Independent Tests of
Anti-Virus Software

Single Product Report

Morphisec Guard

TEST PERIOD: OCTOBER 2020
LAST REVISION: 27TH JANUARY 2021

WWW.AV-COMPARATIVES.ORG

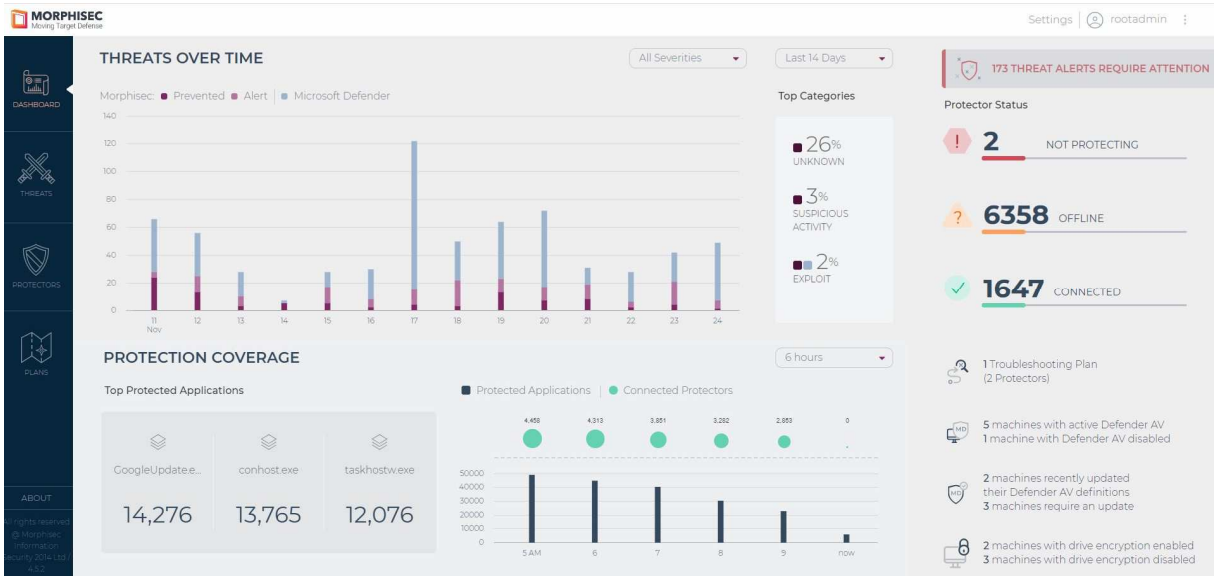
Content

Tested Product

Morphisec Guard 4.5 was evaluated by AV-Comparatives in October 2020.

***Note**: Morphisec Guard is a product which works in combination with Microsoft Defender. References to Morphisec/Morphisec Guard in this document apply to this combination.*

Product Thumbnail



Morphisec Unified Threat Prevention Platform management console

Executive Summary

Morphisec Guard was tested by AV-Comparatives to check whether the endpoint prevention product could provide effective prevention capabilities.

Morphisec Guard did exceptionally well at handling threats targeted at the user, before the threat could progress inside the user environment. The product demonstrated excellent exploit protection and several other safeguards to protect the enterprise end-user against the scenarios we tested. The product's management console was easy to use, intuitive, and provided contextual active response data. The product was easy to configure and deploy in a domain or workgroup environment.

Active Response / Prevention: An active response is an effective response strategy that combines detection with automatic prevention and reporting capabilities. Morphisec had an active response to **47 out of 49** scenarios across all the phases tested. This represents a cumulative active response rate of **95.9%**.

The table below depicts Morphisec's prevention & detection rates across Workflow-1 and Workflow-2, across the different phases and categories of attack.

Phases	Combined Prevention & Detection (T0: Time of Attack)	Combined Prevention & Detection (T1: 24 Hrs)
Phase 1 (Compromise & Foothold)		
Active Response & Detection	93.9%	93.9%
Phase 2 (Internal Propagation)		
Active Response & Detection	100%	100%
Phase 3 (Asset Breach)		
Active Response & Detection	N/A[1]	N/A[1]

Morphisec Guard offered strong prevention capabilities, preventing 93.9% of the scenarios in the "Initial Access" phase of the prevention workflow. One scenario was able to progress to Phase 2, but Morphisec Guard was able to prevent it before it could progress to Phase 3.

