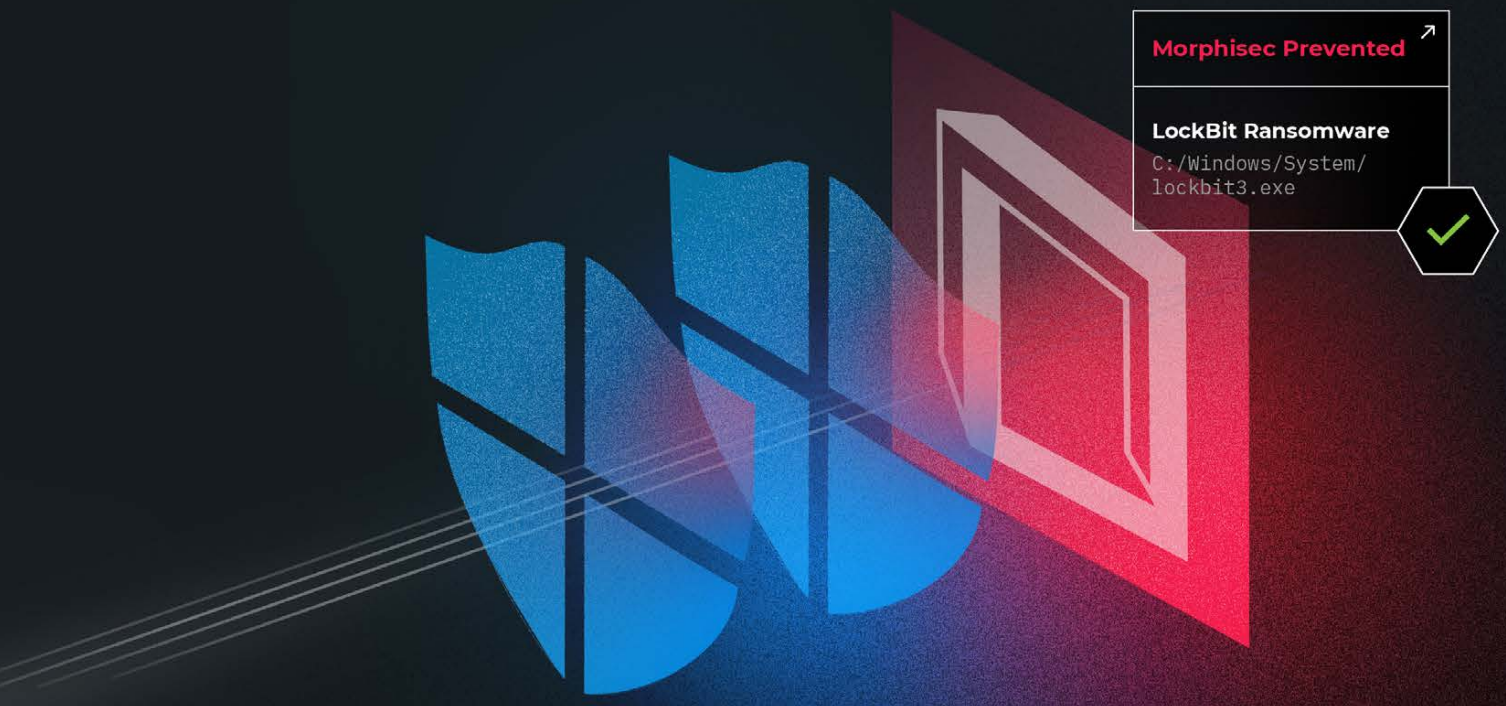
MORPHISEC

WHITE PAPER

FORTIFY YOUR ENDPOINT AGAINST RANSOMWARE AND ADVANCED THREATS

Achieve Defense in Depth with Morphisec integrated into Microsoft Defender for Endpoint



Microsoft Security

Table Of Contents

Executive Summary

CHALLENGE

- As enterprises increasingly depend on Microsoft O365 E3/E5 licenses for endpoint security, they face a relentless evolution of ransomware attacks designed to penetrate Microsoft Defender's standard protective measures.
- This escalating threat landscape demands an additional, robust layer of defense to shield against sophisticated ransomware tactics.

