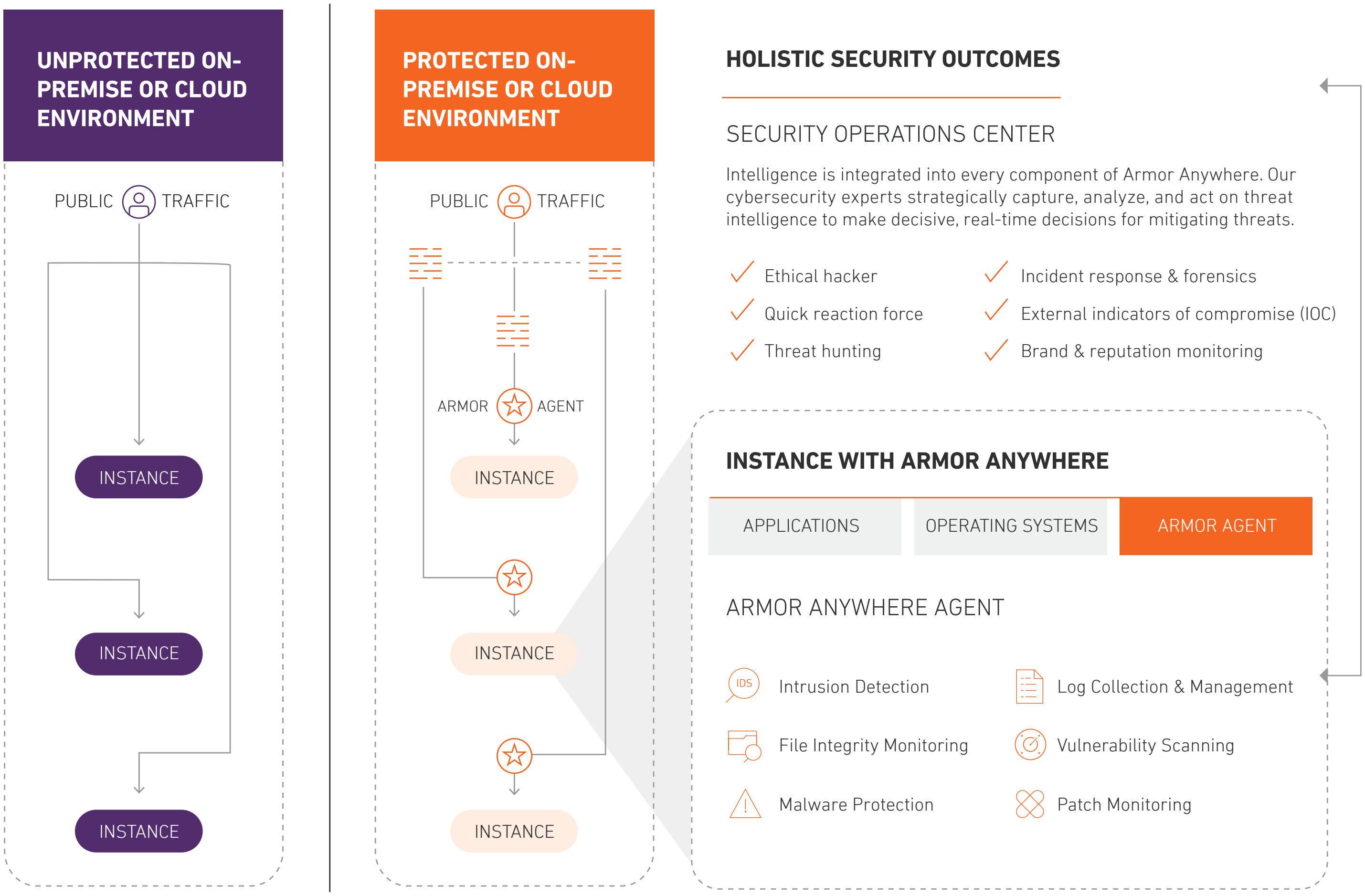
The Armor Anywhere security-as-a-service (SECaaS) comprises four key components: Armor Anywhere agent, Spartan threat prevention and response platform, SOC, and Armor mnagement portal (AMP).



