SOLUTIONS BRIEF

Armor Agent for Servers

Protect your applications and data, anywhere.

Integrate a suite of critical security

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.

- Malaware 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?

- Simplify adherence to major compliance frameworks
- Stop advanced threats across distributed endpoints
- Reduce the accidental risks in the public cloud
- Get deeper context and enhanced security protection from existing security investments
- Single-pane-of-glass view of your Armor-protected workloads with the Armor Management Portal

 |

Armor Agent for Servers Features

Armor Agent for Servers for cloud Window and Linux workloads integrate 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 is a global leader in cloud-native managed detection and response. Trusted by over 1,700 organizations across 40 countries, Armor delivers cybersecurity, compliance consulting, and 24×7 managed defense built for transparency, speed, and results. By combining human expertise with AI-driven precision, Armor safeguards critical environments to outpace evolving threats and build lasting resilience.

Contact Us

www.armor.com/contact

Member of Microsoft Intelligent Security Association

 |