Armor | Complete

TECHNICAL SOLUTIONS BRIEF

ARMOR COMPLETE | TECHNICAL SOLUTION BRIEF

ARMOR COMPLETE – SECURE CLOUD HOSTING

The speed of business in our digitally transformed world continues to accelerate. While IT teams leverage the agility of the cloud to match that pace, the need to protect against evolving security threats puts a heavier toll on the management of their cloud infrastructure. Control and agility become competing priorities, forcing businesses to compromise speed-to-market in order to guarantee a strong security posture.

Armor Complete, our secure cloud hosting platform, is a market-proven Infrastructure-as-a-Service solution that has been answering business needs for security and agility for nearly a decade. By delivering real-time, on-demand cloud services that are secure from day one, Armor Complete removes the burden of security from your team and empowers your business to move fast without compromising security. Our end-to-end solution includes:

1 Uncompromised Security

Uncompromised security in the cloud is only possible when you have a team of proven, talented experts leveraging best-of-breed security technology and scalable processes. This unparalleled combination of talent, technology, and techniques is the core of Spartan, our

2 Unrivaled Performance

Armor Complete is managed for performance. We don't oversubscribe; we over deliver network, compute and storage performance. It's simple math: fewer clients sharing the same resources result in higher performance for each client. We offer virtual servers with up to 16 vCPUs and 96 GB of RAM, and three storage tiers ranging from high performance to low cost.

3 Seamless Compliance

Armor Complete actively reduces your security and compliance burden by providing the highest level of managed security for your customers' data. Our uncompromised security approach enables you to more easily meet HIPAA/HITRUST, PCI DSS and GDPR cloud compliance requirements. With nearly a decade of hosting compliance-driven applications, we have built an audit-friendly reputation that simplifies compliance.

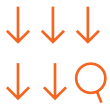
4 End-to-End Support

Our technology is cutting edge, but our support is built on a tradition of white-glove, personal service. Every Armor Complete customer receives assistance on their terms, from hosting management to insightful security discussions and effective incident response. It starts with our white-glove onboarding and continues with ongoing support from engineers, compliance specialists, security experts, and customer success managers.

SECURITY CAPABILITIES

INTERNET PROTOCOL REPUTATION MANAGEMENT (IPRM)

Our Threat Resistance Unit team provides actionable cyber threat intelligence that allows us to anticipate and block a large majority of the cyber-attacks against our customers, allowing us to provide unparalleled protection in the cloud. IPRM leverages that intelligence and filters public internet traffic matched to an IP blacklist.



DDoS PROTECTION

Denial-of-Service and Distributed Denial-of-Service (DoS and DDoS) protection is provided at every datacenter location. Once a DDoS attack is detected, Armor's security team directs traffic through a series of filters effectively mitigating the threat.

WEB APPLICATION FIREWALL (WAF)

The Web Application Firewall (WAF) provides protection from layer seven attacks targeted toward customer applications such as: cross site scripting, directory traversal, and SQL injection. Armor's WAF is a global security service that protects the Armor ecosystem and its customer by creating a unique understanding of application structure, elements and expected user behavior powered by dynamic profiling technology.

NETWORK INTRUSION DETECTION (NIDS)

Network intrusion detection provides real-time inspection of HTTP (port 80) network traffic that has passed through the Armor Complete perimeter for malicious and anomalous behavior.

FILE INTEGRITY MONITORING

FIM is designed to monitor critical system file locations and alert when your files have changed. It monitors critical operating system (OS) files for changes that may allow threat actors to control your environment. File integrity monitoring (FIM) utilizes 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 leverage your servers for illicit activity. In the event an alert is created, Armor's threat analysts begin an in-depth investigation. Armor utilizes 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, operating system logs, and other applications to determine their validity and severity. Customers can view 30 days of logs in the Armor Management Portal and store up to 13 months of log events consistent with applicable regulatory requirements.

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.

A FULLY-FEATURED PLATFORM DELIVERING NATIVE CLOUD INFRASTRUCTURE AND SERVICES

With nearly a decade of secure cloud hosting under our belts, we have built an ecosystem of core and ancillary services that make us a true one-stop shop for Infrastructure-as-a-Service.