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 patch status and updates. The Armor Anywhere agent is lightweight and can be deployed in under 2 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.



HOLISTIC SECURITY OUTCOMES

SECURITY OPERATIONS CENTER

Intelligence is integrated into every component of Armor Anywhere. Our cybersecurity experts strategically capture, analyze, and act on threat intelligence to make decisive, real-time decisions for mitigating threats.

- ✓ Ethical hacker
- ✓ Quick reaction force
- ✓ Threat hunting
- ✓ Incident response & forensics
- ✓ External indicators of compromise (IOC)
- ✓ Brand & reputation monitoring

INSTANCE WITH ARMOR ANYWHERE

APPLICATIONS | OPERATING SYSTEMS | ARMOR AGENT

ARMOR ANYWHERE AGENT

- Intrusion Detection
- File Integrity Monitoring
- Malware Protection
- Log Collection & Management
- Vulnerability Scanning
- Patch Monitoring

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

aws | Google Cloud | PRIVATE CLOUD | HYBRID CLOUD | OTHER CLOUDS | ON-PREMISE INFRASTRUCTURE

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 MANAGEMENT

Log management captures, documents, analyzes, and reports on log events from firewalls, servers, OS logs, and other applications to determine their validity and severity. Clients can view 30 days of logs in the Armor management portal (AMP) and store up to 13 months of log events consistent with applicable regulatory requirements.

VULNERABILITY SCANNING

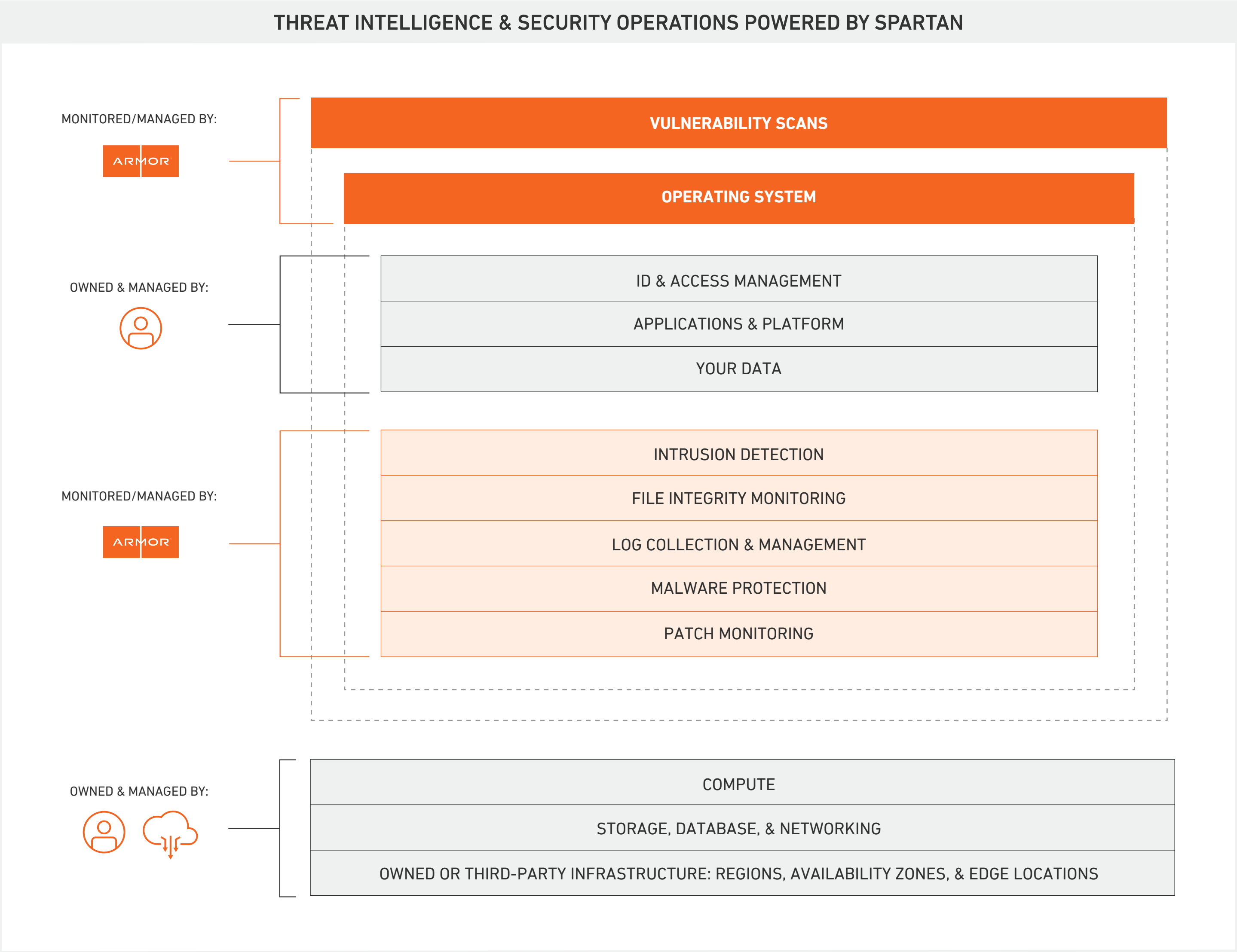
Armor scans for potential points of risk to help reduce the surface area of attack. Weekly scheduled scans provide you a visible audit report to identify the vulnerabilities that attackers could use to penetrate your network, so you can develop your remediation plan.

