

# Independent Tests of Anti-Virus Software



## Stormshield Endpoint Security Evolution 2.2

TEST PERIOD: APRIL 2022

LAST REVISION: 20<sup>TH</sup> MAY 2022

COMMISSIONED BY: STORMSHIELD

[WWW.AV-COMPARATIVES.ORG](http://WWW.AV-COMPARATIVES.ORG)

# Content

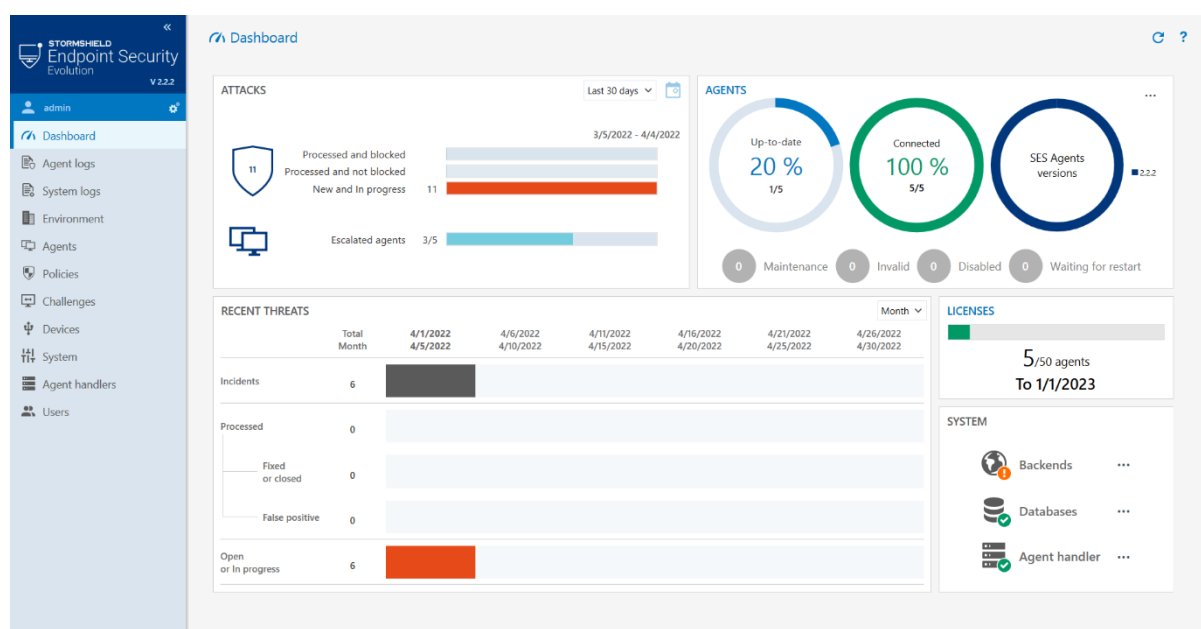
INTRODUCTION	3
ADVANTAGES	3
SERVER INSTALLATION	4
MANAGEMENT CONSOLE	4
WINDOWS ENDPOINT PROTECTION CLIENT	9
ADDITIONAL FEATURES OF THE PRODUCT	10
COPYRIGHT AND DISCLAIMER	11

## Introduction

This report was commissioned by Stormshield (<https://www.stormshield.com>). Stormshield Endpoint Security Evolution (SES Evolution) is an enterprise security product that provides behaviour-based malware detection and blocking. It is not signature-based, and can be used in conjunction with Microsoft Defender Antivirus or other antivirus solutions.

At the time of the review (April 2022), the product includes monitoring and protection services; manual response options for dealing with malware detections are due to be introduced in version 2.4, which is planned for release in Q2 2023. A server-based management console is provided, and this is reviewed on the following pages.

The review covers everyday use of the product, starting with installation of the server-based management console.



## Advantages

- Easy-to-navigate console
- Straightforward setup of server and clients
- Comprehensive filtering options for detection events
- Tamper protection for client PCs
- Detailed policies allow fine-grained configuration control

## Server Installation

All the required components of the management server and console can be installed using a single .EXE file. Prerequisites are Microsoft Visual C++, .NET Framework and SQL Server Express; installer files for compatible versions of these are included, and can be installed by the setup wizard if required. We found the server installation process to be very quick and straightforward.

## Management Console

All the console's functionality is easily accessible from a single menu panel on the right-hand side. The main menu items are: *Dashboard*; *Agent Logs*; *System Logs*; *Environment*; *Agents*; *Policies*; *Challenges*; *Devices*; *System*; *Agent Handlers*; *Users*.