CORE COMPONENTS

CLOUD SERVERS[1]

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 LINUX Windows CentOS

STORAGE

Flexible storage options

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

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

Tier 3 – High Volume
Fast disk 250 GB to 2 TB

BUILT-IN NETWORKING

- Native firewall
- Private IP addresses
- VPN Services-SLL and L2L/IPSec

[1] *All servers include high-performance SSD storage (Windows 60GB | Linux 30 GB)*

ADD-ON COMPONENTS & SERVICES

Tailor your environment to best meet your workload requirements with compliance, scalability, data protection and many other options:

COMPLIANCE, DATA PROTECTION & RECOVERY

Persistent Data Encryption
Scalable data encryption at rest, powered by Vormetric Data Security Manager

Advanced Log Management
Extend log retention and access to 13 months, meeting compliance requirements

Vulnerability Scanning
Compliance-as-a-Service includes scheduled scans and self-assessment portal

Backup Service
Flexible backup solution with simple recovery options, fully supported by our customer care team

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

SECURITY, NETWORK, SCALABILITY & PERFORMANCE

Load Balancers
Build and deploy horizontal scalability into your cloud with our flexible virtual load balancer options supporting up to 1 Gbps

Advanced WAF
Customers who have requirements for WAF rules and performance may deploy a dedicated virtual WAF in their cloud

SSL Certificates
Single-domain, wildcard, Extended Validation and organizational SSL certificates are available

Advanced DNS
Active failover and traffic management DNS services provided by Dyn

Advanced Application Monitoring
Closely monitor your workload performance with APM powered by New Relic

Resource Monitor
Highly detailed view into your cloud resources, providing a valuable tool to plan capacity

MICROSOFT SQL DATABASES

Armor can provision your server with a licensed Microsoft SQL DB server, saving you upfront money and providing you with flexibility for future upgrades. We offer the following editions:

MS SQL Web Edition
Offered in 4, 6, 8, 12 and 16 vCPU (processor) configurations

MS SQL Standard Edition
Offered in 4, 6, 8, 12 and 16 vCPU (processor) configurations

MS SQL Enterprise Edition
Offered in 4, 6, 8, 12 and 16 vCPU (processor) configurations