PATCH MANAGEMENT

Patch management provides visibility into your environment to identify critical OS-level patches for resolution. Armor provides you visibility into your environment running the Armor agent and coordinates software updates with your team so you can ensure your OS is consistently up to date.

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.



THREAT INTELLIGENCE & SECURITY OPERATIONS POWERED BY SPARTAN

MONITORED/MANAGED BY: ARMOR

VULNERABILITY SCANS

OPERATING SYSTEM

OWNED & MANAGED BY:

ID & ACCESS MANAGEMENT

APPLICATIONS & PLATFORM

YOUR DATA

MONITORED/MANAGED BY: ARMOR

INTRUSION DETECTION

FILE INTEGRITY MONITORING

LOG COLLECTION & MANAGEMENT

MALWARE PROTECTION

PATCH MONITORING

OWNED & MANAGED BY:

COMPUTE

STORAGE, DATABASE, & NETWORKING

OWNED OR THIRD-PARTY INFRASTRUCTURE: REGIONS, AVAILABILITY ZONES, & EDGE LOCATIONS

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

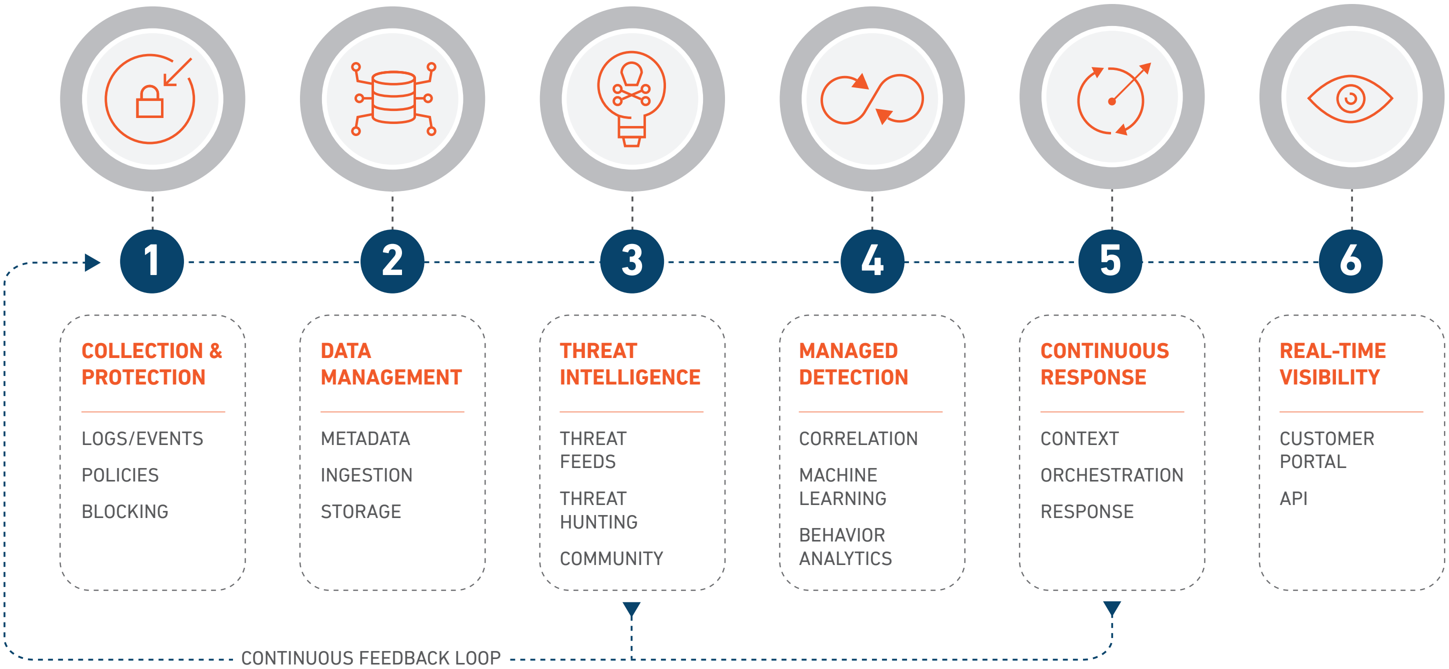
Armor Anywhere creates a turnkey security program designed with compliance requirements in mind to include PCI DSS, HIPAA, HITRUST CSF, and GDPR. We help you accelerate your compliance processes and help you meet your compliance requirements whether you have payment data, ePHI, or PII while reducing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

Explore how Armor Anywhere security solutions and services aligns with various compliance requirements and regulations. [Learn More>]

POWERED BY SPARTAN THREAT PREVENTION & RESPONSE PLATFORM

Armor Anywhere is powered by Spartan—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—Spartan provides a proactive approach to cyberthreats.

The Spartan platform is the connective tissue between Armor Anywhere, our SOC analysts, the Threat Resistance Unit (TRU), and AMP. 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.