### Dashboard page

This is the page you see when you first log on to the console. It's shown in the screenshot above. There are information panels, illustrated with bar and doughnut charts, showing attack status, agent status, recent threats, licence usage and server status. The latter shows three different server components, namely *Databases*, *Backends* and *Agent Handlers*. The *Backend* component provides the sole means of communicating with the database, and makes the data available via Microsoft Internet Information Services (IIS). An *Agent Handler* acts as a relay between computers in the LAN of e.g. a branch office and the *Backend*.

### Agent logs page

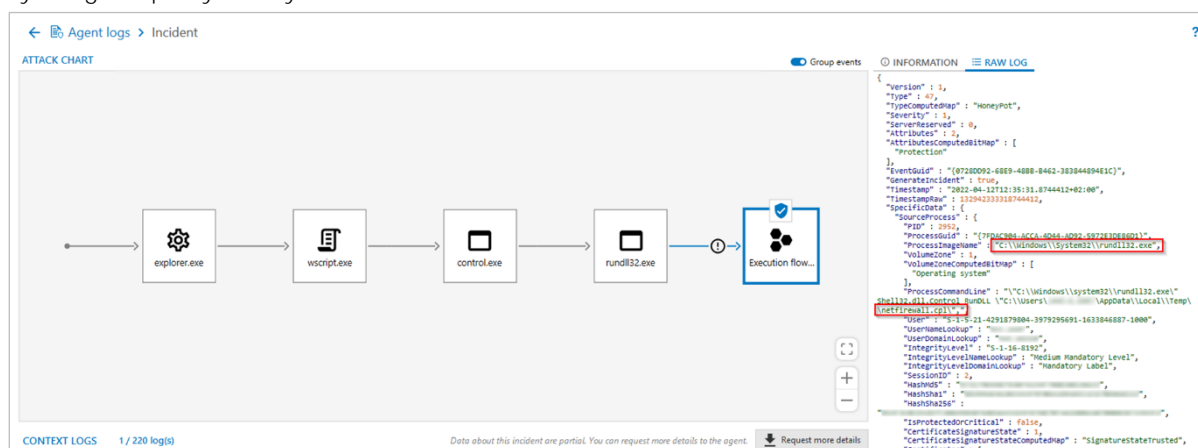
The screenshot displays the 'Agent logs' interface. At the top, there's a header with 'Agent logs' and a search bar. Below this is a 'FILTERS' section with tabs for 'Status: New, In progress' and 'Default filters'. The main area is a table with columns: Log type, Severity, Status, Attribute, Category, Agent group, Agent, and Application. The 'Status' column has a dropdown menu with options like 'New (13)', 'In progress (0)', 'False positive (0)', 'Fixed (0)', and 'Closed (0)'. The 'Agent' column has a search bar. Below the filters is a table of log entries with columns: DATE, BLOCKED, AGENT, TYPE, MESSAGE, POLICY, STATUS, and ACTIONS. The logs show various security events, including attempts to execute malicious code and execution flow hijacking.

Log type	Severity	Status	Attribute	Category	Agent group	Agent	Application
Event (8)	Very High (5)	New (13)	Self-protection (0)	Threats (13)	Default group (13)	WmiPrvSE.exe (8)	WmiPrvSE.exe (8)
Incident (5)	High (8)	In progress (0)	Protection (13)	File (0)		chrome.exe (7)	chrome.exe (7)
	Medium (0)	False positive (0)	Internal (0)	Registry (0)		1.exe (5)	1.exe (5)
	Low (0)	Fixed (0)	Audit (0)	Process (0)		RuntimeBroker.exe (1)	RuntimeBroker.exe (1)
		Closed (0)	External (0)	Network (0)			
				Device (0)			
				Internal (0)			
				External (0)			

DATE	BLOCKED	AGENT	TYPE	MESSAGE	POLICY	STATUS	ACTIONS
4/6/2022 11:36:31 AM	1/1		1	The '1.exe' process attempted to execute malicious code (source process aborted)	Stormshield ...	New	
4/6/2022 11:36:31 AM	1/1		1	Execution flow hijacking The '1.exe' process attempted to execute malicious code (source process aborted)	Stormshield ...	New	
4/6/2022 11:36:02 AM	1/1		1	The '1.exe' process attempted to execute malicious code (source process aborted)	Stormshield ...	New	
4/6/2022 11:05:36 AM	1/1		1	The '1.exe' process attempted to execute malicious code (source process aborted)	Stormshield ...	New	
4/6/2022 10:23:15 AM	1/1		1	The '1.exe' process attempted to execute malicious code (source process aborted)	Stormshield ...	New	
4/6/2022 10:22:54 AM	1/1		1	The '1.exe' process attempted to execute malicious code (source process aborted)	Stormshield ...	New	
4/6/2022 10:03:26 AM	1/1	NT AUTHORITY\SYSTEM	1	The 'WmiPrvSE.exe' process attempted to inject code into the 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe' process	Stormshield ... Protection	New	