SHARED RESPONSIBILITY MODEL

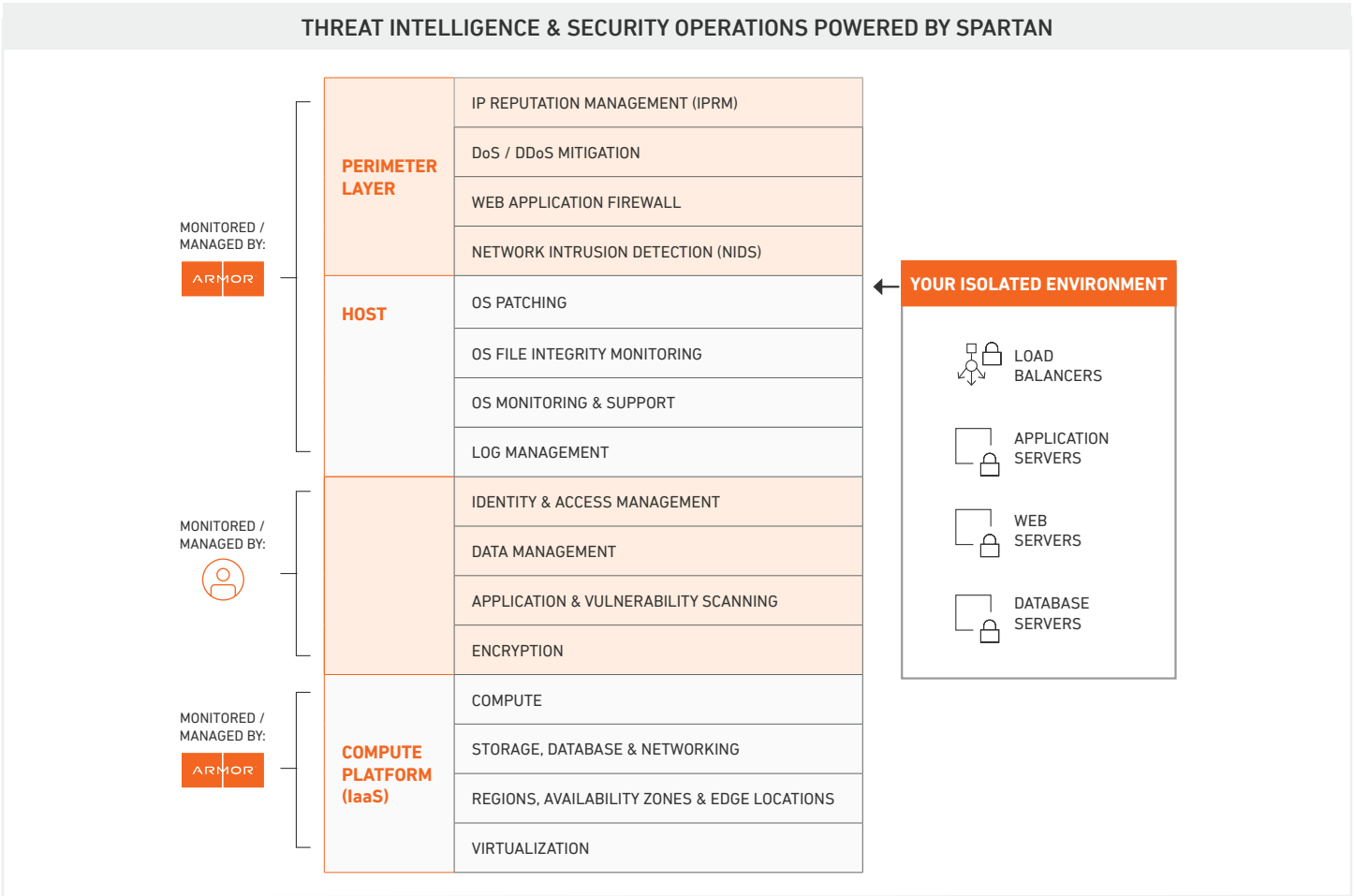
What is my responsibility in the security of my cloud workload?

Armor Complete addresses the aspects of shared responsibility that are often neglected by organizations looking to maximize the agility and flexibility of their cloud environment. It is a highly cost-effective way to avoid the significant capital and human investment required to deploy the multitude of solutions required to address those gaps.

Armor Complete is designed for easy deployment that is aligned with the typical tools and processes used in a DevOps framework. This approach ensures that each aspect of a security program is performed by the organization best suited for it and that no responsibilities are overlooked or duplicated. Armor and your organization become partners in securing your environment.

As an answer to organizations looking for help in handling all those security and compliance controls, Armor provides the industry's most comprehensive cloud security solution through Armor Complete. Our solution is designed to offload most of your organization's security responsibilities to Armor's proven Security Operations Center (SOC) and threat analytics experts.

Because of the end-to-end nature of our service, physical, network and virtual infrastructure security are either monitored or managed by Armor; in doing so, we achieve the elusive goal of delivering "turnkey compliance" by handling every security control within our scope. All you have to do is manage your data, applications and users.



Explore how Armor Complete Security solutions and services aligns with various compliance requirements and regulations. **Learn More>**