1 **COLLECTION & PROTECTION**

LOGS/EVENTS

POLICIES

BLOCKING

2 **DATA MANAGEMENT**

METADATA

INGESTION

STORAGE

3 **THREAT INTELLIGENCE**

THREAT FEEDS

THREAT HUNTING

COMMUNITY

4 **MANAGED DETECTION**

CORRELATION

MACHINE LEARNING

BEHAVIOR ANALYTICS

5 **CONTINUOUS RESPONSE**

CONTEXT

ORCHESTRATION

RESPONSE

6 **REAL-TIME VISIBILITY**

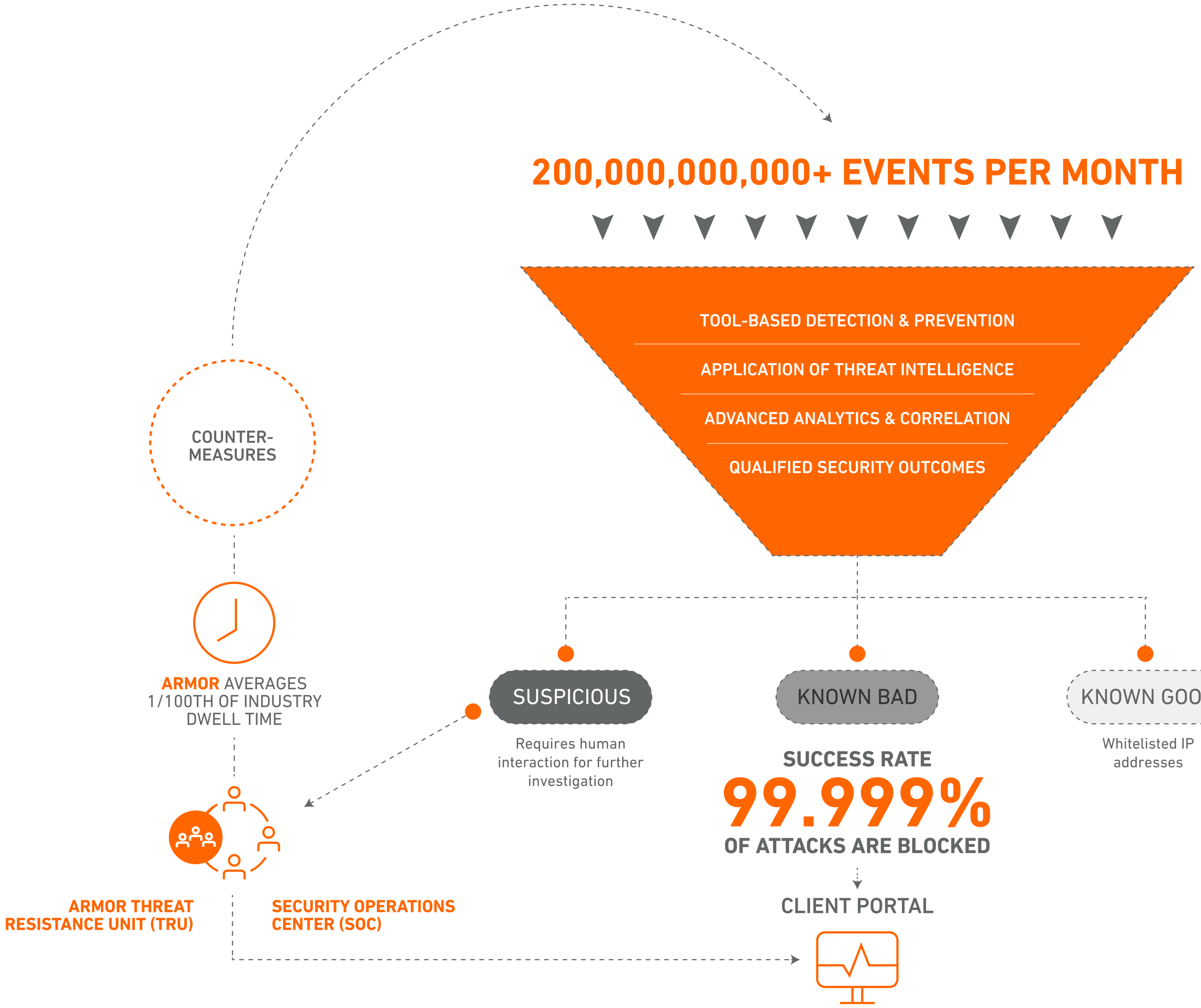
CUSTOMER PORTAL

API

CONTINUOUS FEEDBACK LOOP

> One thing that intrigued us with Armor vs. our other managed security provider was Armor's cloud aptitude and competency. Working with the SOC has provided great resource-saving value. The team members are knowledgeable about their clients, as well as security, so there aren't unnecessary escalation events sent to our team to deal with.
>
> — Baxter Credit Union

WHAT SPARTAN DOES



200,000,000,000+ EVENTS PER MONTH

TOOL-BASED DETECTION & PREVENTION

APPLICATION OF THREAT INTELLIGENCE

ADVANCED ANALYTICS & CORRELATION

QUALIFIED SECURITY OUTCOMES

SUSPICIOUS

Requires human interaction for further investigation

KNOWN BAD

SUCCESS RATE

99.999%

OF ATTACKS ARE BLOCKED

KNOWN GOOD

Whitelisted IP addresses

CLIENT PORTAL

COUNTER-MEASURES

ARMOR AVERAGES 1/100TH OF INDUSTRY DWELL TIME

ARMOR THREAT RESISTANCE UNIT (TRU)

SECURITY OPERATIONS CENTER (SOC)

SPARTAN PLATFORM—CAPABILITIES THAT COUNT

COLLECTION & PROTECTION

The Spartan platform serves as a central point of aggregation for event and log data regardless of the solution deployed. (Armor Complete or Armor Anywhere). This enables Armor to accelerate the process of threat identification. For security events known by Spartan to be malicious, Armor blocks them, preventing any impact (Armor blocks 99.999% of security events).