We tested a total of 49 scenarios, and only one of these was able to bypass the active response mechanism in two phases.

Phase 1:

- 46 out of 49 scenarios prevented & detected
- 1 scenario was able to progress to Phase 2

Phase 2:

- 1 out of 1 scenario prevented & detected

Phase 3:

- Not applicable, because no scenario was able to progress to Phase 3

[1] No scenario progressed to Phase 3

Reduction in TTP (Time to Prevent)

The ability of the product to rapidly identify and prevent a threat, and display relevant information, is a very important factor. This could also be referred to as the effective reduction in active time to respond. The table below provides a breakdown of Morphisec Guard's overall prevention rate. This is as measured at the time of the attack (T0) and then at 24 hours, Time (T1) = T0 +24 Hrs.

	Time of Attack (in hours)								
Time to Prevent	**0 (T0)**	**<1**	**<2**	**<5**	**<10**	**<15**	**<20**	**<24**	**24 (T1)**
Phase 1	93.9%	93.9%	93.9%	93.9%	93.9%	93.9%	93.9%	93.9%	93.9%
Phase 2	100%	100%	100%	100%	100%	100%	100%	100%	100%
Phase 3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Time to Active Response

Immediate protection and response against new attacks is critical. Attackers use different websites to host their attacks, in order to bypass reputation engines. Therefore, products that fail to prevent or respond to an attack in a timely manner may be too late to counter a threat.

We recorded the time the threat was introduced into the test cycle and how long it took the product to prevent it. Within the 24 window, cumulative protection and detection rates are calculated each hour until attacks were prevented and responded to by the product.

Validation Scenario Overview

The table below provides some examples of scenarios used as part of this test. We tested 49 operational enterprise scenarios, comprised of several different operational workflows under normal operational environments, executed by different user personas. The aim of this test was to evaluate if the tested product was able to prevent attacks, without having to triage the threats, while offering active response and reporting capabilities.

Scenario: A scenario comprises enterprise operational workflows with one or more attack samples, executed using different techniques.

Kill Chain:	Delivery Exploitation Installation	Installation Command and Control	Denial of Service Action on Objectives Command and Control	
MITRE:	Initial Access Execution Persistence	Privilege Escalation Lateral Movement Credential Access Discovery Defense Evasion	Collection Exfiltration Impact	MITRE ID:
Phase 1	Scenario 1, 2, 3 Scenario 4, 5, 6 Scenario 7, 8, 9			T1193, T1189, T1192 T1106, T1086, T1182 T1103, T1053, T1183
Phase 2		Scenario 10, 11, 12		T1068, T1046, T1003
Phase 3			Scenario 13, 14	T1113, T1485

Example Scenarios

Workflow-1 Phase-1: Initial Access

Based upon Prevention Workflow-1, Phase 1 (Endpoint Compromise and Foothold), we tested several scenarios using different file formats and methods, such as spear-phishing attachments and drive-by download attacks, to obtain initial access into the environment.

Workflow-1 Phase-2: Internal Propagation

If this scenario was successful, we moved into Phase 2 (Internal Propagation) and then finally Phase 3 (Asset Breach) of the prevention Workflow-1. We also tested some scenarios where an attacker is opportunistic and jumps directly from Phase 1 to Phase 3 as well.

Workflow-1 Phase-3: Asset Breach

For each of these phases we evaluated the Response Workflow-3 and Reporting Workflow-4 as stated in the methodology. **Note:** Every attempt was made to ensure that atomic test cases are not run as part of the workflow wherever applicable.

Based on the good-faith vulnerability disclosure policies, we are specifically NOT disclosing all the scenarios and the technique(s) used. Details of the missed attacks were provided to the vendor after the test.

Phase-1 Metrics: Endpoint Compromise and Foothold

Phase-1 can be triggered by an attack based on the MITRE ATT&CK and other methods, and can be effectively mapped to Lockheed's Cyber Kill Chain. This workflow can be operationalized by going through the various attack phases described below.