Security-related events are shown on this page. For each event, there are details such as the date and time, computer, user account involved, event details (e.g. attempt to execute malicious code), and name of the applicable policy. The section at the top of the page allows you to filter the list by log type, severity, status (e.g. "in progress"), attribute (e.g. "protection"), category (e.g. "file", "registry"), agent group, agent name (= hostname), and application involved (e.g. chrome.exe). You can select single or multiple items in each column, and then click *Apply* to filter the list.

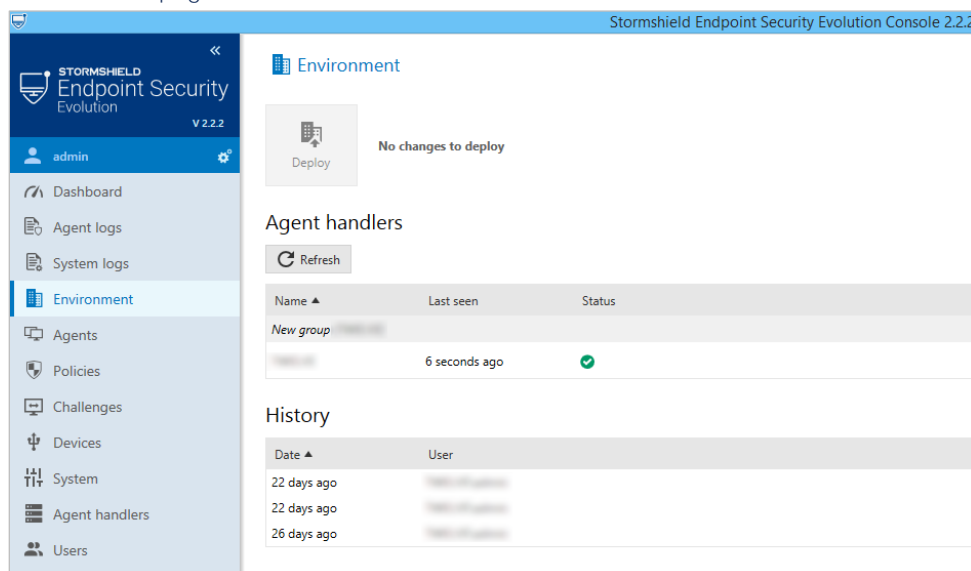
Stormshield Endpoint Security Evolution differentiates between two types of logs: *Events* and *Incidents*. An *Incident* includes all the events that took place on the machine before the attack, thus providing context. *Incidents* are created following one or more alerts when an attack is detected by the agent. This data is used to automatically generate an *Attack Chart* (an example is provided in the screenshot below). For each process, detailed information is provided to assist in the analysis. The administrator can enhance the chart by pinning to it any additional events that he/she considers relevant to the investigation. This helps create a complete picture of the attack. In the example test case shown below, JavaScript was used to employ DLL sideloading that executes Meterpreter shellcode by a signed proxy binary.



### System logs page

This is laid out in the same way as *Agent Logs*, and has similar filtering options. It displays system events such as logins to the management console, and start-up of *Backend* and *Agent Handler* components of the management server.

### Environment page



This page allows you to synchronise policy changes from the server to the clients. When a policy change has been made, an orange dot will appear next to the *Environment* entry in the menu panel, making it obvious that it needs to be synchronised. You then just need to open the *Environment* page, and click *Deploy*.

