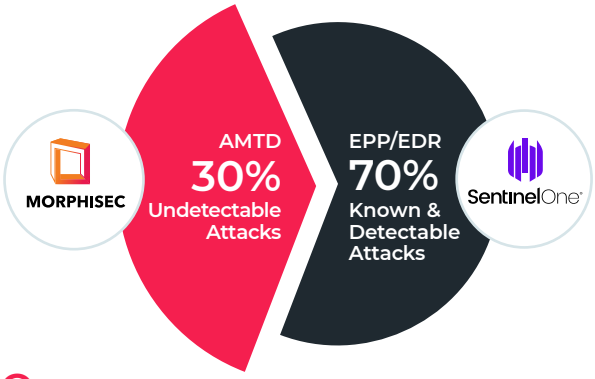
MORPHISEC

The SentinelOne Security Gap

Problem Defined

SentinelOne Singularity Endpoint 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 SentinelOne.

SentinelOne cannot stop what it cannot detect.



Closing The Gap: Morphisec + SentinelOne

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	SentinelOne Singularity
Protection Efficacy	**Protection Gaps**
✓ True prevention without prior knowledge (signatures, rules, IOAs, etc.).	✗ Relies on reactive threat classification, using known signatures, behavioral rules, and ML.
✓ Halts the execution of threats versus analysis-based reactive detection.	✗ IOA-based detection discovers malicious behaviors post-breach.
✓ Prevents sophisticated evasive and memory-based attacks capable of bypassing EPPs/EDRs.	✗ Prone to EPP and EDR evasive techniques, in-memory attacks.
✓ Deterministic threat prevention, with minimal false positives.	✗ Generates false positives, specifically with binaries.
Operational Efficiency	**Operational Gaps**
✓ Extremely lightweight agent with negligible performance impact (CPU, RAM) highly suitable for critical environments, Windows & Linux Servers, and Workloads.	✗ Critical performance penalties on Servers/Workloads (Windows, Linux).
✓ Fully autonomous, does not require connectivity to the cloud for prevention (works offline or online).	✗ Requires cloud-based connectivity to ensure using fully updated IOAs.
✓ Full support for Legacy operating systems since the solution does not rely on modern OS visibility capabilities.	✗ Lacks Legacy OS (Windows, Linux) protection due to insufficient OS visibility.
✓ Immediate threat prevention, providing conclusive prioritization of alerts, with minimal false positives.	✗ Delayed response time allows attackers to achieve persistence. Generates false positives, leading to alert fatigue and missed threats.
✓ Does not require additional headcount. Easy to deploy, operate and maintain.	✗ Requires skilled and costly analysis and maintenance.

Evidence: Threats bypassing SentinelOne, prevented by Morphisec

Attack Prevented	Description
Cobalt Strike backdoor Read more	Cobalt Strike is used by threat actors to infiltrate networks, and by Pen Testers as an adversary simulation tool. Morphisec blocked multiple instances of using CobaltStrike which bypassed detection by SentinelOne.
Metasploit backdoor Read more	Similar to Cobalt Strike, Metasploit framework is a powerful tool which can be used by cybercriminals as well as ethical hackers to probe for vulnerabilities. Morphisec blocked multiple instances of Metasploit which bypassed SentinelOne.
Babuk ransomware Read more	Morphisec prevented a major breach by a new variant of Babuk ransomware. The malicious side-loaded DLL was detected by SentinelOne, but the detection did not prevent the Shellcode injection phase that executed the ransomware.
AMSI bypass	Morphisec prevented attacks that attempted to bypass the Windows Anti-malware Scan Interface (AMSI). SentinelOne did not detect the attacks. Furthermore, SentinelOne is dependent on AMSI for its script detection mechanisms.
Gamarue malware	Morphisec blocked multiple variants of Gamarue (malware that downloads files to enable information theft) that evaded SentinelOne. Gamarue is usually executed from USB or .ISO devices through windows legitimate processes.
Defense evasion – Reflective code injection Read more	Morphisec prevented multiple shellcode and executable injections into legitimate applications after SentinelOne missed an attack where malicious codes attempted to persist through applications such as regsvr, rundll32, InstallUtils, Msbuild.
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 SentinelOne.
Quakbot Malware Read more	Qakbot malware is a multi-purpose banking trojan used to exfiltrate financial information and deliver next-stage payloads such as ransomware. Morphisec prevented multiple Qakbot variants that bypassed SentinelOne.

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

"Morphisec prevented multiple attacks on our company – all which bypassed our resident EDR."

"We're a manufacturing company, with an infrastructure containing Legacy systems. Their full compatibility was a key to choosing the solution."

Global CISO of a Multi-National, $3B Pharmaceuticals company

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