SOLUTION

- Morphisec fortifies Microsoft Defender for Endpoint by seamlessly integrating a decisive layer of protection, powered by Automated Moving Target Defense (AMTD) technology.
- Unlike traditional defenses, AMTD confronts ransomware attacks by dynamically altering endpoints, creating a hostile environment for attackers and preventing them from gaining a foothold.

RESULTS

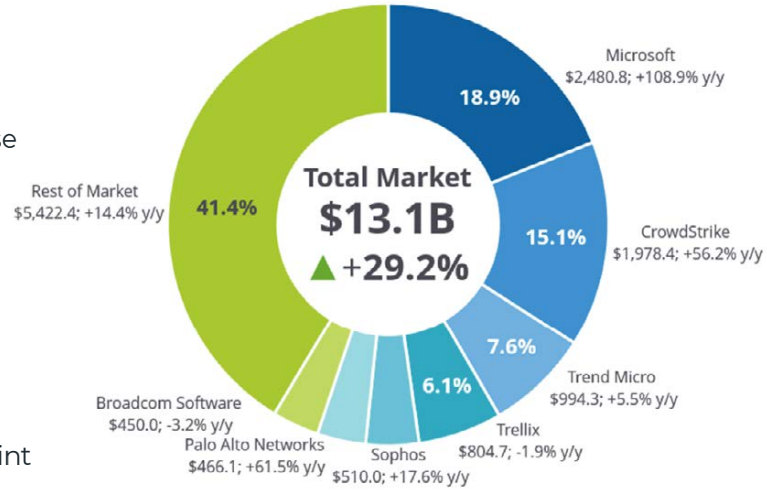
- Morphisec, integrated into Microsoft Defender, transforms the organization's ransomware protection into a formidable barrier.
- This strategic integration significantly reduces the risk of breaches, streamlines security operations and threat management, and optimizes the organization's overall security posture.

Introduction

The rise of Microsoft Defender for Endpoint

Amidst a landscape where efficiency and cost-effectiveness are a priority, security leaders are increasingly choosing Microsoft 365 Enterprise plans, with **Office 365 E3 and E5** licenses. An integral component of these plans is **Microsoft Defender for Office 365**, which provides robust frontline defense against cyber threats.

Worldwide Corporate Endpoint Security Share Snapshot



Source: IDC, "Worldwide Corporate Endpoint Security Market Shares", **link**

Microsoft Defender is the fastest growing endpoint protection platform, boasting over a 19% market share, and named a market leader, according to an **IDC report**. Additionally, the solution is consistently ranked as a "leader" in the Gartner **Magic Quadrant for Endpoint Protection** (Gartner subscribers can access the 2023 report **here**).

Microsoft Defender for Endpoint, also known as MDE (Microsoft Defender EDR) or MDEP (Microsoft Defender for Endpoint), and previously referred to as Windows Defender ATP, which encompasses **Microsoft Defender EDR and Plan 2 (P2)**, offers comprehensive protection against a multitude of sophisticated cyber-attacks.

Yet, when faced with the evolving complexity of ransomware attacks, this solution falls short. The absence of a critical ransomware defense layer means organizations are not fully equipped to stop advanced ransomware attacks.

The Challenge – Ransomware and Evasive Threats are Evolving

According to the IBM **Cost of a Data Breach Report 2023**, only one-third of reported breaches were identified by the reporting organization's internal security teams and tools; 27% of breaches were disclosed by attackers (typically classified as ransomware) at an average cost of USD$5.23M. Notably, breach events disclosed by attackers averaged 233 days to identify (MTTI - Mean Time to Identify) and 87 days to contain (MTTC - Mean Time to Contain), which is 80 days longer (or 28.2%) than the MTTI and MTTC for breaches identified by the organization's security teams and tools.