## Agents page

COMPUTER	IP ADDRESS	VERSION	OPERATING SYSTEM	HOST TYPE	POLICY	LAST CONNECTION	DOMAIN	USER	GROUP	MODE	PINNED
server01	192.168.1.100	2.2.2	Windows Server 2022 (Standard Evaluation build 22H2) x64	Virtual machine	Stormshield - Default policy	3/1/2022 12:40:29 PM	Outside domain		Default group	Normal	
vm01	192.168.1.101	2.2.2	Windows 10 Pro (build 19044) x64	Virtual machine	Stormshield - Default policy	4/4/2022 4:41:25 PM	Outside domain		Default group	Normal	
vm02	192.168.1.102	2.2.2	Windows 11 Pro (build 22H2) x64	Virtual machine	Stormshield - Default policy	4/1/2022 6:08:15 PM	Outside domain		Default group	Normal	
vm03	192.168.1.103	2.2.2	Windows 10 Pro (build 19044) x64	Virtual machine	Stormshield - Default policy	3/1/2022 12:22:21 PM	Outside domain		Default group	Normal	
vm04	192.168.1.104	2.2.2	Windows 8.1 Pro (build 9600) x64	Virtual machine	Stormshield - Default policy	4/1/2022 6:07:36 PM	Outside domain	No connected user	Default group	Normal	

This page shows the protected computers on your network. Information provided for each one includes hostname, local IP address, agent version, OS version, host type (virtual or physical), policy applied, last connection to the management server, and management group. You can create new agent groups here, and assign computers to these. By selecting a group and clicking the *Configuration* tab, you can see the policy applied to that group, along with other group-wide settings.

## Policies page

**Compatibility**  
Add all applications that are not compatible with the following system protections: Keylogging, Application-defined hooks installation, Execution flow hijacking or Heap spraying. No IDs selected.

**Application-defined hooks installation**  
Prevents code injection and keylogging attempts that target a particular process or all processes on the host. ☒ Generate an incident. Status: Audit.

**Driver loading**  
Monitors drivers loaded by the operating system. ☒ Generate an incident. Status: Allow. Workaround - Microsoft Console Hosts. Status: Allow. Microsoft - Drivers written by TrustedInstaller. Status: Audit. Malicious - Deny list of Drivers.

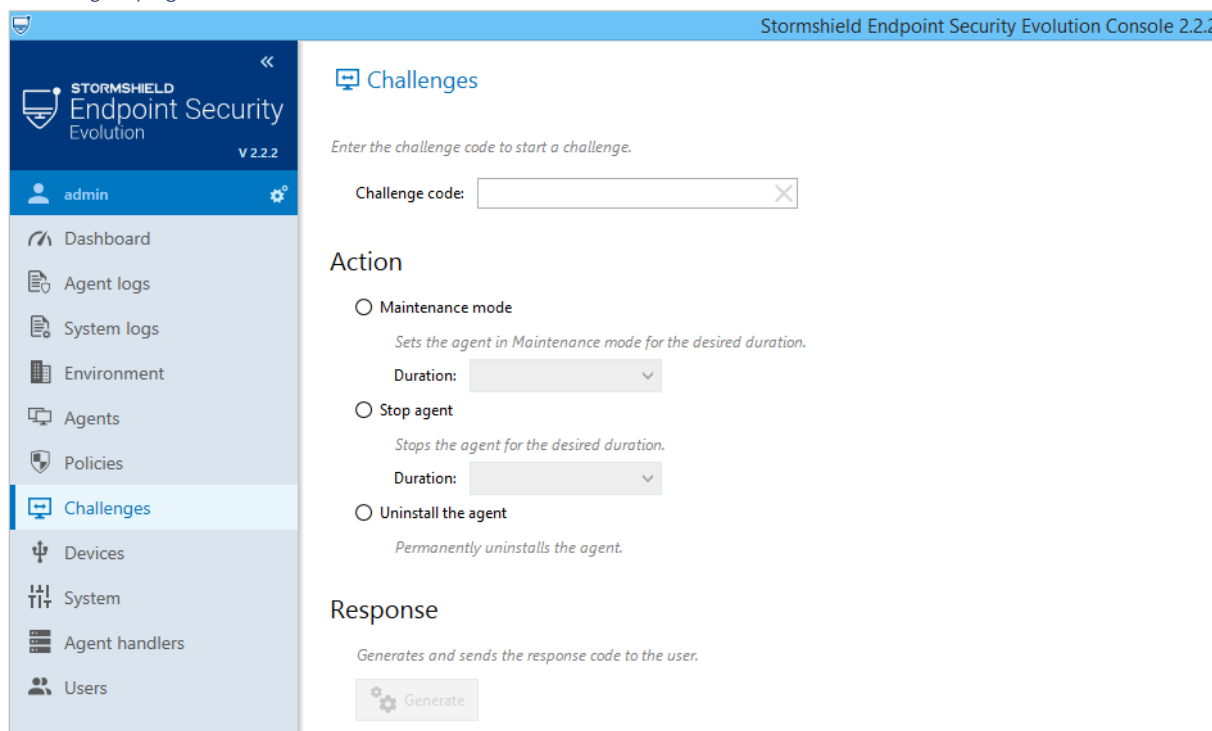
**Driver integrity**  
Monitors changes to tables of major driver functions. ☒ Generate an incident. Status: Audit.

