STORMSHIELD

ENDPOINT SECURITY

EVOLUTION

Increase the level of protection for your workstations with a proactive EDR solution

Deployment

ON-PREM
AND SAAS

API REST

INTEGRATION
ECOSYSTEM

Highly customiza-ble

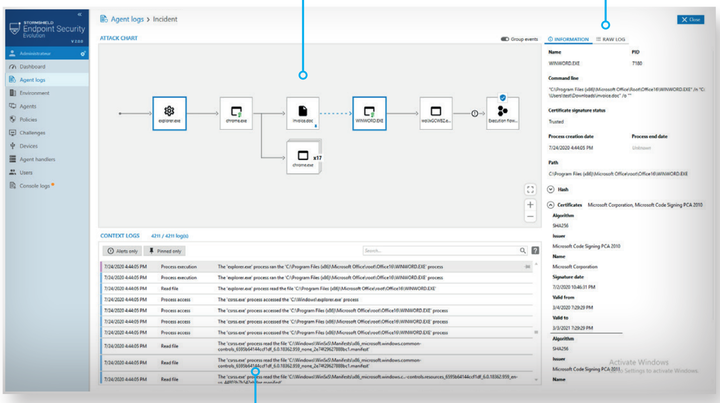
SECURITY PARAMETERS
ADJUSTABLE

Standalone

PROTECTION OF
DISCONNECTED
ENVIRONMENTS

DETAILED VIEW

ATTACK GRAPH



```
7/24/2020 4:44:05 PM   Process execution   The 'explorer.exe' process ran the 'C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE' process
7/24/2020 4:44:05 PM   Process execution   The 'explorer.exe' process ran the 'C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE' process
7/24/2020 4:44:05 PM   Read file           The 'explorer.exe' process read the file 'C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE'
7/24/2020 4:44:05 PM   Process access      The 'csrss.exe' process accessed the 'C:\Windows\explorer.exe' process
7/24/2020 4:44:05 PM   Process access      The 'csrss.exe' process accessed the 'C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE' process
7/24/2020 4:44:05 PM   Process access      The 'csrss.exe' process accessed the 'C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE' process
7/24/2020 4:44:05 PM   Process access      The 'csrss.exe' process accessed the 'C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE' process
7/24/2020 4:44:05 PM   Read file           The 'csrss.exe' process read the file 'C:\Windows\WinSxS\Manifests\x86_microsoft.windows.common-
                                           controls_6595b64144ccf1df_6.0.18362.959_none_2e74f29627888bc1.manifest'
7/24/2020 4:44:05 PM   Read file           The 'csrss.exe' process read the file 'C:\Windows\WinSxS\Manifests\x86_microsoft.windows.common-
                                           controls_6595b64144ccf1df_6.0.18362.959_none_2e74f29627888bc1.manifest'
7/24/2020 4:44:05 PM   Read file           The 'csrss.exe' process read the file 'C:\Windows\WinSxS\Manifests\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.18362.959_en-
                                           us_44803b7b542e[illegible]fae.manifest'
```

Name: WINWORD.EXE
PID: 7180

Command line: "C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\test\Downloads\invoice.doc" /o ""

Certificate signature status: Trusted

Process creation date: 7/24/2020 4:44:05 PM
Process end date: Unknown

Path: C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

Hash

Certificates: Microsoft Corporation, Microsoft Code Signing PCA 2010

Algorithm: SHA256
Issuer: Microsoft Code Signing PCA 2010
Name: Microsoft Corporation
Signature date: 7/2/2020 10:46:31 PM
Valid from: 3/4/2020 7:29:29 PM
Valid to: 3/3/2021 7:29:29 PM

Algorithm: SHA256
Issuer: Microsoft Code Signing PCA 2011
Name

LIST OF EVENTS

Optimal protection with our EDR solution

Stormshield Endpoint Security Evolution is the next-generation endpoint and server protection solution. Based on signatureless analysis technology, the agent detects attacks and threats and responds accordingly.

Proactive security

- Attack blocked in real time
- Predefined and customizable analysis and remediation
- Attack graph and Threat Hunting (IoC, Yara rules, etc.)

Behavioural analysis

- Signatureless protection against 0-day attacks
- Counters vulnerability exploitation techniques
- Anti-ransomware protection