USD 30B

2023 Global Ransomware Damages

Ransomware attacks continue to escalate in frequency, sophistication, and post-breach damages; in 2023, ransomware damages **exceeded USD 30 billion** — an all-time high. Threat actors are increasingly using evasive techniques to deploy ransomware and other threats, which can bypass the protection provided by endpoint protection solutions.

Microsoft Defender for Endpoint detects and responds to cyber threats with recognizable signatures, behavioral patterns and Indicators of Attacks (IOAs). Endpoint Detection and Response (EDR) solutions are fundamental base layer of protection that have become a best practice.

With Microsoft Defender's rising market share, threat actors will ensure payloads delivered to targets will include evasive techniques capable of and tested to bypass this solution.

The rise of these targeted and evasive threats means that no single security solution can be relied upon to stop attacks. Instead, security teams must establish a multi-layered security obstacle course between critical assets and potential threats.

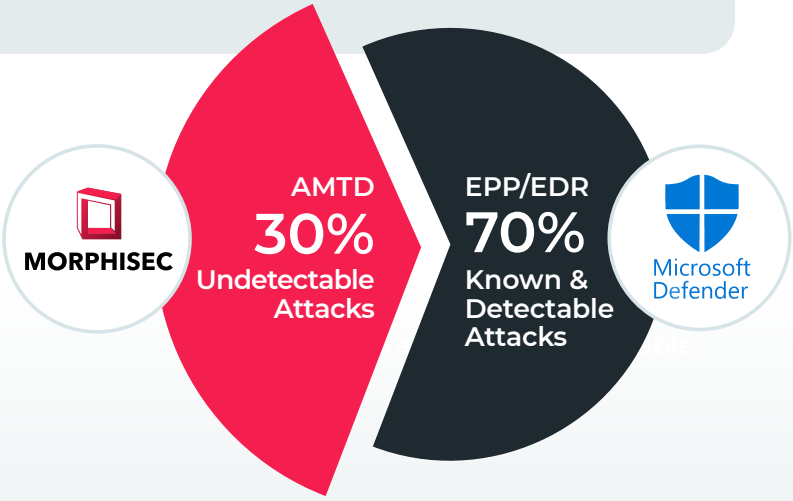
Microsoft Defender for Endpoint protection gaps exist due to:

- Reliance on reactive threat classification, using known signatures and Indicators of Attacks (IOAs).
- Dependance on cloud-based connectivity for updated threat intel.
- A lack of in-memory protection, making it prone to EDR evasion techniques.
- Insufficient **legacy OS protection** due to reliance on Microsoft Defender AV for telemetry, and other OS architectural capabilities such as AMSI and ETW.
- Skills requirements, including costly and time-consuming analysis of security alerts for incident response.

Like all endpoint protection solutions, Microsoft Defender for Endpoint cannot stop what it cannot detect.

Gartner emphasizes[1], "In today's volatile cyber landscape, detection and response is simply not enough — organizations of all sizes need more to stay ahead of the most advanced attackers."

Gartner



Read more about Microsoft Defender for Endpoint security gaps and How Morphisec Helps

Learn More

Achieving Defense-in-Depth

Member of Microsoft Intelligent Security Association

Microsoft

Morphisec, a member of the **Microsoft Intelligent Security Association (MISA)** brings Defense-in-Depth to Microsoft Defender for Endpoint users.

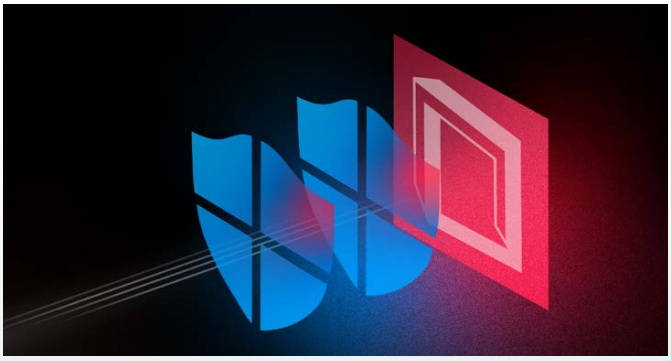
Morphisec fortifies your organization by diminishing the blast radius of attacks, to pre-emptively reduce the organization's exposure to cyber risk, proactively prevent advanced threats and ensure optimal anti-ransomware defense.

