MORPHISEC

Prevention-First Security

The Evolution of Endpoint Security

Runtime Memory Security & Continuous Vulnerability Visibility

Threat actors keep increasing in sophistication, exploiting the reactive nature of leading endpoint and server security solutions to successfully breach even the most well-defended organizations. Dealing with these advanced attacks requires a novel approach —one that's proactive and prevention-first. Morphisec's Automated Moving Target Defense (AMTD) technology, coupled with continuous visibility into application vulnerabilities, offers the next step in the evolution of endpoint security. Morphisec stops the advanced, undetectable attacks that evade NGAV, EPP, and EDR/XDR. Morphisec fortifies traditional vulnerability management and endpoint security solutions to stop advanced attacks before they occur, and rescues cybersecurity teams from drowning in false positive alert fatigue.

CORE CAPABILITIES

- Automated Moving Target Defense secures runtime memory
- Prevents ransomware, supply chain attacks, data theft, zero-days, polymorphic attacks, and other advanced attacks
- Continuous application inventory visibility, and risk-based vulnerability prioritization
- Secures legacy Microsoft workstations going back to Windows 7, servers back to 2008-R2, and extensive Linux distributions, with negligible CPU, memory, disk requirements, or performance impact

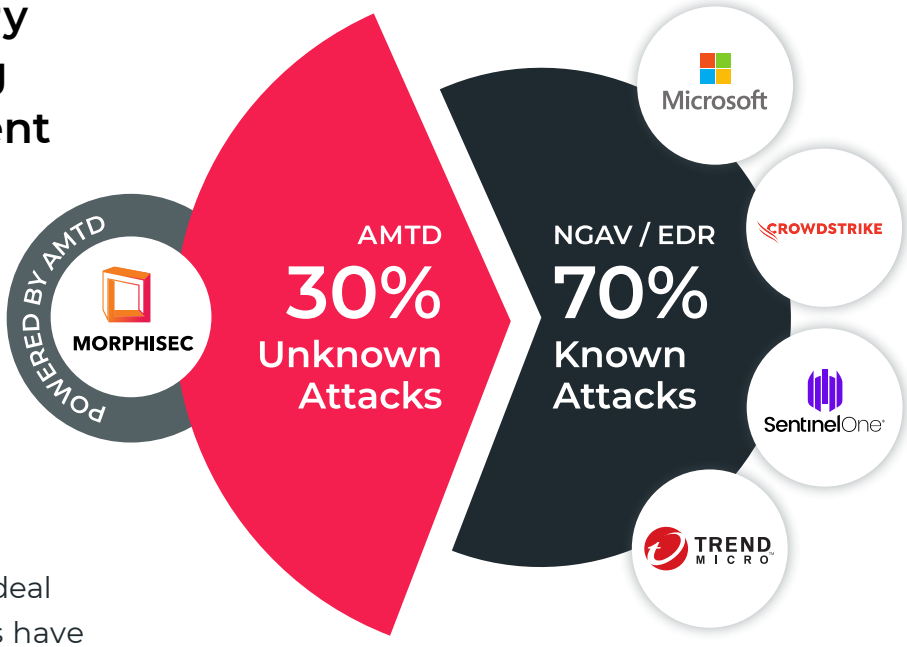
BENEFITS

- Accelerates the evolution of cybersecurity with Automated Moving Target Defense to stop advanced attacks on Windows and Linux that NGAV, EPP, and EDR/XDR miss
- Reduces costs, boosts operational efficiency: Better security with no extra staff needed. Ultra lightweight 6MB agent ensures negligible performance impact
- Secures legacy operating systems: Shrinks the attack surface of vulnerable legacy systems; no internet connection or downtime for deployment or maintenance needed

PROVEN RESULTS

- Trusted by 5,000+ organizations across nine million endpoints and workloads
- TruGreen slashed false positives by 95 percent and cut costs by two-thirds
- PACCAR: "Morphisec fills the gaps of our XDR solution for a true defense in depth strategy with minimal footprint and few false positives."
- Sample attacks stopped at day zero: DECAF ransomware, Explosive Mirrorblast, Jupyter via MSI installer