DATA MANAGEMENT

The Spartan platform ingests, tags, segments, and stores all logs/events to enable incident response and forensics (IRF) investigations.

THREAT INTELLIGENCE

Spartan gathers data from a variety of sources, analyzes it, and adds it to our database, enabling it to protect, detect, and respond. Spartan's capabilities connect the vast amounts of information gathered by TRU with community insights from more that 1,200 clients across cloud workloads, on-premise, and hybrid IT environments. This provides additional context and accelerates investigations to answer not just the what and how, but the who and why of an attack.

MANAGED DETECTION

Armor uses best-of-breed toolsets and machine learning technologies to uncover hidden threats and detect malicious activity endangering cloud, on-premise, and hybrid IT environments. Using advanced analytics, Spartan correlates and analyzes threat data to reduce false-positives and speed decision-making. With each new event it processes, Spartan continually learns and evolves, improving overall security.

CONTINUOUS RESPONSE

Spartan automates detection and event investigation and quickly orchestrates effective responses for security threats across cloud, on-premise, and hybrid IT environments. Incident investigation and response services are included as part of the Armor Anywhere service with TRU and SOC teams performing continuous threat hunting and developing countermeasures to combat future attacks.

REAL-TIME VISIBILITY

The platform unifies visibility across your Armor Complete environment. Customers can tap into the power and value of Spartan through AMP.

SECURITY OPERATIONS CENTER

The Armor SOC seamlessly combines a specialized combination of cybersecurity disciplines—providing a broad level of managed protection, detection, and response from known and emerging threats. When you partner with Armor, our security experts extend your security program through 24/7/365 monitoring and protection.

Our SOC and the processes they use are organized to ensure the highest level of security for our clients. TRU collects, enriches, and disseminates threat intelligence to ensure that our experts stay ahead of threats that could affect customer environments. Our indicators and warnings (I&W) team monitors customer environments for anomalies around the clock. The IRF team focuses on mitigating and responding to potential points of compromise. Each of the teams in our SOC work together to constantly improve processes and fine-tune our tools—staying ahead of threats.

<1 DAY

THREAT ACTOR DWELL TIME

99.999%

SECURITY EVENTS AUTOMATICALLY BLOCKED

5,000

SECURITY INCIDENTS MANAGED YEARLY

$200B

IN PAYMENTS PROTECTED YEARLY

> 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

SECURITY OPERATIONS CENTER COMPONENTS

INDICATIONS & WARNINGS

24/7/365, this team is monitoring your organization's environments, looking for anomalies and suspicious activity. In the event of potential compromise, they quickly escalate security events for a deeper assessment and response.

INCIDENT RESPONSE & FORENSICS

When suspicious activity is detected, our IRF team delves into forensic analysis to determine if the incident is a true positive. If a compromised host is detected, they work with the client to contain, eradicate, and recover from the threat—usually in less than 24 hours. After the threat is remediated, they coordinate with the client to address the root cause of the compromise and prevent future attacks through the same vector.

VULNERABILITY THREAT MANAGEMENT

Threat actors are always looking for an easy way into your environment. This is why vulnerability and patch management are essential for lowering your environment's attack surface. Our aggressive vulnerability assessment program keeps our customers' infrastructure hardened against attack.

THREAT RESISTANCE UNIT

TRU provides actionable cyberthreat intelligence that enables us to anticipate and block a majority of the cyberattacks against our clients, allowing us to provide unparalleled protection for your cloud, on-premise, and hybrid IT environments. We collect and analyze data from threat intelligence feeds to create a detailed overview of current and emerging threats. This keeps us a step ahead of threat actors, able to block their attacks before they even have a plan of attack.