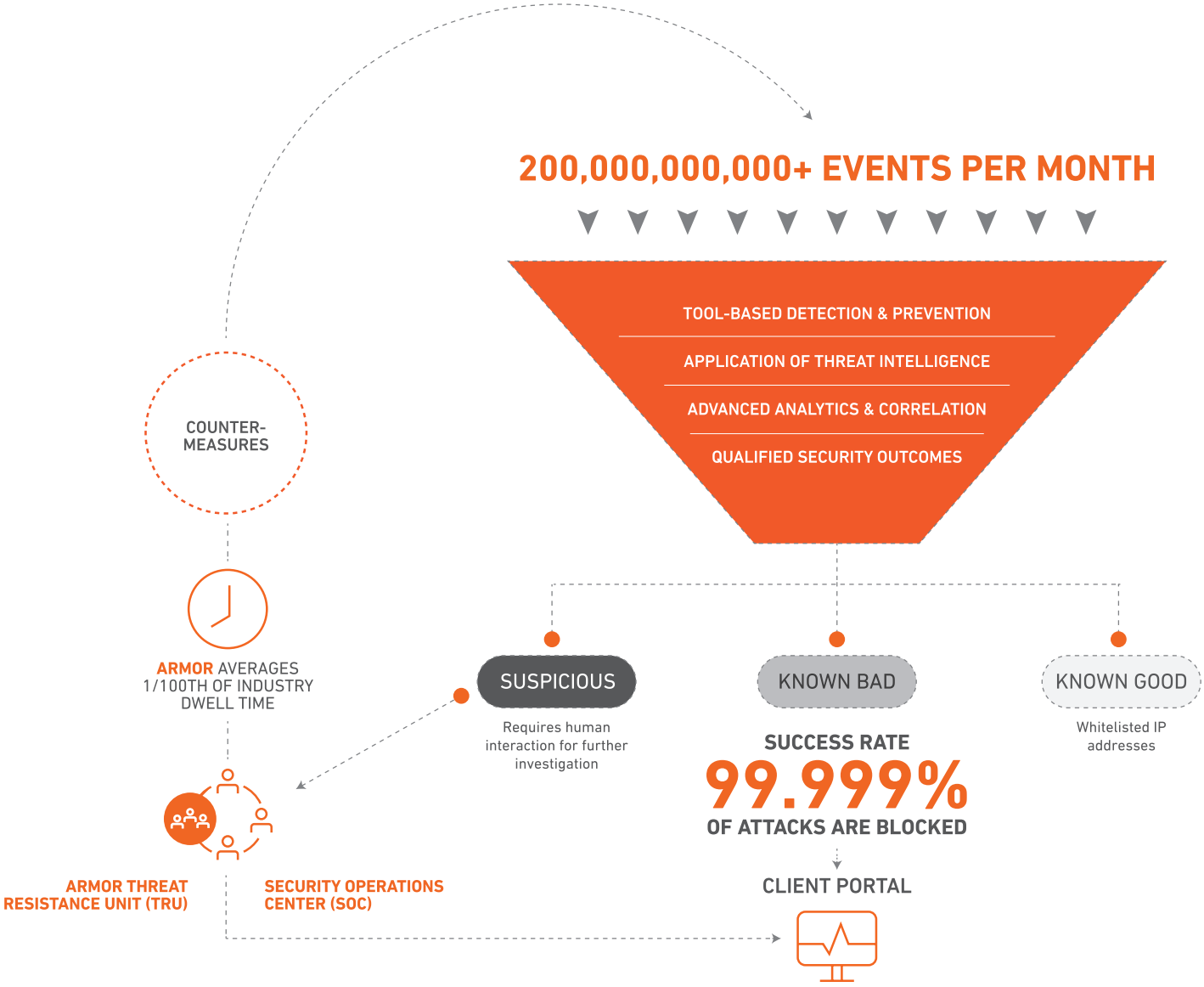
POWERED BY SPARTAN THREAT PREVENTION AND RESPONSE PLATFORM

Armor Complete is 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. Telemetry from over 1,200 customers drives community insights.

The Spartan platform is the connective tissue between Armor Complete, our Security Operations Center analysts and the Threat Resistance Unit team, and the Armor Management Portal. Our solutions are designed from the ground up to be scalable, deployable and manageable in diverse environments, and provide unparalleled monitoring, protection, detection and response capabilities to boost security and reduce the dwell times of attackers.

> We are able to stand in front of a customer and look them in the eye and say, 'I know that your data is safe.'
>
> — Steve Roderick I CEO, gotoBilling

WHAT SPARTAN DOES



SPARTAN PLATFORM CAPABILITIES OF NOTE

COLLECTION & PROTECTION

The Spartan platform serves as a central point of aggregation for event and log data regardless of the platform (Armor Complete or Armor Anywhere). This enables Armor to accelerate the process of threat identification. For security events already known by Spartan to be malicious, Armor blocks those events thereby 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 investigations.