Secure Runtime Memory With Automated Moving Target Defense to Prevent Advanced Attacks



PREVENTION-FIRST SECURITY POWERED BY AMTD

Today's cybersecurity technology stack is no longer enough to protect endpoints, servers, and workloads. Anywhere between 25 percent and 95 percent of cybersecurity alerts are false positives, costing considerable time and resources to deal with. Over 80 percent of companies have suffered at least one data breach, and detection-based tools take an average of 277 days (nine months) to detect and respond to ransomware and other advanced threats, leaving ample time for adversaries to successfully execute attacks. The fundamental problem is that NGAV requires malware file signatures from previous attacks to recognize malicious files and respond to them. EPP and EDR/XDR need behavior patterns based on previous attacks to detect and respond to them.

The necessity of matching a new attack to previous attacks presents a critical security gap for detection-based solutions. It means they can't reliably stop unknown attacks or undetectable attacks which **hide in runtime memory** where these tools can't effectively scan. To quantify this gap, Morphisec analyzed data from the **Picus Labs 2023 Red Report**, which examined 500,000 malware samples, along with data from 5,000+ Morphisec customers, nine million endpoints, and 10,000+ daily incidents. Detection-based solutions struggle to stop at least three of the top 10 MITRE ATT&CK techniques, a critical 30 percent security gap. (And legacy systems struggle with even more of these techniques.)

Morphisec's Automated Moving Target Defense (AMTD) technology was specifically designed to stop these advanced attacks and close the runtime memory security gap. (To learn about the evolutionary nature of AMTD, read the Gartner report: Emerging Tech: Security —The Future of Cyber is Automated Moving Target Defense.[1])

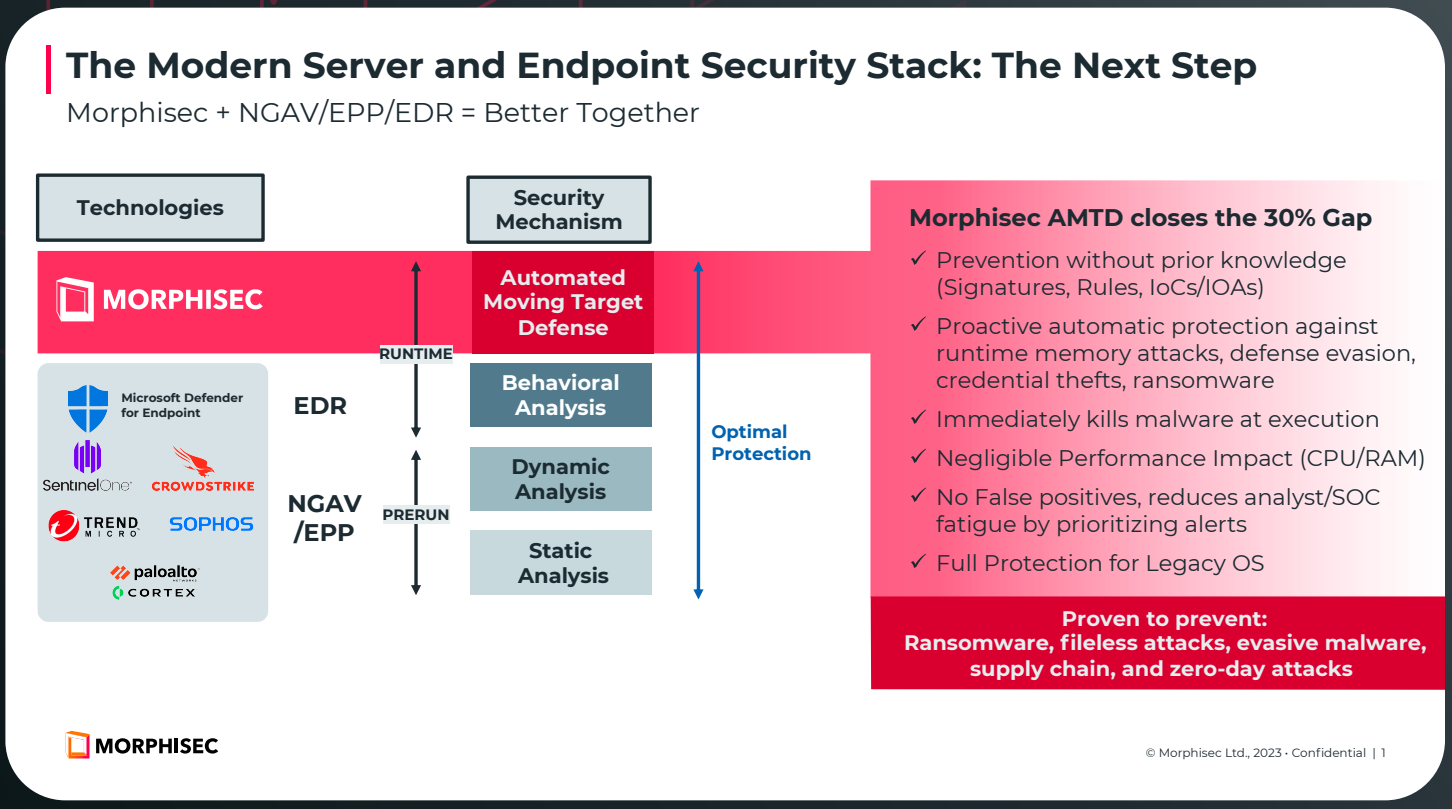
"Automated Moving Target Defense is an emerging game-changing technology for improving cyber defense."

