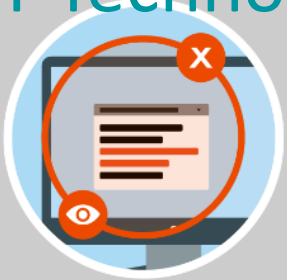


A group of four business professionals are gathered around a wooden conference table in a modern office setting. A man with glasses and a dark blazer is seated at the head of the table, gesturing with his hands as he speaks. To his left, a woman with curly hair is looking towards him. In the foreground, a man is seen from the back, looking at a tablet. To the right, a woman with long blonde hair is also looking towards the man at the head of the table. The table is cluttered with various items including a laptop, notebooks, pens, and a small calendar. The entire image is overlaid with a semi-transparent teal color. A white rectangular box is centered horizontally across the middle of the image, containing the text 'Endpoint Security ESET Module' in a bold, white, sans-serif font.

Endpoint Security ESET Module

ESET Technologie

BESTÄNDIG



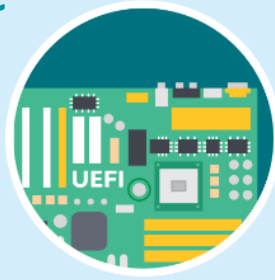
VERHALTENSBASIERTE
ERKENNUNG UND
BLOCKIERUNG - HIPS