**Privilege escalation**  
Prevents privilege escalation. ☒ Generate an incident. Status: Audit. Code Hosts - Windows Scripting Interpreters. Code Hosts - Scripting Interpreters or Byte-Code. Status: Allow. Windows Programs started by TrustedInstaller. Status: Allow. Security Solutions - Anti-Malware. Status: Allow. Apps - Task Managers and Crash Handlers.

**ARP spoofing** Version 2  
Monitor whether network traffic is being intercepted, modified or stopped through ARP spoofing. Every 5 Minutes. Status: Detect only.

As you would expect, this section allows you to create and edit the policies that define the product's protection capabilities. A default audit and protection policy is provided and updated by the Stormshield security team. Stormshield policies are very detailed, allowing very granular configuration. To make it easy to navigate, the policies pages have tabs (and sub-tabs in some places) at the top, as shown in the screenshot above.

## Challenges page



A “challenge” is a means of deactivating tamper protection on a client, allowing the administrator to carry out maintenance on the endpoint software, temporarily stop the agent, or uninstall it. It works as follows. On the endpoint client, the user or IT support technician clicks *Request a challenge* on the *Help and Support\Diagnosis* page of the Stormshield client window. This generates a code, which needs to be communicated to the administrator. The admin then enters this code on the *Challenges* page of the console, selects the required action (e.g. *Uninstall the agent*), and generates a response code. This code is communicated to the user/technician, who enters it into the Stormshield client window and clicks *Start the Challenge*; this will carry out the desired action.

## Devices page

This page shows USB flash sticks and external drives that have been connected to a Stormshield-protected computer.

## System page

Here you can specify how long (in months) to retain agent and system logs.

## Agent handlers page

This page shows servers operating the *Agent Handler* role (described above). These servers can be renamed and sorted into groups.

## Users page

This lets you create and modify accounts for console users. There are three preconfigured roles that can be assigned to console users: Administration, Audit and Help Desk. You can also create a custom user role, with the options no access, read only, and modify, for each individual area of console functionality, such as *Policies*, *Licenses* and *Agent Groups*.

### *Preferences page*

This is accessed from the cogwheel icon at the top of the menu panel. It allows you to change the console display language in real time, and also provides licensing information about third-party products (such as Microsoft's .NET framework) that are used by Stormshield Endpoint Security Evolution.