Powered by **Automated Moving Target Defense (AMTD)**, this streamlined solution seamlessly integrates with Microsoft Defender for Endpoint, enhancing the existing protection capabilities, or operating independently when necessary.

The premise of AMTD maintains that instead of attempting to identify threats, move the target.

Morphisec's efficacy is proven by real-world analysis of 7,000+ customers, nine million endpoints and 30,000 daily incidents discovered that installed detection-based solutions struggle to stop. As noted by the **2024 Picus Security Red Report**, over 30% of threats observed in the wild contain defense evasion techniques.

Morphisec proactively prevents advanced ransomware, in-memory, fileless and other threats capable of bypassing the protection provided by Microsoft Defender for Endpoint, closing this critical security gap.

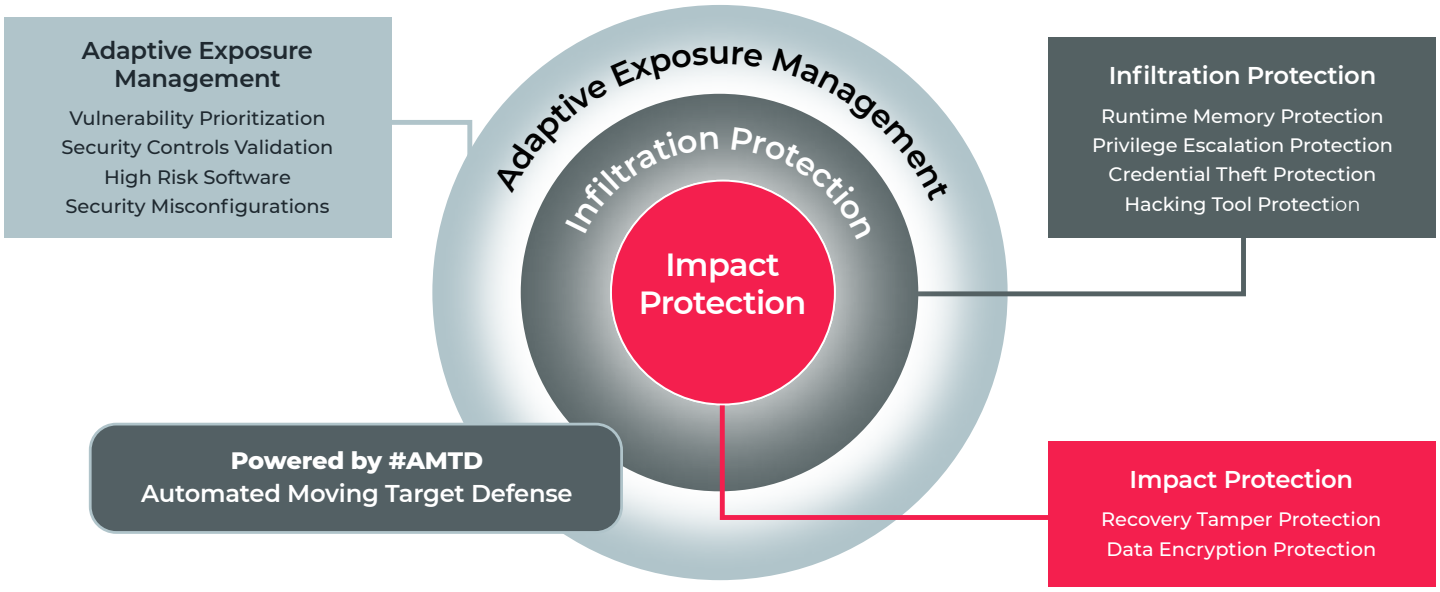


Gartner emphasizes[1], "for every attack prevented using AMTD, the downstream implications on security operations and IR personnel time, data processing, analysis, latent response, false positive volume and forensics costs can be significantly reduced." [2]

