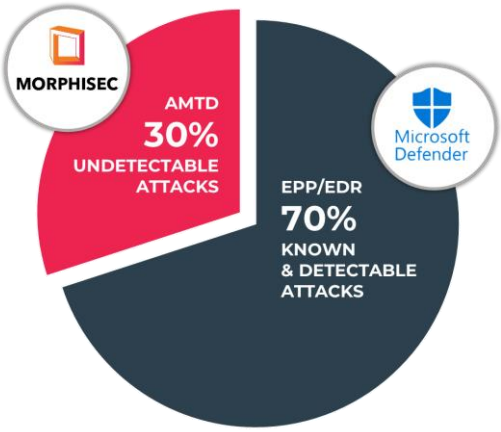
MORPHISEC

The Microsoft Defender EDR Security Gap

Problem Defined

Microsoft Defender EDR (MDEP / Defender P2) detects and responds to cyber threats with recognizable signatures and behavioral patterns. However, threat actors are deploying evasive techniques capable of bypassing the protection provided by Microsoft Defender EDR.

Defender EDR cannot stop what it cannot detect.



Closing The Gap: Morphisec + Defender EDR

Instead of relying on detection, Morphisec's Automated Moving Target Defense (AMTD) protects by morphing — randomizing —system resources, creating an unpredictable attack surface, while malicious code that attempts to execute is instantly trapped and blocked as soon as it attempts to run.

Instead of attempting to identify threats – move the target.

Morphisec

Protection Efficacy

- ✓ True prevention without prior knowledge (signatures, rules, IOAs, etc.).
- ✓ Halts the execution of threats versus analysis-based reactive detection.
- ✓ Prevents sophisticated evasive and memory-based attacks capable of bypassing EPPs/EDRs.
- ✓ Deterministic threat prevention, with minimal false positives.

Operational Efficiency

- ✓ Extremely lightweight agent with negligible performance impact (CPU, RAM) highly suitable for critical environments, Windows & Linux Servers, and Workloads.
- ✓ Fully autonomous, does not require connectivity to the cloud for prevention (works offline or online).
- ✓ Full support for Legacy operating systems since the solution does not rely on modern OS visibility capabilities.
- ✓ Immediate threat prevention, providing conclusive prioritization of alerts, with minimal false positives.
- ✓ Does not require additional headcount. Easy to deploy, operate and maintain.

Defender EDR

Protection Gaps

- × Relies on reactive threat classification, using known signatures, behavioral rules, and ML.
- × IOA-based detection discovers malicious behaviors post-breach.
- × Lacking in-memory protection, prone to evasive techniques.
- × Generates false positives, specifically with binaries.

Operational Gaps

- × Critical performance penalties on Servers/Workloads (Windows, Linux).
- × Requires cloud-based connectivity to ensure using fully updated IOAs.
- × Lacks Legacy OS due to reliance on Defender AV for threat visibility and telemetry.
- × Delayed response time allows attackers to achieve persistence. Generates false positives, leading to alert fatigue and missed threats.
- × Requires skilled and costly analysis and maintenance.

MORPHISEC

Evidence: Threats bypassing Defender EDR, prevented by Morphisec

Attack Prevented	Description
Metasploit backdoor Read more	Metasploit framework is a powerful tool used by cybercriminals as well as ethical hackers to probe for vulnerabilities. Morphisec blocked multiple instances of Metasploit which bypassed Defender EDR.
Cymulate Attack Simulation	Cymulate is used by Pen Testers for security audits, providing threat and attack simulation based on in-the-wild malware. Morphisec prevents the usage of Cymulate, helping customers increase their security scores.
GuLoader	GuLoader is a widely used malware known for its complex obfuscation techniques, distribute malware such as FormBook, Remcos, AgentTesla and more. Morphisec blocked multiple GuLoader variants which bypassed Defender EDR.
BlueKeep exploit Read more	Morphisec blocked real-life BlueKeep attacks (an RDP network vulnerability that enable remote code execution), that were undetected by Defender EDR.
RedLine Stealer Read more	RedLiner is an info stealer targeting windows credentials, available as 'Malware as a Service', and observed to load other malware. Morphisec consistently prevented RedLine variants bypassing Microsoft EDR.
Babuk ransomware Read more	Morphisec prevented a major breach of a new variant of Babuk ransomware. The variant was observed to evade Defender EDR for over two weeks post-attack.
SMB Server Exploit (Windows Legacy)	Protection of Legacy machines running Windows 7: Morphisec prevented multiple Server Message Block (SMB) protocol exploits, attempting to achieve lateral movement. The attack continually bypassed protection by Defender EDR.
Browser Credential Theft	Morphisec prevented multiple credential harvest attempts saved in Edge, Internet Explorer, and Chrome browsers (across multiple Windows OS, including Legacy systems) Window 7, 2008 R2 and 2012 – while bypassing Defender EDR.

SUMMARY

Trusted by 5,000+ companies across 9M+ endpoints and servers, Morphisec's AMTD technology prevents supply chain attacks, ransomware, fileless attacks, zero-days and evasive attacks that other solutions don't.
It closes critical security gaps in Defender EDR to stop the most advanced attacks, with negligible performance impact with no additional headcount requirements.

Morphisec + Defender EDR offers fully optimized Defense-In-Depth to protect against today's evolving threat landscape.

"Morphisec complements our Defender AV and EDR infrastructure with a true prevention methodology. This helped in our decision to retire our previous EDR and transition to O365 E5".

"Morphisec is easy to install, operate and maintain, with highly dedicated support"

CISO of a Global, $13b Health Insurance company

Gartner "Automated Moving Target Defense is the Future of Cyber" Read the 2023 Report