Gartner

The Evolution of Endpoint Security

Morphisec, powered by AMTD, is the solution for stopping the attacks that NGAV, EPP, and EDR/XDR miss. We take a fundamentally different approach to cybersecurity based on proactive prevention, rather than reactive detection and remediation.

Instead of detecting attacks after they've happened, Morphisec's patented AMTD technology blocks attacks preemptively, without needing signatures, recognizable behaviors, or any kind of foreknowledge.



AMTD does this by creating a dynamic attack surface in memory that threats can't penetrate. It regularly morphs (randomizes) application memory, APIs, and other operating system resources during runtime. Effectively it continuously moves the doors to the house while leaving fake doors behind in their place, hiding key assets. Any code that tries to open a fake door is trapped for forensic analysis. 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.

Morphisec's ultra-lightweight 6MB agent has no performance impact, doesn't generate false positive alerts, and doesn't require extra staff. We offer continuous application inventory and risk visibility, and unmatched protection against threats like supply chain attacks, data theft, fileless attacks, ransomware, wipers, and other advanced attacks. It's the next evolution of cybersecurity, creating Defense-in-Depth that augments NGAV, EPP, and EDR/XDR/MDR solutions. And our proven AMTD technology is coupled with added anti-ransomware security layers for unrivaled Defense-in-Depth.

Continuous Vulnerability Visibility

The known vulnerabilities in the world vastly exceed security teams' resources to patch promptly. So which ones do you prioritize patching first? Not all vulnerabilities matter equally to everyone, because thanks to differing application usage, no two organizations have the same risk profile. If an application is unused, the attack surface of even a severe vulnerability shrinks to near zero, and the risk of a successful exploit with it. Conversely, a lower severity vulnerability in an application your organization widely uses means a larger attack surface—and higher risk to you. Morphisec's patented approach updates your usage data and new CVE information daily to re-prioritize your vulnerabilities based on your specific risk environment.

Because most vulnerability management solutions use scanners prone to logging errors, system crashes, and user disruption, companies limit scans to monthly or quarterly events, offering only limited "snapshot" vulnerability visibility. Morphisec is not scanning-based, removing the risk of system crashes or user disruption, while offering continuous vulnerability visibility. Always knowing where you're vulnerable is key to a proactive, preventive cybersecurity strategy.

Morphisec Anti-Ransomware Protection

Ransomware is still many CISOs' top concern. Morphisec's comprehensive Defense-in-Depth anti-ransomware capability provides four distinct security layers that prevent ransomware, do not affect productivity or performance, and integrate seamlessly with cybersecurity stacks:

DATA ENCRYPTION & DESTRUCTION PROTECTION:

Deploys decoys throughout the operating file system. Any attempt to encrypt, delete, or otherwise tamper with a decoy automatically terminates the process.