THREAT INTELLIGENCE

Spartan stockpiles input from a variety of sources and feeds it back into our systems to enhance our ability to detect and respond. Spartan's capabilities connect the vast amounts of information gathered by Armor's Threat Resistance Unit (TRU) with community insights from over 1,200 clients across cloud workloads, on-premises 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 leverages best-of-breed toolsets and Machine Learning technologies to uncover hidden threats and detect malicious activity endangering cloud workloads, on-premises and hybrid IT environments. Using advanced analytics, Spartan correlates and analyzes threat data to reduce false-positives and speed and machine learning decision-making. With each new event it processes, Spartan continually learns and evolves, improving overall security efficacy even further.

CONTINUOUS RESPONSE

Spartan automates detection and event investigation, and quickly orchestrates effective responses for security threats across cloud workloads, on-premise and hybrid IT environments. Incident investigation and response services are included as part of the Armor Complete service with Threat Resistance Unit (TRU) and Security Operation Center (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 the Armor Management Portal.

SECURITY OPERATIONS CENTER

The Armor security operations center 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 Security Operations Center and the processes they use are organized to ensure the highest level of security to our customers. The Threat Resistance Unit (TRU) collects, enriches and disseminates threat intelligence to ensure that our experts stay ahead of threats that could impact customer environments. Our Indicators and Warnings (I&W) team monitors customer environments for anomalies around the clock. The incident Response and Forensics (IRF) team focuses on mitigating and responding to potential points of compromise. Each of the teams in our Security Operations Center 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 YEARSLY

$200B

IN PAYMENTS PROTECTED YEARLY

> We chose Armor because customer trust is at the heart of what we do at Ultius—and Armor was the only provider that showed security to be its core competency.
>
> — Boban Dedovic, Founder and CEO, Ultius

> Armor's commitment to security has helped strengthen our brand reputation.
>
> — Michael Frederick | Vice President Assurance Services & Product Development, HITRUST

SECURITY OPERATIONS CENTER (SOC) COMPONENTS

INDICATIONS AND WARNINGS (I&W)

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

INCIDENT RESPONSE & FORENSICS (IRF)

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

VULNERABILITY THREAT MANAGEMENT (VTM)

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 surface area of attack. Our aggressive vulnerability assessment program keeps our customers' infrastructure hardened against attack.

THREAT RESISTANCE UNIT (TRU)

Our TRU team provides actionable cyber threat intelligence that enables us to anticipate and block a large majority of the cyber-attacks against our customers, 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 (FNF)

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 customer 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.

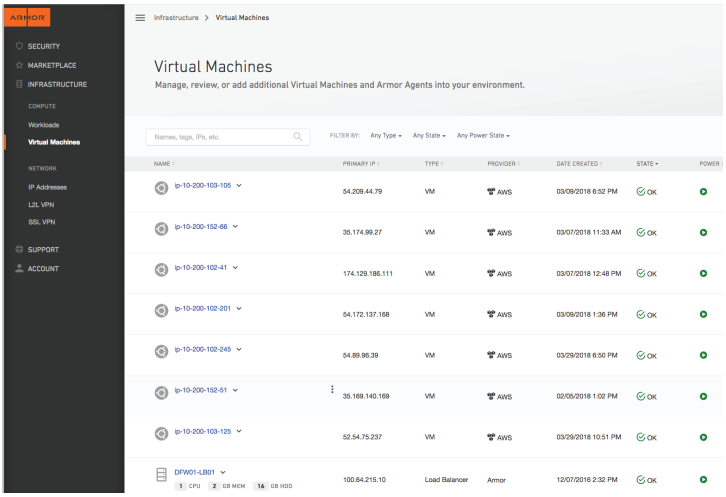
Explore how you can extend your security team. https://www.armor.com/extend-security-team/

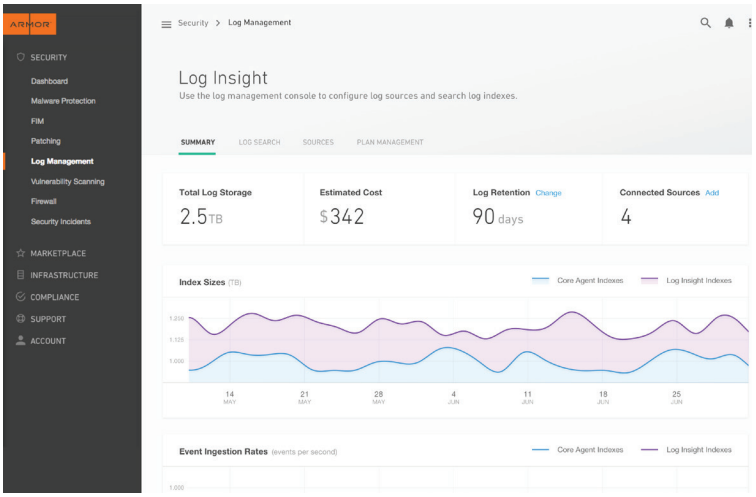
VISIBILITY AND CONTROL THROUGH THE ARMOR MANAGEMENT PORTAL