Gartner

Anti-Ransomware Assurance Suite

Morphisec's Anti-Ransomware Assurance Suite is proven to stop ransomware by providing distinct layers of anti-ransomware protection, to pre-emptively reduce the organization's exposure, and proactivelyprevent the attacks at multiple phases, from early infiltration attempts to protecting critical system resources and data when ransomware attempts to execute.



Adaptive Exposure Management

Elevate your security posture with Adaptive Exposure Management that prioritizes vulnerabilities, automates the assessment of your security controls, identifies high-risk software, and addresses security misconfigurations.

Infiltration Protection

Prevent the execution of ransomware attacks at early infiltration stages with Morphisec's prevention-first technology that constantly changes a system's configuration or environment. This makes it harder for attackers to exploit vulnerabilities as the attack surface is always shifting.

Impact Protection

Safeguard your systems against the ransomware impact phase with dedicated anti-ransomware protection that proactively defends critical assets and files with a prevention-first strategy, minimizing recovery times and strengthening your anti-ransomware stance.

Read more about Morphisec's Anti-Ransomware Assurance Learn More

Seamless Ransomware Defense with Morphisec and Microsoft Defender for Endpoint

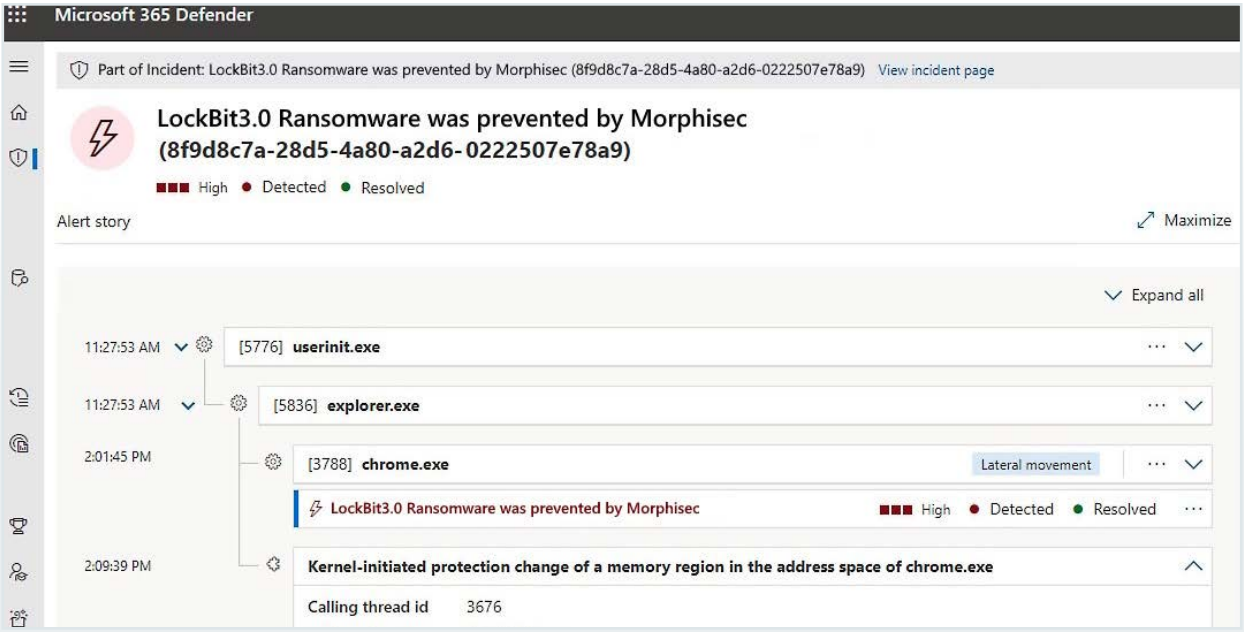
The Morphisec platform integrates seamlessly with Microsoft Defender for Endpoint to prevent ransomware, and highly evasive threats, providing full visibility into the attack chain. Morphisec delivers high priority alerts directly into the Microsoft Defender for Endpoint console to assist security analysts with event prioritization. This integration helps transition into Microsoft E5 license and reduces an organization's Total Cost of Ownership (TCO) by removing the need for an additional third-party EDR.

