MORPHISEC

For Windows Servers & Workloads

The Evolution of Server and Workload Security

Servers hold the highest-value information assets in an organization, making them a prime target for hackers. Morphisec for Windows Servers and Workloads is built on our patented Automated Moving Target Defense (AMTD) technology. AMTD proactively prevents the most sophisticated, damaging cyberattacks on physical and virtual servers that evade detection-based technologies like NGAV, EPP, and EDR/XDR. Morphisec deterministically blocks attacks against both physical and virtual servers, on-premises and in the cloud.

Protect Servers Across All Attack Vectors

- **Admin Access**
  Morphisec prevents browser, document, and supply chain attacks that target servers during admin logon sessions
- **Lateral Movement**
  Morphisec stops attackers moving laterally from a workstation to a server or from server to server
- **Virtual Applications**
  Morphisec's ultra-lightweight agent secures virtual apps without impacting performance

CORE CAPABILITIES

- AMTD technology secures runtime memory against advanced attacks like ransomware, supply chain attacks, data theft, zero-days, polymorphic attacks, and more
- Continuous application inventory visibility, and risk-based vulnerability prioritization
- Protects legacy Microsoft servers back to 2008-R2 with negligible CPU, memory, disk requirements, or performance impact

BENEFITS

- Stops advanced attacks that NGAV, EPP, and EDR/XDR miss
- Reduces costs, boosts operational efficiency: Ultra lightweight 6MB agent slashes false positive alerts and boosts security with no extra staff needed
- Shrinks the attack surface of vulnerable legacy systems; no internet connection or downtime for deployment or maintenance needed

RESULTS

- TruGreen slashed false positives by 95 percent and cut costs by two-thirds
- Sample attacks stopped at day zero: Babuk ransomware, Explosive Mirrorblast, Jupyter via MSI Installer

Automated Moving Target Defense for Maximum Protection

Unlike detection-based solutions, Morphisec's patented AMTD technology doesn't need a signature or behavior pattern to detect and stop a threat. Instead, Morphisec proactively prevents attacks by creating a dynamic attack surface in runtime memory that threat actors can't penetrate. AMTD regularly morphs (randomizes) application memory, APIs, and other operating system resources during runtime, leaving decoys in their place. Effectively it continuously moves the doors to the house, hiding real doors and leaving fake doors in their place. Any code that tries to open a fake door is trapped for forensic analysis and triggers an alert notification. Even if a threat actor could find a real door—it won't be there when they return, stopping adversaries from reusing an attack on the same endpoint, let alone on other endpoints.

> **Gartner calls AMTD "the future of cyber" and says, "Automated moving target defense is an emerging game-changing technology for improving cyber defense."** [1]
>
> Gartner

Morphisec protects servers and workloads from all exploit-based, memory injection attacks in endpoint applications like browsers and productivity tools. We prevent ransomware, supply chain attacks, zero-days, and attacks targeting known but unpatched vulnerabilities within whitelisted applications. Morphisec does this via an ultra-lightweight, easy to install 6MB agent that requires no administration.

Key Benefits

STOP ADVANCED THREATS AND ZERO DAYS

- Prevents zero-days and advanced attacks without prior knowledge of the threat form, type, or behavior

VIRTUALLY PATCH VULNERABILITIES

- Protects servers and workloads from the most severe vulnerability exploitation when patches are not yet available or deployed

PREVENT LATERAL MOVEMENT

- Stops attackers engaging in lateral movement to increase their attack surface

SET AND FORGET

- Rapid, easy rollout with no system conflicts and zero maintenance—no databases, signatures, or rules to configure and update, or logs or alerts to analyze

NO SYSTEM IMPACT

- Ultra-lightweight, stateless agent with minimal footprint, no run-time components, and negligible performance impact

CUT SECURITY OPERATIONAL COSTS

- Negligible false positive alerts, removing the need to investigate, analyze, or remediate

Morphisec agent system requirements

Supported Microsoft operating systems: Windows Server 2008 R2, Windows Server 2012 + 2012 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022

Disk Space: 30MB minimum

About Morphisec

Morphisec provides prevention-first security against the most advanced threats to stop the attacks that others don't, from endpoint to the cloud. Morphisec's software is powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity. AMTD stops ransomware, supply chain attacks, zero-days, and other advanced attacks. Gartner® research shows that AMTD is the future of cyber. AMTD provides an ultra-lightweight, Defense-in-Depth security layer to augment solutions like NGAV, EPP and EDR/XDR. We close their runtime memory security gap against the undetectable cyberattacks with no performance impact or extra staff needed. Over 5,000 organizations trust Morphisec to protect nine million Windows and Linux servers, workloads, and endpoints. Morphisec stops thousands of advanced attacks daily at Lenovo, Motorola, TruGreen, Covenant Health, Citizens Medical Center, and many more.

To learn more, visit morphisec.com/schedule

Footnotes

[1] https://engage.morphisec.com/gartner-automated-moving-target-defense