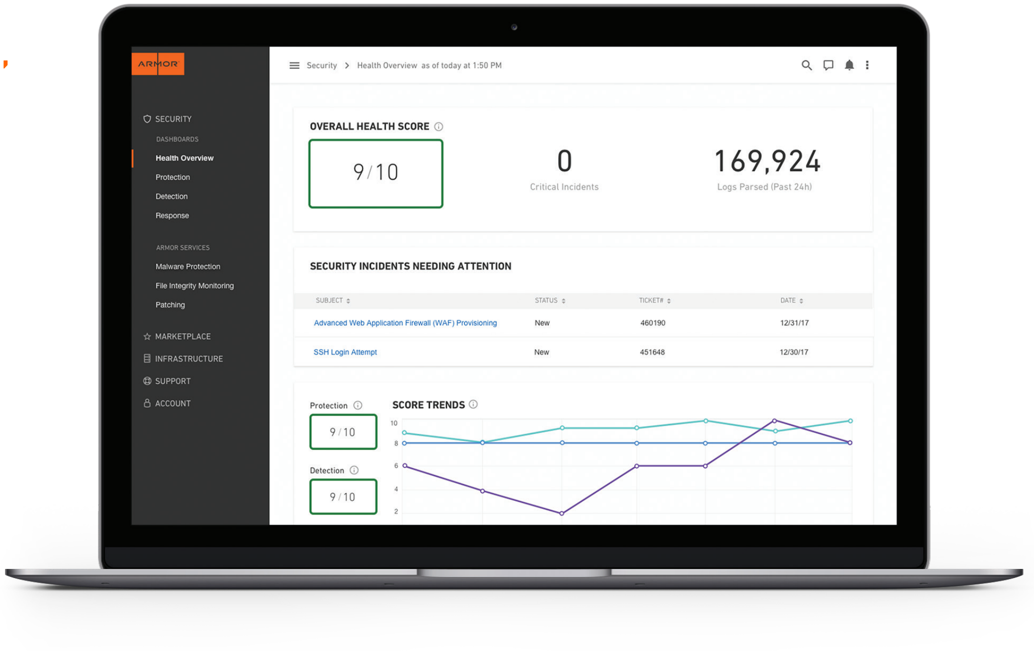
FRIENDLY NETWORK FORCES

We combine former National Security Agency online operators with our most experienced Armor engineers to create an internal threat hunting team. These talented threat hunters look for gaps or seams in the security surveillance of our clients networks. In other words, we have the best white hat hackers in the world working to break into our environment to make sure no one else can.

Explore how you can extend your security team. **Learn More>**

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 the newly enhanced AMP, your organization gains access to powerful self-service capabilities that speed incident detection and response, and provide critical insights that your security analysts need to make their jobs easier.



Security > Health Overview as of today at 1:50 PM

OVERALL HEALTH SCORE

9/10

0 Critical Incidents

169,924 Logs Parsed (Past 24h)

SECURITY INCIDENTS NEEDING ATTENTION

SUBJECT	STATUS	TICKET#	DATE
Advanced Web Application Firewall (WAF) Provisioning	New	460190	12/31/17
SSH Login Attempt	New	451648	12/30/17

Protection 9/10

Detection 9/10

- **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.

- **OS 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 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.

- **OS Patching Updates:**

  AMP provides Armor clients with patch details by host, including the update/patch name, patch version number, whether it is a security or feature patch, and an indication of when the patch was made available.

UNDERSTANDING YOUR HEALTH SCORES

AMP provides health scores designed for users such as CISOs, directors, and other managers seeking an understanding of their level of protection, operations, and security posture.

- **How is the overall score calculated?**

  The overall score is an average of your protection, detection, and response scores.