Central to our promise of agility and control is the Armor Management Portal (AMP). It is the interface through which our customers manage their environment by adding or removing resources, changing configurations, and accessing support options. It is also provides the single-pane-of-glass dashboard that gives full insight into the performance and the security of their workloads.

Through the Armor Management Portal, our customers can:

- Instantly add and scale cloud resources such as virtual servers and storage;
- Make instant firewall policy changes with self-service rules;
- Manage their IP space (public and private);
- Create and manage site-to-site (L2L) VPN tunnels;
- Control access to the environment by managing users, roles and permissions;
- Create and interact with support tickets;
- Shop for additional services such as additional IP addresses, data replication, backups, encryption and many others in the Armor Marketplace;
- Real-time visibility into security metrics through the Security Dashboard.



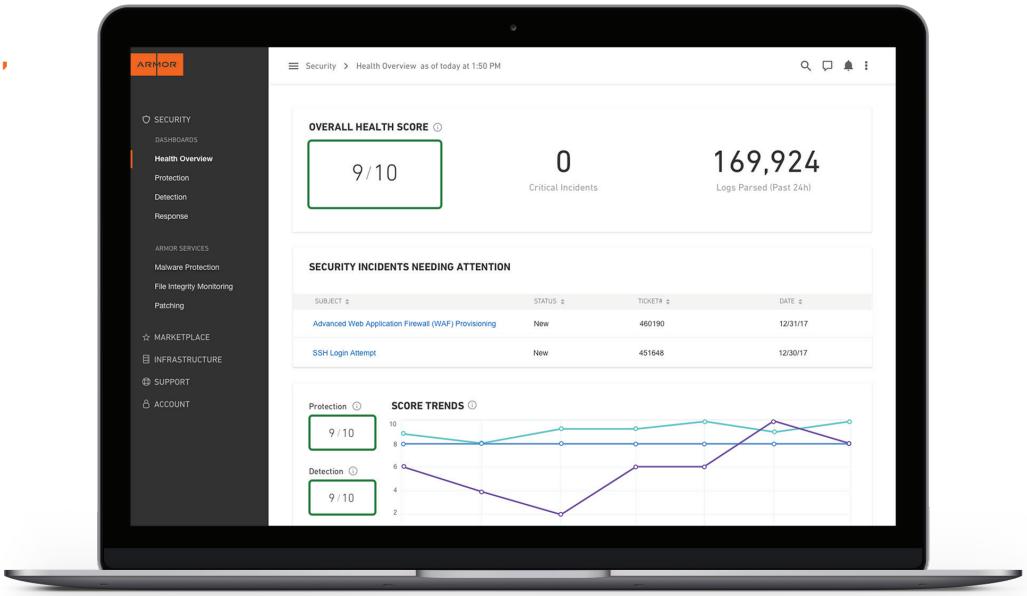


FULLY-FEATURED PUBLIC API

The need for agility and control manifests itself most strongly within organizations that embrace a DevOps philosophy. Those customers can automate the management of their cloud with Armor's RESTful HTTP API, and programmatically integrate Armor's native cloud capabilities into their cloud strategy. This process is further facilitated by the interactive Armor API tool, powered by Swagger, which is a cloud-based tool used to build, deploy, and document APIs. Customers can use this tool to test, review, and implement API calls.

OVERALL HEALTH, PROTECTION, DETECTION, AND RESPONSE SCORES

The Armor Management Portal (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 Armor Management Portal (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 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:**

  The Armor Management Portal provides our users with a look at the telemetry data coming off our intrusion detection system.

- **Malware Protection Service Health:**

  View state of malware service engine and review previously detected malware items.

