ARMOR ®

Armor Agent for Servers

Protect your applications and data, anywhere

Integrate a suite of critical security capabilities

Armor's cloud workload protection is delivered through the Armor Agent for Servers
The agent is lightweight and can be deployed in private, public, and hybrid clouds as well as in on-premise environments.

Advance protection for cloud Windows and Linux workloads

Armor Agent for Servers is a scalable, cloud security product that integrates best-of-breed security technology to protect your hosted applications and data, otherwise referred to as workloads.

- Malware protection

- File integrity monitoring (FIM)

- Host-based intrusion detection/intrusion prevention system (IDS/IPS)

- Vulnerability scans

- Recommendation scans

- Log Management

Armor Agent for Servers is the perfect solution for companies who want an integrated toolset and simple deployment with simple pricing.

Standalone and full-service options

Armor Agent for Servers integrated within our MDR offering provides advanced protection, visibility, and scalability for any organization. It is the perfect solution for companies who want an integrated toolset and simple deployment.

Why Armor Agent for Servers?

- Single-pane-of-glass view of your Armor-protected workloads with the Armor Management Portal

- Reduce the accidental risks in the public cloud

- Stop advanced threats across distributed endpoints

- Get deeper context and enhanced security protection from existing security investments

- Simplify adherence to major compliance frameworks

PCi   GDPR   ISO

Armor Agent for Servers features

Armor Agent for Servers for cloud Windows and Linux workloads integrates a suite of critical security capabilities including:

MALWARE PROTECTION

Safeguard your environment from harmful malware and botnets, including viruses, spyware, and rootkits.

FILE INTEGRITY MONITORING (FIM)

Examines critical system file locations on your hosts as well as critical OS files for changes that may allow threat actors to control your environment.

INTRUSION DETECTION/PREVENTION

Installed on a host, IDS/IPS analyzes network or host traffic and identifies if that traffic matches signatures of known attacks.

VULNERABILITY SCANS

Search for application vulnerabilities that could be exploited by a threat actor and put your applications and data at risk.

POLICY RECOMMENDATION SCANS

Identify vulnerabilities and the state of controls with scans that provide recommendations and can be set to automatically apply new rules and changes.

LOG MANAGEMENT

Enhance threat detection, expand effective response context, and satisfy compliance for log storage. Ingests logs from agent and third-party sources into the cloud security platform.

About Armor

Armor, a global cybersecurity leader, provides comprehensive managed detection and response (MDR) and compliant cloud solutions. By combining advanced technology with expert services, Armor protects businesses from cyber threats, mitigates their risk, and ensures regulatory compliance. Dedicated to innovation and excellence, Armor is trusted by thousands of customers worldwide. The company is headquartered in Dallas, Texas, and has offices in the United States and Singapore.

Contact Us

https://go.armor.com/contact

Learn more about Armor Cloud Solutions

https://www.armor.com/solutions/armor-cloud/

For more information

(US) +1 877 262 3473   **(SG)** +65 6681-6609