Initial Access: Initial access is the method used by the attacker to get a foothold inside the environment that is being targeted. Attackers may use a single method, or a combination of different techniques. Threats may come from compromised websites, email attachments or removable media. Methods of infection can include exploits, drive-by downloads, spear phishing, macros, trusted relationships, valid accounts, and supply-chain compromises.

Execution: The next goal of the attacker is to execute their own code inside the target environment. Depending upon the circumstances, this could be done locally or via remote code execution. Some of the methods used include client-side execution, third party software, operating system features like PowerShell, MSHTA, and the command line.

Persistence: Once the attacker gets inside the target environment, they will try to gain a persistent presence there. Depending upon the target operating system, an attacker may use operating system tools and features to gain a foothold inside the environment. These include registry manipulation, specifying dynamic-link-library values in the registry, shell scripts that can contain shell commands, application shimming, and account manipulation.

Morphisec Guard was subjected to the various attack phases as highlighted above. The resulting tables below showcase the product's active response and detection capabilities against the validated attack scenarios.

Tested Scenario	Description	Active Response	Detect
1	Customized File generated from Koadic	✓	✓
2	Custom Office Macro Document	✓	✓
3	Custom Office Macro Document	✓	✓
4	Custom Signed reverse Shell payload	✗	✓
5	Custom PowerShell File	✗	✓
6	Custom PowerShell File	✗	✓
7	Custom Office Macro Document	✓	✓
8	Custom Payload Generated from MSF Template	✓	✓
9	Custom Payload Generated from MSF Template	✓	✓
10	Custom Payload Generated from MSF Template	✓	✓
11	Custom Payload Generated from MSF Template	✓	✓
12	Custom Payload Generated from MSF Template	✓	✓
13	Custom Payload Generated from MSF Template	✓	✓
14	Custom Payload Generated from MSF Template	✓	✓
15	Custom Payload Generated from MSF Template	✓	✓
16	Macro enabled SYLK file	✓	✓
17	Internet Explorer Vulnerability	✓	✓
18	Custom Backdoored Obfuscated bat File	✓	✓
19	Custom Backdoored HTA File	✓	✓

20	Custom Backdoored Executable	✓	✓
21	Custom Backdoored Executable	✓	✓
22	Custom Backdoored Executable	✓	✓
23	Custom Remote Access Trojan	✓	✓
24	Custom Remote Access Trojan	✓	✓
25	Custom Payload Generated using windows shellcode injection	✓	✓
26	Custom Payload Generated using windows shellcode injection	✓	✓
27	Custom Payload Generated using windows shellcode injection	✓	✓
28	Custom Payload Generated using windows shellcode injection	✓	✓
29	Custom Payload Generated using windows shellcode injection	✓	✓
30	Custom Payload Generated using windows shellcode injection	✓	✓
31	Custom Payload Generated using windows shellcode injection	✓	✓
32	Custom Payload Generated using windows shellcode injection	✓	✓
33	Custom Payload Generated using windows shellcode injection	✓	✓
34	File less Attack	✓	✓
35	File and embedded command obfuscated using Content obfuscation	✓	✓
36	File obfuscated using Content obfuscation with variable naming	✓	✓
37	Custom Excel Macro	✓	✓
38	Customized File generated from Koadic	✓	✓
39	Customized File generated from Koadic	✓	✓
40	Customized File generated from Koadic	✓	✓
41	Customized File generated from Koadic	✓	✓
42	C# stager using DotNetToJScript using VBScript	✓	✓
43	C# stager using DotNetToJScript using JScript	✓	✓
44	Remote Service Vulnerability	✓	✓
45	Custom Payload Generated from MSF Template	✓	✓
46	Malicious Office Document 1	✓	✓
47	Malicious Office Document 2	✓	✓
48	Malicious Office Document 3	✓	✓
49	Malicious Office Document 4	✓	✓

Phase 1: Active Response versus Detection of Morphisec Guard

✗ - Indicates the product **failed** to prevent/detect (as applicable) the attack in the tested scenario.
✓ - Indicates the product **successfully** prevented or detected the attack in the tested scenario.

For an active response (preventative action) to occur, we verified whether the product made an active response during any of the three phases. Similarly, for a detection event to occur, we verified that the product saw various indicators that tied the threat to the adversary.

Morphisec Guard performed exceptionally well in blocking the attack scenarios before the attacker was able to get a foothold inside the environment.

