



ANALYSIS

MORPHISEC ATTACK ANALYSIS ON-DEMAND

Gain a deeper understanding of the threats your organization is facing when and where you need it. Morphisec experts perform a deep-dive analysis of granular attack data and recommend actions to limit damage and keep your organization safer.

Advanced Analysis for Advanced Threats

Your Morphisec Endpoint Threat Prevention already provides detailed information about every attack it blocks: the attacked user and machine, date and time, attack type (the file and its signature, malicious URL or evasive malware variant). Since Morphisec prevents an attack at its earliest stages, this information, found in the Attacks dashboard of the Morphisec management console, is generally sufficient for rapid incident response and to track ongoing incidents.

However, the Morphisec system also captures unique, technical data about the attack's full execution stack and memory access, which can be used to reconstruct the attack lifecycle, its intended scope and uncover other valuable insights. This information is not contained on the default console, but can be accessed as part of the Morphisec Attack Analysis On-Demand service.

This service puts Morphisec's team of cyber professionals to work for you, offering the support you need to understand specific threats better and help prevent future instances of the attack. Our experts will analyze your threat data to reconstruct an attack, identify and prioritize threats, and recommend remediation strategies.

Service Components

Upon request, Morphisec investigators analyze any attack prevented by Morphisec Endpoint Threat Prevention and provide a comprehensive report of their findings and recommendations. Depending on your company's specific needs, this can include:

- A full walkthrough of the attack lifecycle starting from the root cause – how did the attack penetrate your organization? Were there any preliminary stages?
- A determination of the scope of impact – did the attack attempt to run on additional machines or attack additional users?
- Remediation recommendations and suggested actions to prevent attack repercussions and avoid similar attack instances in the future, if possible.
- Correlation, when possible, to a specific CVE or a known threat in order to verify patching levels.

How it Works

Morphisec Attack Analysis On-Demand is a for-fee, remote expert service. Morphisec professionals may take up to three business days to analyze the attack, document and prepare a report.

This service requires that you provide Morphisec access to the following:

1. Morphisec dashboard
2. The attacked machine
3. Additional information that may be available in other organizational security tools