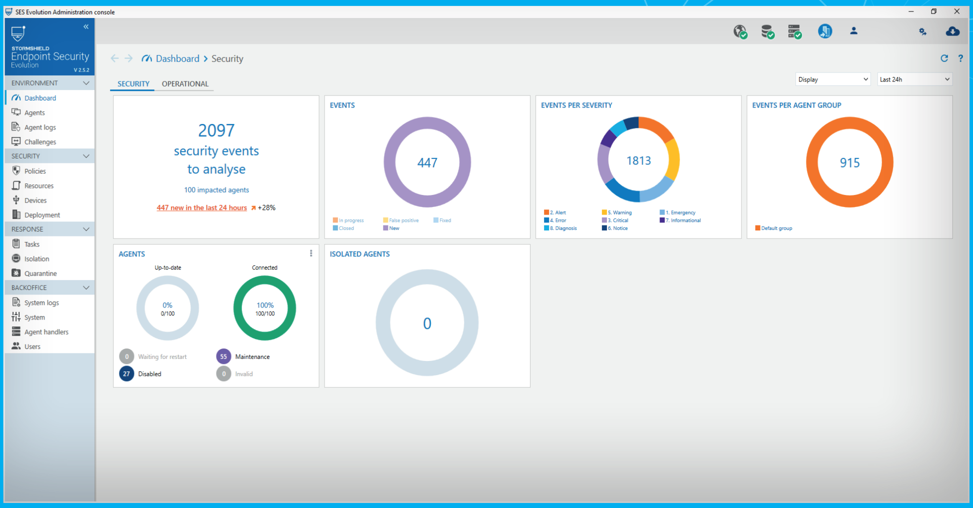
Contextual protection

- Security policy dynamically adapts to the environment, even offline
- Policies customizable by user group
- Default security policies and updates by Stormshield Customer Security Lab security teams

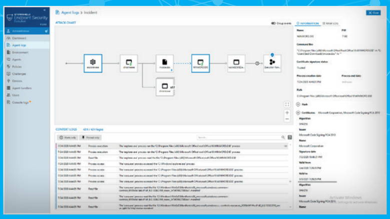
NEXT-GENERATION
ENDPOINT PROTECTION

MEDIUM AND LARGE
COMPANIES

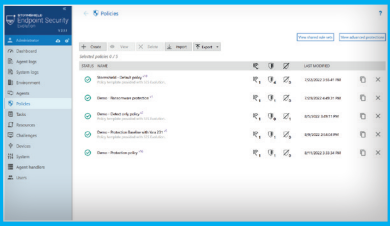
WWW.STORMSHIELD.COM



Dashboard



Detailed view of an incident



View of the security policy

FEATURES

Zero-day protection against known and unknown threats

Analysis techniques

- Memory corruption (buffer overflow, heap spray)
- Privilege escalation (token stealing)
- Theft of sensitive information (keylogging, process access)
- Process hollowing and its variants
- Code injection (application hooking)
- Protection against fileless attacks

Ransomware protection

- Malicious encryption processes
- Restore files encrypted by ransomware
- Windows Shadow Copy
- Backup policy

Signatureless protection

Personalised remediation

- Kill a process
- Delete a file
- Delete or modify a registry key or its value
- Run PowerShell scripts for custom actions (stopping and removing a service, etc.)
- Automatic malware quarantine
- Isolation of compromised workstations

Identification of indicators of compromise (IoC)

- Suspicious text (file name, host name, object name, etc.)
- Network information (IP addresses, suspicious URLs, DNS)
- Hash SHA1, SHA256, MD5 and SSDEEP
- Immediate, scheduled or on-detection search for indicators of compromise
- Protection against bypassing EDR detection devices

Device control

- WiFi networks • USB stick • Bluetooth • Disk volume access • Network connections • Execution control

Optimised agent

- Memory usage
- CPU usage

Security policy

- Adapts dynamically according to context
- Behavioural analysis and device control rule sets provided and maintained by Stormshield
- Management of Yara rules

Centralised administration

- Policy management by agent groups
- Role-based user management
- Activation/deactivation of modules by agent group
- API REST for integration with third-party products
- Activity report with MCS and MCO indicators in HTML format
- Automatic email notification of security alerts

COMPATIBILITY

AGENT

Resources

CPU:
1 core 1 GHz (min.) - 2 cores 2 GHz (recommended)

RAM:
1 GB (min.) - 2 GB (recommended)

Disk space:
100 MB (installation) - 200 MB (data)

Operating system

Client:
Windows 7 SP1, 8.1, 10, and 11

Serveur:
Windows Server 2008 R2, 2012 R2, 2016, 2019, and 2022 (including Core version)

ADMINISTRATION

Possibility of SaaS or on-premise management

FOR THE ON-PREMISE MANAGEMENT

Backend

CPU:
1 core 1GHz (min.) - 2 core 2Ghz (recommended)

RAM:
1 GB (min.) - 2 GB (recommended)

Disk space:
100 MB (installation) - 200 MB (data)

Server:
Windows Server 2012 R2, 2016, 2019, and 2022 (including Core version)

Agent handler

CPU:
2 cores 2 GHz (minimum)

RAM:
2 GB (minimum)

Disk space:
200 MB (installation) - 1 GB (data - minimum)

Client:
Windows 10 and 11

Server:
Windows Server 2008 R2, 2012 R2, 2016, 2019, and 2022 (including Core version)

Database:
SQL Server 2017 or later