Phase-2 Metrics: Internal Propagation

In this phase, the product should be able to prevent internal propagation. This phase is triggered when the initial identification and prevention of the threat fails. The product in this phase should enable the analyst to immediately identify and correlate the internal propagation of the threat in real time.

Privilege Escalation: In enterprise networks, it is standard practice for users (including system admins on their own personal computers) to use standard user accounts without administrator privileges. If an enterprise endpoint is attacked, the logged-on account will not have the permissions the attacker requires to launch the next phase of the attack. In these cases, privilege escalation must be obtained, using techniques such as user-access token manipulation, exploitation, application shimming, hooking, or permission weakness. Once the adversary gets a foothold inside the environment, it tries to escalate the privilege. For an active response to occur, we looked at various phases inside that method to see if there was a preventative action by the product.

For a detection event to occur, we looked at various indicators that tied the threat to the adversary.

Tested Scenario	Description	Active Response	Detect
4	Custom Signed reverse Shell payload	✓	✓
5	Custom PowerShell File*	N/A	N/A
6	Custom PowerShell File*	N/A	N/A

Phase 2: Active Response versus Detection of Morphisec Guard

✗ - Indicates the product **failed** to prevent/detect (as applicable) the attack in the tested scenario.
✓ - Indicates the product **successfully** prevented or detected the attack in the tested scenario.

**Scenarios 5 and 6 using custom PowerShell did not have Phase-2 associated with it. They count as unknown breaches.*

Discovery for Lateral Movement: Once the attacker has gained access to the target network, they will explore the environment, with the aim of finding those assets that are the potential target of the attack. This is typically done by scanning the network.

Credential Access: This is a method used by the attacker to ensure their further activities are carried out using a legitimate network user account. This ensures that they are able to access the resources they want and will not be flagged by the system's defences as an intruder. Different credential access methods can be used, depending on the nature of the targeted network. Credentials can be obtained on-site, using a method such as input capture (e.g. keyloggers). Alternatively, it might be done using the offline method, where the attacker copies the entire password database off-site, and can then use any method to crack it without fear of discovery.

Lateral Movement: The attacker will move laterally within the environment, so as to access those assets that are of interest. Techniques used include pass the hash, pass the ticket, and exploitation of remote services and protocols like RDP.

Phase-3 Metrics: Asset Breach

The final phase of the workflow is asset breach. This is the stage where an attacker starts carrying out their ultimate objective.

Collection: This involves gathering the target information – assuming of course that information theft, rather than sabotage, is the object of the exercise. The data concerned could be in the form of documents, emails or databases.

Exfiltration: Once the attacker has reached the objective of collecting the target information, they will want to copy it covertly from the targeted network to their own server. In almost all cases, exfiltration involves the use of a command-and-control infrastructure.

Impact: Having found and extracted the target information, the attacker will try to delete or destroy all the evidence of the attack that remains within the target network. An ideal scenario for the attacker is one in which the victim does not even realize that the attack has taken place. Whether or not this is possible, the attacker will try to manipulate data inside the target environment to ensure that their tracks are covered as far as possible. This will ensure that the victim does not have the forensic information needed to understand the attack or trace the attacker. Data manipulation, deletion and encryption (as used in ransomware) are the typical techniques that are used to do this.

As previously mentioned, Phase-3 scenario-based were not applicable for to Morphisec, as the threats were already prevented in a previous phase.

Central Management and Reporting

Management workflow is a top differentiator for any security control - if a product is difficult to manage, it will not be used. The intuitiveness of a product's management interface is a good determiner of how useful the product will be - minutes saved per activity can translate into days and even weeks over the course of a year.

Management: Threat Visibility, System Visibility, and Data Sharing

The ability to provide threat visibility is a key component of a product. This visibility can be critical when organizations are deciding to either supplement an existing technology or replace it. The table below provides information on the capabilities of the product.