Integration overview

- Morphisec delivers security alerts into the Defender EDR console, including attack details and analytics.
- The alerts are defined as high priority, prevented events.
- The Morphisec alerts can be viewed and handled by the security analysts managing Defender EDR.

Benefits

- Morphisec alerts are high priority – assists with alert prioritization and reduces analyst fatigue.
- Defense-In-Depth is enhanced by preventing ransomware execution, in-memory, and evasive threats.
- Total cost of ownership (TCO) savings are realized with the removal of additional third- party EDR.



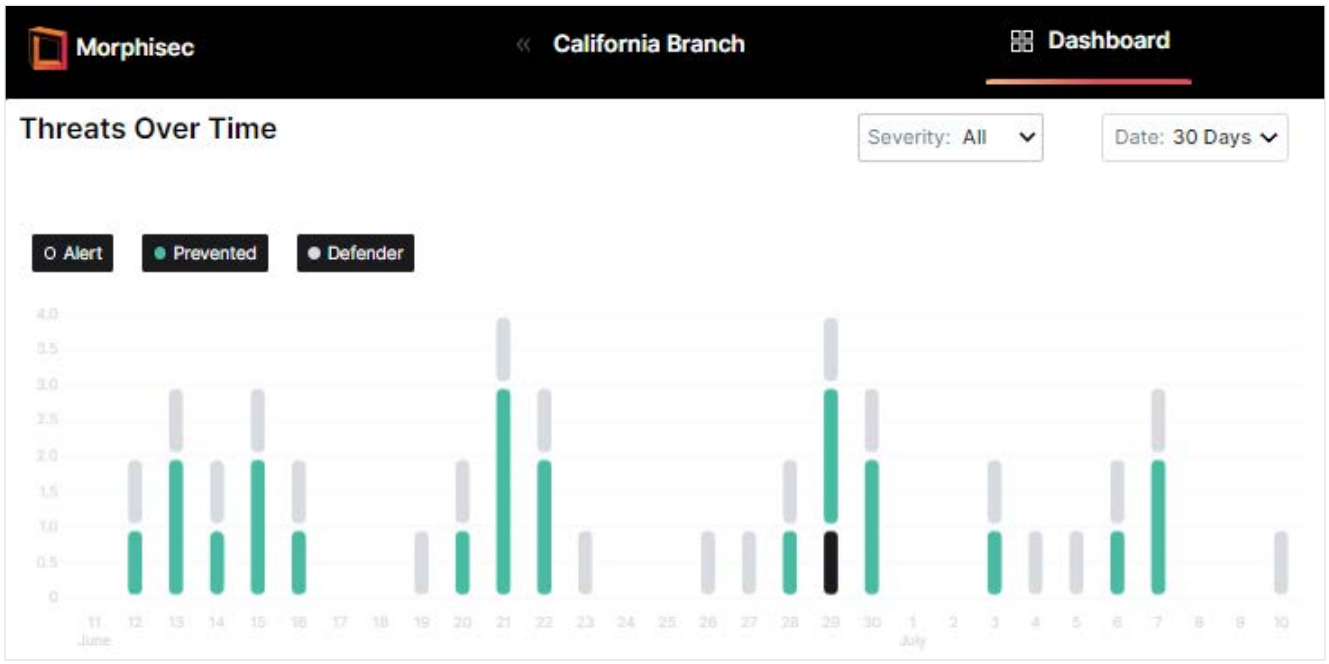
Morphisec alerts are delivered into the Microsoft Defender for Endpoint console

Read more about Morphisec's integration with Defender EDR

Learn More

Integration with Microsoft Defender Antivirus

Morphisec provides a single pane of glass for both advanced threat prevention and baseline protection by serving as the management platform for Microsoft Defender AV. Morphisec receives Defender AV alerts and configures the AV including Windows Firewall, Device Control, providing organizational wide visibility, through a centralized management platform.