### *Help features*

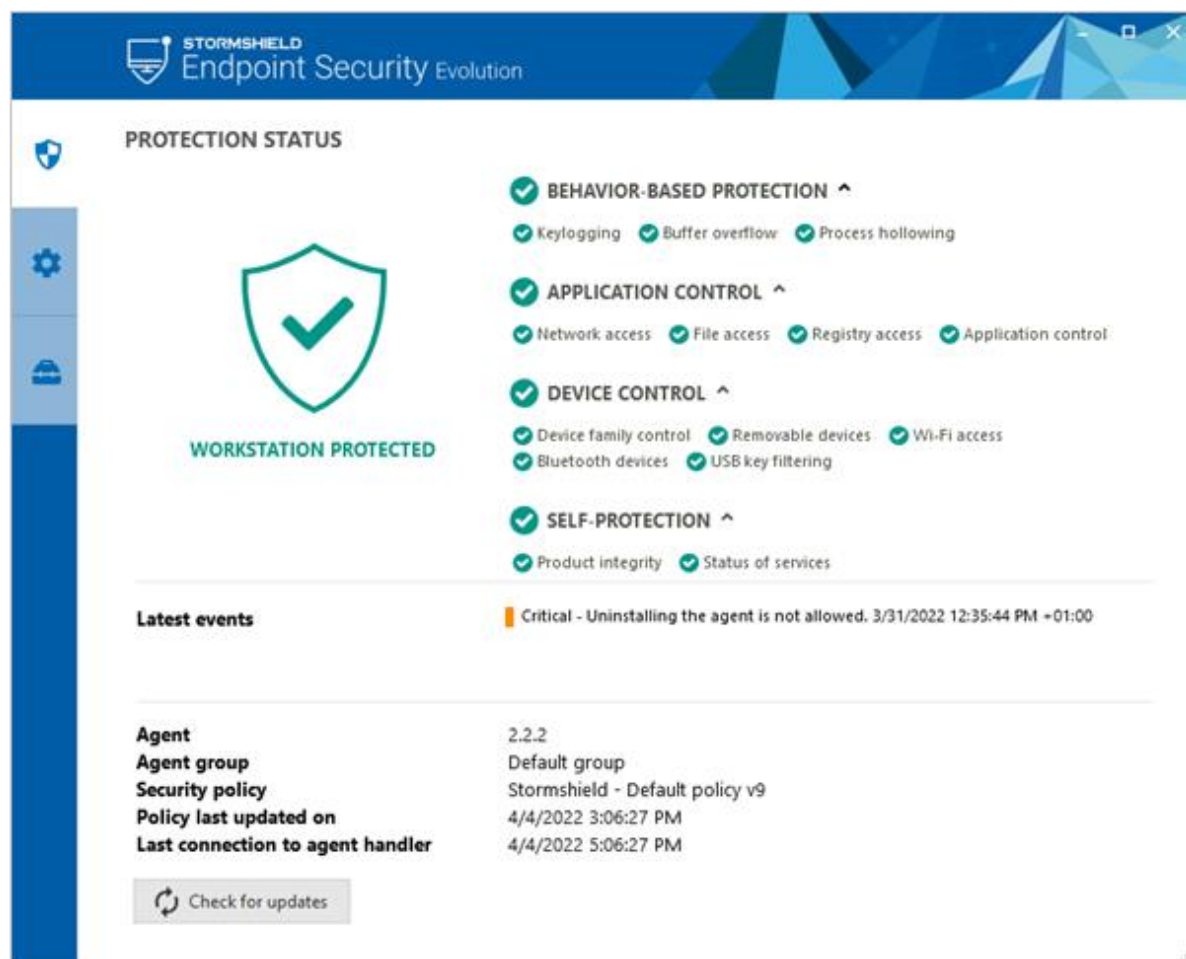
These are accessed by clicking the ? symbol in top right-hand corner of console. This links to the documentation page of Stormshield's website, where online documentation and downloadable .PDF manuals can be found: <https://documentation.stormshield.eu/SES/v2/en/Content/Home.htm>

## Windows Endpoint Protection Client

### Deployment

Installation files in .exe format can be downloaded by going to the *Agents* page and clicking the applicable group; here there is a menu marked *Installer*. There are separate installers for 32- and 64-bit Windows systems. These can be run manually, or via a systems management product such as SCCM or GPO. Additionally, a procedure that will allow for remote push agent installation using GPO is currently under development. Manual installation is extremely quick and easy, although a system reboot is required to complete it.

### User interface



The user interface on protected endpoints consists of a System Tray icon and a program window. The latter displays the status of individual protection components (screenshot above), and event logs. Aside from checking for updates and changing the user-interface language, no functionality is made available to the user. We note that end users, even those with non-administrator accounts, can easily **shut down the program's GUI by right-clicking the System Tray icon and clicking *Quit***. However, this does not disable protection, which continues to work as before.

### Malware detection scenario

When we tried to execute some malware samples on our test PC, Stormshield prevented the malicious files from running, and displayed a pop-up alert. No user action was required or possible, and the alert closed after a few seconds.

## Additional features of the product

The information below was provided by the vendor.

### Ransomware Protection

This has four main functions: to enable daily backups of the Windows Shadow Copy feature; to block ransomware from deleting Shadow Copies (command-line filtering); to monitor file modification and block the start of an encryption process; to provide a list of encrypted files to enable their recovery (using Shadow Copies).

### Trusted USB Storage Management

The SES Evolution agent can be integrated into a decontamination station to ensure that the content of a USB stick is not modified outside the SES environment. The SES Agent installed on the decontamination station creates a fingerprint on the USB stick to track any change in content. As long as the content of the key is modified within the SES environment, access is granted. If a change is made on an external machine, the level of trust is lost, and the USB stick must be scanned again by the decontamination station. The use of untrusted or unknown sticks can be restricted or blocked.

### Tamper Protection

The product includes self-protection of the agent. The agent consists of micro-services to ensure maximum system security. Each service has a precise role and given only the privileges needed to fulfil it (application of the principle of least privilege). All communications between the agent modules are secure and authenticated and are validated by a specific self-protection driver.



## Copyright and Disclaimer

This publication is Copyright © 2022 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives  
(May 2022)