SYSTEM RECOVERY TAMPER PROTECTION:

Blocks unauthorized access to shadow copies and terminates unauthorized processes that try to delete them, securing system recovery files.

CREDENTIAL THEFT PROTECTION:

Deterministically protects domain credentials stored in LSASS application and browser credentials stored by Chrome and Edge. Blocks multiple types of credential dumping.

RUNTIME MEMORY PROTECTION WITH MOVING TARGET DEFENSE TECHNOLOGY (MTD):

Morphisec's MTD technology creates an unpredictable attack surface while leaving decoy traps in place of system resources. Ransomware that tries to execute is terminated and captured for forensic analysis.

Select Use Cases

STOP THE 30 PERCENT OF ATTACKS NGAV, EPP, AND EDR MISS

NGAV, EPP, and EDR are built to defend against file-based attacks with known signatures and behaviors. Morphisec's Automated Moving Target Defense stops the unknown attacks that lead to ransomware and data theft, preventing up to 95 percent of false positives and better protecting your company.

GO ON THE OFFENSIVE AGAINST RANSOMWARE

Morphisec is tested and proven to prevent ransomware, offering extensive coverage throughout the MITRE ransomware attack chain:

- **Encryption protection**
- **Shadow copy protection**
- **Credential theft protection**
- **AMTD-powered runtime memory protection**

DEFENSE IN DEPTH WITHOUT EXPENSE IN DEPTH

Stop drowning in false positive alerts from NGAV, EPP, and EDR/XDR. Morphisec's prevention-first technology is ultra-lightweight for negligible performance impact, and slashes up to 95 percent of false positives while automatically stopping advanced attacks.

SECURE LEGACY OPERATING SYSTEMS

Microsoft announced the January 2023 end of life for Windows 7, 8, 8.1 (and their embedded derivatives), and 2008 R2. Windows 2012 ends support in October 2023. Millions of devices will become "legacy," creating security risks inherent to unsupported systems. Morphisec for Windows and Linux legacy environments proactively prevents advanced attacks without performance impact.

MORPHISEC + ANY EDR = BETTER TOGETHER

Morphisec adds proven Defense-in-Depth to Microsoft Defender, CrowdStrike, SentinelOne, and more, adding a preventive security layer that blocks advanced attacks with no performance impact and no need for extra staff. Compatible with NGAV, EPP, EDR/XDR/MDR and SIEM, with APIs for SOC/SIEMs.

Morphisec Key Benefits

BETTER SECURITY

Proven, prevention-first security layer enables continuous visibility and application control for Windows and Linux. Stops supply chain attacks, data theft, fileless attacks, ransomware, zero-days, and other advanced attacks in-memory, augmenting detection-based solutions like NGAV, EPP, and EDR/XDR.

OPERATIONAL SIMPLICITY

Ultra-lightweight 6MB/2 CPU cycle agent has negligible impact on performance or compute capacity. Purpose-built for Windows and Linux servers and seamlessly integrates into tech stacks.

Doesn't require continuous monitoring or security updates for rules, signatures, or incidents of compromise. No need to reboot and no internet connection needed—can be air-gapped.

LOWER TOTAL COST OF OWNERSHIP

Automated prevention and minimal false positives reduce labor costs.

- **No human involvement needed to stop attacks; negligible false positives to monitor**
- **Simple and fast installation in hours/days vs. weeks or months. Proven deployment of 6,000+ agents in one hour**
- **Negligible maintenance required**

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. 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. Gartner Emerging Tech: Security— The Future of Cyber Is Automated Moving Target Defense. Lawrence Pingree, Carl Manion, Matt Milone, Sean O'Neill, Travis Lee, Mark Pohto, Mark Wah, Ruggero Contu, Dan Ayoub, Elizabeth Kim, Rustam Malik, Nat Smith, 28 February 2023. https://engage.morphisec.com/gartner-automated-moving-target-defense