

Anti-Ransomware

Prevent ransomware attacks







Morphisec's ultra-lightweight anti-ransomware features offer critical Defense-in-Depth for endpoints, servers, and cloud workloads.




Ransomware Risk and Impact

In 2022, the United Kingdom's National Cyber Security Center (NCSC) warned ransomware was the biggest cybersecurity threat facing the world¹, describing the attacks as "unrelenting." IBM reports ransomware attacks are becoming costlier. From 2021 to 2022, breaches caused by ransomware grew 41 percent and took 49 days longer to identify and contain compared to other data breaches. The average total cost of a destructive ransomware or wiper attack is now \$5.12 million.²


CORE CAPABILITIES

-  Data encryption and destruction protection
-  System recovery tamper protection
-  Credential theft protection
-  Automated Moving Target Defense runtime memory protection

BENEFITS

-  No productivity or performance impact
-  Integrates seamlessly with any cybersecurity tech stack
-  Addresses the entire MITRE ransomware attack chain

RESULTS

-  Stops undetectable ransomware that bypasses NGAV, EPP, and EDR/XDR solutions

"The Future of Cyber Is Automated Moving Target Defense"³

Gartner.

Ransomware Evolution

Ransomware risk is increasing with the rise of ransomware as a service (RaaS) lowering barriers to entry, and fileless, in-memory attacks built to evade detection-based cybersecurity solutions such as next generation anti-virus (NGAV), endpoint protection platforms (EPP), and endpoint detection and response (EDR/XDR). To counter this risk, organizations are turning to prevention-first technology with capabilities that address the entire ransomware attack chain and close the in-memory security gap.

MITRE Ransomware Attack Chain



Prevent Ransomware With Defense-In-Depth

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 your cybersecurity tech stack:

Data Encryption & Destruction Protection

System Recovery Tamper Protection

Credential Theft Protection

Runtime Memory Protection with Automated Moving Target Defense (AMTD)



MORPHISEC
ANTI-RANSOMWARE



Data Encryption & Destruction Protection

This security layer prevents ransomware encryption by deploying decoys throughout the Windows file system. Any attempt to tamper with, delete, modify, or encrypt a decoy triggers Morphisec to kill the ransomware processes in the system. It's a defensive layer at the final "impact" stage of an attack chain. It keeps endpoints and servers safe, offers visibility to incident response teams, and gives you time to contain an incident quickly and effectively. And because this module has no CPU or I/O overhead, it doesn't affect user productivity.



System Recovery Tamper Protection

System shadow copies enable files to be restored in the event of data loss, including from ransomware attacks. So a key element of ransomware attacks is to prevent recovery by deleting shadow copies and backups. Morphisec blocks unauthorized access to shadow copies, automatically terminating unauthorized processes that try to tamper with them, keeping shadow copies safe.



Credential Theft Protection

This feature prevents adversaries from stealing credentials and gaining privilege escalation. Morphisec provides deterministic protection for user credentials stored in Chromium-based browsers such as Chrome and Edge, and blocks credential dumps from Windows Local Security Authority Subsystem Service (LSASS), Remote Desktop Protocol (RDP), DC-Sync, and SAM hashes. Unauthorized processes trying to access system credentials are automatically terminated.



Runtime Memory Protection with Automated Moving Target Defense (AMTD)

Morphisec's patented, Automated Moving Target Defense (AMTD) technology blocks multiple stages in the MITRE ransomware attack chain, from initial access to persistence, privilege escalation, defense evasion, lateral movement, and the impact phase. AMTD morphs (randomizes) runtime memory to create an unpredictable attack surface, moving application memory, APIs, and other system resources while leaving decoy traps in their place. Code that tries to execute on a decoy is automatically terminated and captured for forensic analysis, while the actual system resource remains protected.

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://www.zdnet.com/article/ransomware-attacks-are-the-biggest-global-cyber-threat-and-still-evolving-warns-cybersecurity-chief/>
2. <https://www.ibm.com/reports/data-breach>
3. <https://engage.morphisec.com/gartner-automated-moving-target-defense>