- **How is the protection score calculated?**

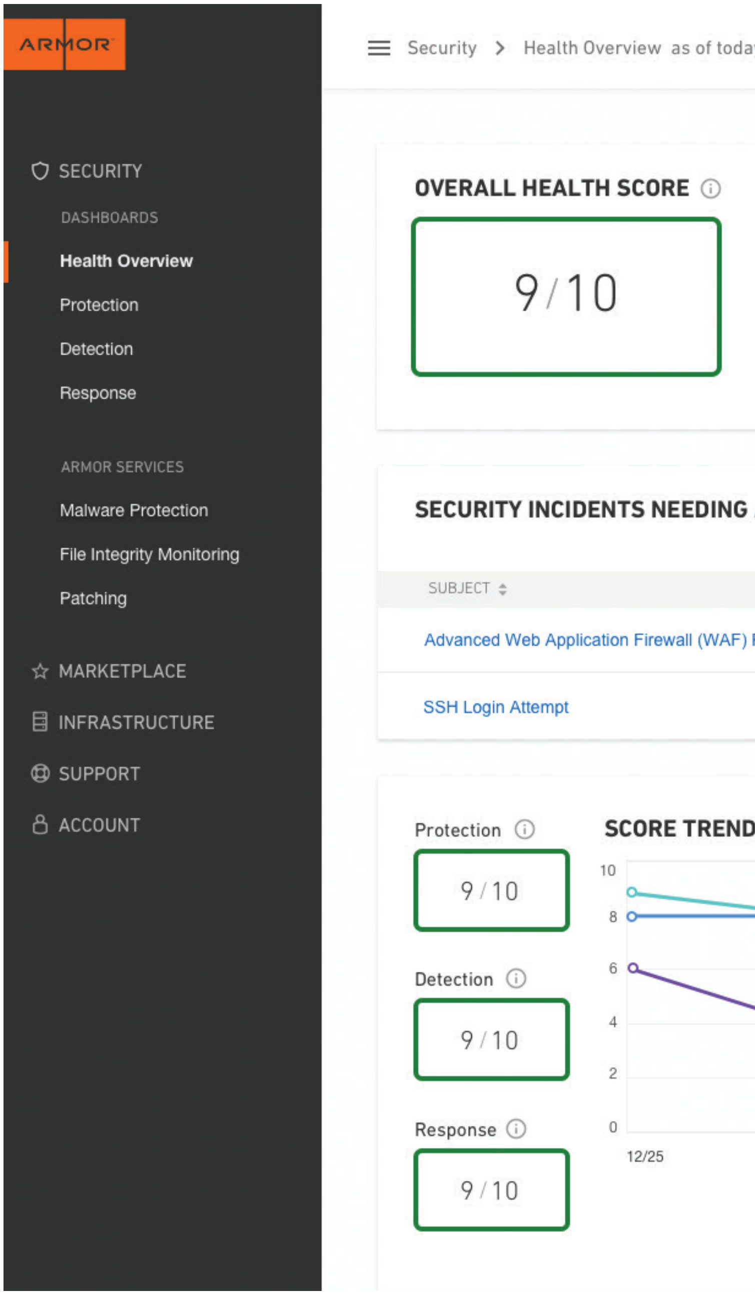
  Protection scoring looks at the subagent service heartbeats and log flow timestamps for services such as antimalware, logging, FIM, IDS, and other capabilities running within the Armor Anywhere agent. It ensures that each of those services has been sending logs and operating without fault over the past 24 hours.

- **How is the detection score calculated?**

  Detection is focused on ensuring that all of the agent and system data we're absorbing is flowing as expected to and that our platform is analyzing and correlating the data as we hunt and detect risks to the client environment. Detection scoring focuses on the log data coming in and our expectations as to the volume, type, and frequency of that dataflow tied back to your environment.

- **How is the response score calculated?**

  Response scoring tracks the time it takes Armor to respond to a client's ticket. Using the timestamps on each ticket over the past 24 hours, we can see how long it took our team to respond and manage each client incident. The response score provides visibility into our committment to responsive security and support.



SET UP

Operating System Support

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

redhat LINUX | CentOS | ubuntu | amazon web services Linux | Windows

DevOps Support

Armor provides install scripts for the Armor Anywhere agent so you can 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. The security results and logs also feed into Armor's SOC 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 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.

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 Linux

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

ARMOR®

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