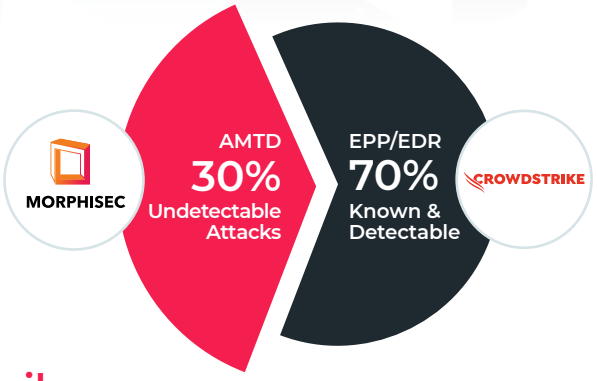
MORPHISEC

The CrowdStrike Security Gap

Problem Defined

CrowdStrike Falcon detects and responds to cyber threats with recognizable signatures and behavioral patterns. However, threat actors have evolved to deploying evasive techniques capable of bypassing the protection provided Crowdstrike.

CrowdStrike cannot stop what it cannot detect.



Closing The Gap: Morphisec + CrowdStrike

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	CrowdStrike Falcon
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, 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 CrowdStrike, prevented by Morphisec

Attack Prevented	Description
Cobalt Strike backdoor Read more	A major financial company calls Morphisec their "secret weapon" as it stops multiple pentesting tools, which bypass their installed CrowdStrike, and include Cobalt Strike.
Babuk ransomware Read more	Morphisec prevented a major breach of a new variant of Babuk ransomware. The variant was observed to evade CrowdStrike for over two weeks post-attack.
AMSI bypass	Morphisec prevented attacks that attempted to bypass the Windows Anti-malware Scan Interface (AMSI). CrowdStrike did not detect the attacks. Furthermore, CrowdStrike 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 CrowdStrike. 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 CrowdStrike missed an attack where malicious codes attempted to persist through applications such as regsvr, rundll32, InstallUtils, Msbuild.
Jupyter info-stealer Read more	Morphisec prevented multiple info-stealer executions on customers' environments including Jupyter, a fileless variant of stealthy info-stealer that executes within legitimate applications and is frequently found on CrowdStrike protected environments.
BlueKeep exploit Read more	Morphisec blocked real-life BlueKeep attacks (an RDP network vulnerability that enable remote code execution), that were undetected by CrowdStrike.
OneNote vulnerability delivering Emotet, Qakbot Read more	Morphisec prevented Emotet, Qakbot, and other malware which bypassed CrowdStrike and were observed to be delivered through OneNote vulnerabilities.

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 CrowdStrike to stop the most advanced attacks, with negligible performance impact with no additional headcount requirements.

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

"Morphisec is true prevention, without relying on signatures or behavior updates, filling the gaps of our XDR solution."

"Morphisec helps us pass our annual pentesting, boosting our BitSight scores, and reducing our Cyber Insurance costs."

CISO of a Nasdaq-100, $20B+ Manufacturing company

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