ARMOR MALWARE PROTECTION

To keep up with industry demand, businesses are innovating rapidly while reaping the benefits of virtualization in the digital economy. With this growth, threat actors are getting smarter—making it imperative to secure your on-premise, hybrid, hosted, and container environments effectively.

The risks are enormous—malicious software (malware) in your network can lead to account compromise, data theft, and possibly additional access to sensitive data in your environment. Today's sophisticated threats require a new approach to protecting users, networks, and data centers. This approach needs to use a blend of threat protection strategies that applies the right technique at the right time. Armor's malware protection service provides an additional layer of detection for indicators of compromise (IOC) or a breach of your environment

ADDITIONAL LAYER OF DEFENSE AGAINST THREATS

Armor malware protection provides an extra level of detection on your hosts to identify suspicious activity and alert you to it. In addition to eradicating malware, each exploit generates community-powered insights—the collective knowledge of these insights is applied across more than 1,200 client environments.

AUDIT-READY COMPLIANCE

Armor malware protection service addresses key change control processes required by PCI DSS, HIPAA, HITRUST, SAN CSC, NIST, and other frameworks.

ADVANCED ANALYSIS & CORRELATION

Events are analyzed and correlated with event data from your other devices under management by our Spartan threat prevention and response platform, delivering enhanced detection of potential threats across your public, private, or hybrid cloud, or on-premise IT environments.

Armor malware protection monitors your hosts 24/7/365 for anomalous and unauthorized activities that indicate potential threats. The malware protection service provides detection of and protection against malware. Armor uses an enterprise-class malware protection application and deploys the application agent with the Armor agent.

ARMOR

RESPONSE THAT GOES BEYOND ALERTING

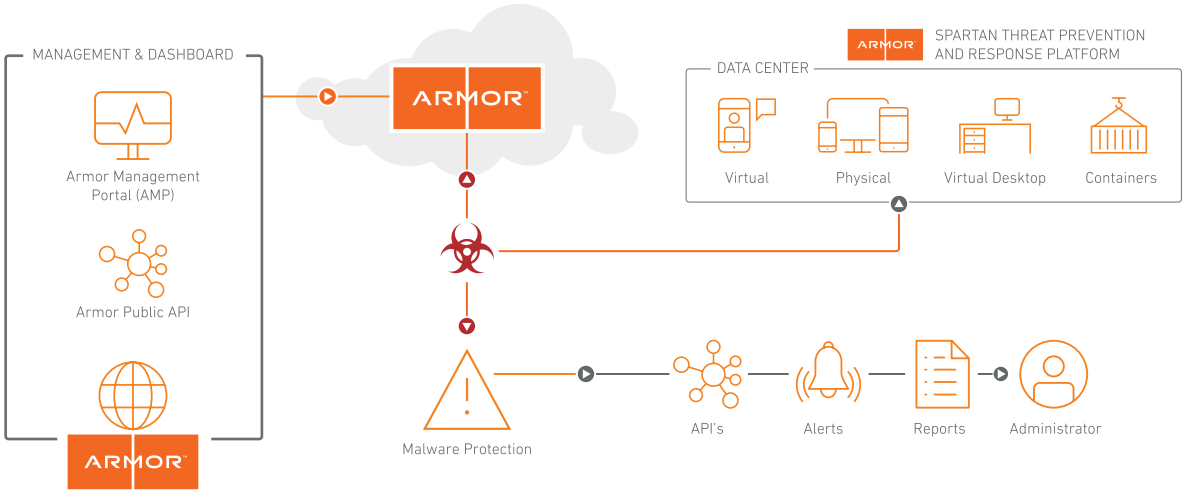
Unlike traditional managed security service providers (MSSPs), Armor goes beyond simple alerting. Our security operations center (SOC) analysts monitor your environment 24/7/365, working closely with your team to investigate and respond to potential incidents.

ARMOR MALWARE PROTECTION DELIVERS TRUSTED SECURITY:

- Unify protection across your cloud, on-premise, hybrid, container, and hosted environments through correlation of malware events with other security controls under our management.
- Get audit-ready—meet compliance regulations and industry guidelines like PCI DSS, HIPAA, DFS-500, ISO, and GDPR that span the data center and cloud.
- Built-in security control helps you integrate security into your continuous integration/continuous deployment (CI/CD) pipeline with API-first tools and resources.
- Get access to time-tested security and compliance experts who monitor your environments 24/7/365.
- Go beyond simple alerting and respond to incidents faster.

HOW DOES IT WORK?

Armor does more than secure the network. Our experts monitor and secure your hosts, providing a defense-in-depth solution that secures your operating system (OS) up to the application layer. The agent-based service is both proactive and reactive protection from malicious payloads and packages that find their way onto a client's server.



CRITICAL PROTECTION ACROSS YOUR HOSTS IN ANY ENVIRONMENT

The malware protection agent registers with the Armor management portal (AMP) console, which receives scan results and activity logs in real-time. These logs are entered into the Spartan platform database, where SOC teams monitor alerts 24/7/365. If a critical detection occurs, the security information and event management platform (SIEM) will alert in near real-time. If new malware is discovered during our security operations and analytics, We work directly with the anti-virus (AV) vendor to have signatures created, and our teams create custom mitigation and/or detection techniques as threats emerge. This means an attack on one Armor customer provides protection for all others.

Armor's SOC also leverages standard operational processes looking for indicators of new malware and viruses, working to protect our customers before the attack, not after. Not only are we using these findings to create custom protection mechanisms, but we also create triggers to alert to suspicious traffic that matches patterns observed in new malware.

Scans are performed three times a week wherein all servers are scanned against the latest definitions, heuristics, and honeypot discoveries. Armor's definition database is sourced by internal, public, and private resources. All servers report back to the AMP console enabling us to manage and report on malware prevention and remediation. Detected threats are monitored and alerted by our security operations team and remediated as necessary.

LEARN MORE

This service is available for all Armor Anywhere and Armor Complete customers. The service runs and is fully supported on AWS, Azure, Google Cloud Platform, and Rackspace for Armor Anywhere customers and is supported on all 5 Armor Complete datacenters (Amsterdam, Dallas, London, Phoenix, and Singapore) for Armor Complete customers. This service is also available for partners' on-premise environments and other datacenter if the Armor agent is running on a supported OS.

Click to learn more about Armor Anywhere or Armor Complete.

OPTIMIZED FOR

aws Microsoft Azure docker vmware

ARMOR