The Morphisec console serves as the management application for Microsoft Defender AV

"The relationship between Microsoft and Morphisec was really key for us. Knowing the two tools could work together as one, stopping known and unknown attacks while functioning from one dashboard was key. We knew with that close relationship and integration we felt confident that any future upgrades or enhancements will be seamless for us."

– John Janthor, Chief Information Officer at Radwell International

Read more about Morphisec's integration with Defender Antivirus

Learn More

Summary

Better Together: Morphisec Anti-Ransomware Assurance + Microsoft Defender for Endpoint

Morphisec takes the capabilities of Microsoft Defender for Endpoint to the next level by adding an essential security layer for comprehensive ransomware defense. Morphisec's seamless integration with Microsoft Defender for Endpoint fills security gaps while fortifying the last mile of defense with the highest level of anti-ransomware assurance.

Key benefits

Continuous Monitoring and Ransomware Exposure Management —Ensures Microsoft Defender for Endpoint is operational and functioning as intended and provides a clear prioritization to remediate software vulnerabilities.

Advanced Anti-Ransomware Defense — Surpassing conventional protection to prevent even the most sophisticated ransomware from bypassing endpoint protections. Provides a multi layered defensive approach to stop ransomware across multiple attack phases.

Improved Cybersecurity Posture —Boosts audit scores and helps in achieving compliance, which can contribute to reduced cyber insurance premiums, thus enhancing the overall cybersecurity posture.

Enhanced operational efficiency — By preventing threats as early as possible and classifying them accurately, Morphisec significantly reduces the time and costs for tech resources as well as the financial impact.

Together, Morphisec and Microsoft Defender for Endpoint deliver a powerful and integrated defense system that diminishes the blast radius of ransomware attacks.

This empowers organizations to maintain a strong security posture in the face of increasingly sophisticated threats, providing peace of mind, and ensuring operational continuity.

"The Morphisec and Defender EDR integration helps us to understand which solution reacted to an incident first. Morphisec acts as a fail safe for attacks that bypass the EDR — it's the last line of defense."

– Alexander Realpe, Head of Security and Risk at Bupa Global Latin America

See how Morphisec can complement your Microsoft Defender for Endpoint investment — book a demo today.

See Morphisec in action

Experience advanced anti-ransomware, threat prevention, and vulnerability prioritization

Get a Demo

[1] Gartner, Emerging Tech: Security — Emergence Cycle for Automated Moving Target Defense, Lawrence Pingree, Carl Manion, Mark Pohto, Travis Lee, Rustam Malik, Ruggero Contu, Dan Ayoub, Dave Messett, 01 May 2023

[2] Gartner Emerging Tech: Security — AMTD Transforms Endpoint Protection, Lawrence Pingree, Rustam Malik, published 15 January 2024

Gartner Disclaimer

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Morphisec

Founded in 2014, Morphisec, a pioneer in blast radius resiliency, keeps your business safe by intelligently anticipating and neutralizing threats - minimizing the impact and blast radius of cyber incidents and ensuring uninterrupted business operations without the need for constant tech team intervention or impact to performance.

Powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity, Morphisec protects over 7,000 organizations across nine million Windows and Linux endpoints, servers and workloads. Morphisec stops thousands of advanced attacks daily at Lenovo/Motorola, TruGreen, Covenant Health, Citizens Medical Center, and many more. Learn more at www.morphisec.com

To learn more, visit morphisec.com/schedule