- **OS File Integrity Monitoring Status View:**

  The Armor Management Portal 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. Aggregated log information including top sources by event ingestion and index size are reported within AMP.

- **Vulnerability Scanning (Bottom):**

  View Vulnerability Scanning (Bottom) scan results to identify risks and determine appropriate next steps for updating and patching.

- **OS Patching Updates:**

  The Armor Management Portal provides Armor customers 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

The Armor Management Portal 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?**

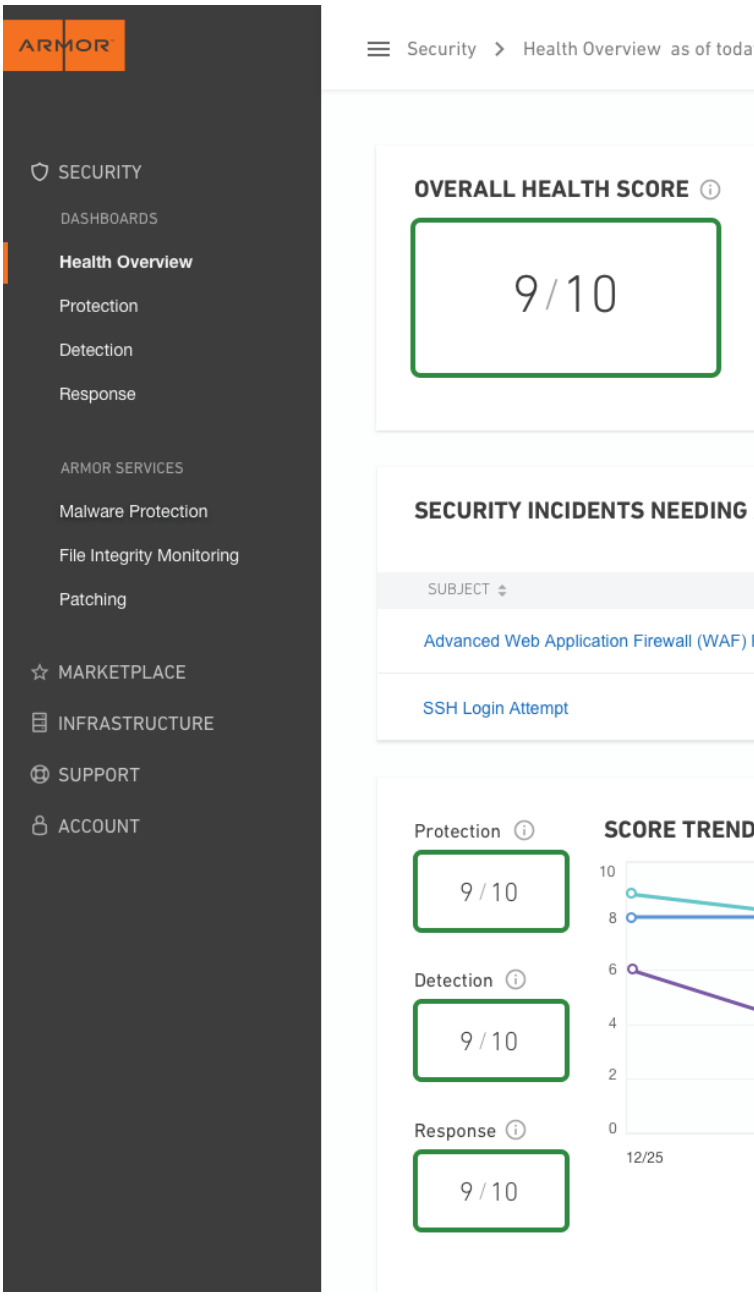
  Protection scoring looks at the sub-agent service heartbeats and log flow time stamps for services such as anti-malware, logging, file integrity management, intrusion detection and other capabilities running within the Armor Anywhere Agent and ensures that each of those services has been sending logs and heart beating 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 bringing back in are flowing as we expect them to and that our Spartan 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 data flow tied back to your environment.

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

  Response scoring looks at the time to communicate and respond between Armor and our customers based on the timestamps for tickets created and managed within the previous 24 hours. The Response score provides visibility into our commitment to responsive security and support.



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