Reporting Features	Morphisec
Threat Visibility	
Attack Visualization	✓
Attack Timeline	✓
Attack Phases	✓
Attack Context	✓
System Visibility	
Continuous Monitoring	✓
Running applications	✓
Running processes	✓
Behaviour Monitoring (File/registry/etc..)	✓
Whitelisting capability	✓
Data Sharing	
Standards-based Application Programming Interface (API) for access	✗
Standard output format (JSON, Syslog, CEF, etc..)	✓
Automated Data Export	✓
Syslog Integration	✓
Splunk Integration	✓
Additional Reporting Features	✓
Encryption of data at rest	✓
Targeted capture/e-discovery	✓
Customizable default security policies	✓
Policy and/or signature rollback	✓
Management to agent encryption	✓
Built-in-reporting capabilities for different user categories	✓
Multiple Analyst/User-focused workflow support	✗
Report Automation	✓
Compliance reports (GDPR, PCI-DSS, etc.)	✓
Audit Trail support in the management console	✓
System scanning capability	✓
Disaster Recovery	✓
Cloud Marketplace Support	✓
Integration with security products	✓
Enterprise recording and data storage – Forensic analysis	✓
Customized Reporting and Management	✓
Custom Reporting and filtering	✓

Management: Threat Visibility, System Visibility, and Data Sharing

Morphisec Product Reporting Capabilities

A good endpoint prevention product should have the ability to unify data, that is to say, bring together information from disparate sources, and present it all within its own UI as a coherent picture of the situation. Technical integration with the operating system and third-party applications (Syslog, Splunk, SIEM or via API) is an important part of this. An system should be able to offer response options appropriate to the organization. While providing maximum flexibility to senior analysts, the product should support predefined (but configurable) workflows for less experienced personnel, who will be assigned specific tasks during an investigation. In the following, the reporting capabilities of Morphisec Guard are being listed.

IOC Integration

This is to identify the digital footprint wherein the malicious activity in an endpoint/network can be identified. We will examine this use case by looking at the product's ability to use external IOCs including Yara signatures, snort signatures or threat intelligence feeds etc. as shown in the table below.

External IOC Correlation	Product Capabilities
SIEM	✓
DNS Logs	
Network traffic flow logs	
DHCP Logs	
Scan Results	✓
YARA Signatures	✓
Multi-factor Authentication logs	✓
Sandboxing logs	
Retrospective Analysis and Logs	
Endpoint Prevention Product logs	✓
Proprietary product integration (NGFW, IPS, ...)	✓
Threat intelligence data assimilation	✓

External Data Correlation supported by Morphisec Guard

Morphisec Product Configurations and Settings

In business environments, and with business products in general, it is usual for products to be configured by the system administrator, in accordance with vendor's guidelines, therefore we asked the vendor to configure their product to achieve the best protection available. Results presented in this test were only accomplished by applying the respective product configurations as described here.

Morphisec Guard was tested with default configuration in this test. This configuration is typical in enterprises, which have their own teams of SOC analysts looking after their defences. The personas and the threat emulation that was run in this evaluation, depicts such scenarios.

Competitive Product Differentiator (provided by Morphisec)

1. Morphisec Guard is a single agent solution that leverages native Windows 10 security capabilities such as anti-virus, device control, disk encryption, and personal firewall together with patented Moving target Defense technology to prevent against exploits, zero-days, fileless attacks, and evasive malware. All of these components are centrally managed in the Morphisec Security Center console.

2. Morphisec applies patented prevention technology on any running application, doing so it secures runtime zero-trust security model.

3. The trusted runtime becomes unknown to a foreign code and therefore cannot be abused or utilized for a successful exploitation of its runtime resources. It's this unique approach that allows for the prevention of fileless attacks, evasive malware, exploits, and zero-days without relying on passive response.

4. Morphisec Guard leverages native OS controls to remove the dependency for third-party AV products.

5. Morphisec does not rely on investigation or remediation so any business can gain value from the product, even without security analysts.

6. Morphisec uses a lightweight 3MB agent that does not consume many end-user resources like CPU, network or RAM.

7. Morphisec is easy to install and simple to operate, requiring no reboot, no configuration, instantaneous value out of the box.

8. Morphisec's management server can be deployed via the cloud or on-prem.

9. Morphisec's product catalogue is built to support on-prem, cloud, and hybrid cloud environments.

10. In addition to Guard, Morphisec offers protection for Windows and Linux servers.

11. Morphisec Shield, which was not tested during this test, can offer all of the advanced prevention capabilities of Guard alongside any other detection-centric solution without interference.

Copyright and Disclaimer

AV-Comparatives
(January 2021)

Icons: feathericons.com