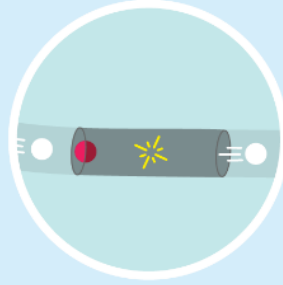
ESET LIVEGRID



MACHINE LEARNING



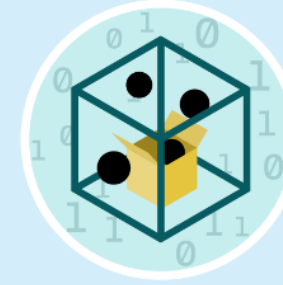
UEFI SCANNER



SCHUTZ VOR
NETZWERKANGRIFFEN



REPUTATION
& CACHE



IN-PRODUCT
SANDBOX



DNA ERKENNUNG

VOR AUSFÜHRUNG



ERWEITERTE
SPEICHERPRÜFUNG



RANSOMWARE
SHIELD

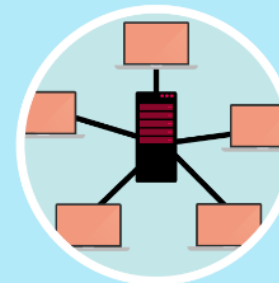


EXPLOIT
BLOCKER

NACH AUSFÜHRUNG



CLOUD-BASIERTER
SCHUTZ VOR MALWARE



BOTNET-
ERKENNUNG

- PRE-EXECUTION
- EXECUTION
- POST EXECUTION



Reputation
and Cache



DNA
Detections



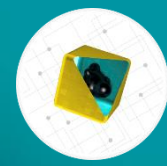
UEFI
Scanner



Device
Control



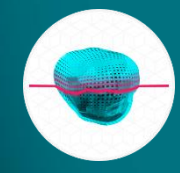
Network Attack
Protection



In-product
Sandbox



Ransomware
Shield



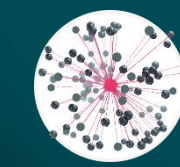
Advanced
Memory Scanner



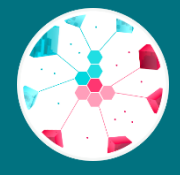
Deep Behavioral
Inspection



LiveGrid®
Protection



Botnet
Protection



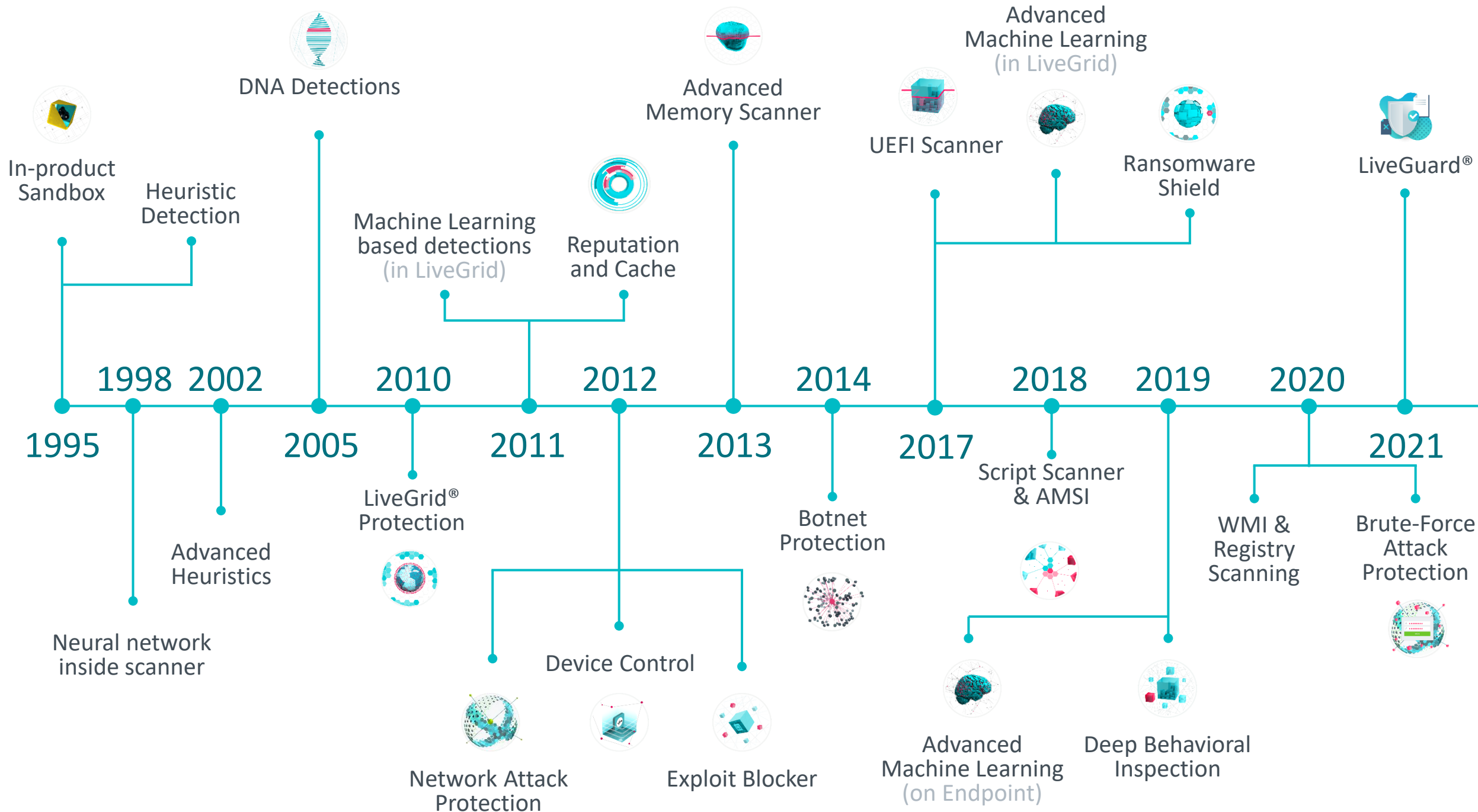
Script Scanner
& AMSI



Exploit
Blocker



Advanced
Machine Learning





Modul – UEFI Scanner

Der Unified Extensible Firmware Interface (UEFI)-Scanner ist Teil des Host Intrusion Prevention System (HIPS), das die UEFI-Firmware auf Ihrem Computer schützt. Die UEFI-Firmware wird zu Beginn des Systemstarts in den Arbeitsspeicher geladen.

Der Code befindet sich auf einem Flashspeicherchip, der auf der Hauptplatine verlötet ist. Angreifer können diesen Chip infizieren und Malware installieren, die auch Neustarts und Neuinstallationen des Systems übersteht. Diese Malware verbirgt sich außerdem besser vor entsprechenden Schutzlösungen, da ein Großteil von ihnen diese Ebene nicht überprüft.

Modul – UEFI Scanner

ESET Endpoint for Windows

Zu suchender Typ...

ERKENNUNGSRoutine	58
Echtzeit-Dateischutz	14
Cloudbasierter Schutz	8
Malware-Scans	33
HIPS	1
UPDATE	43
NETZWERKSCHUTZ	9
WEB UND E-MAIL	11
MEDIENKONTROLLE	
TOOLS	7
BENUTZEROBERFLÄCHE	4
OVERRIDE-MODUS	4

+
ALLGEMEIN
1

-
THREATSENSE-PARAMETER
13

ZU SCANNENDE OBJEKTE

☐ ☒ ☐ ☐ Bootsektoren/UEFI

Bootsektoren und UEFI werden auf Rootkits, Bootkits und andere Malware gescannt.

☐ ☒ ☐ ☐ Laufzeitkomprimierte Dateien
☒

SCAN-EINSTELLUNGEN

☐ ☒ ☐ ☐ Heuristik
☒

☐ ☒ ☐ ☐ Advanced Heuristik/DNA-Signaturen
☒

SÄUBERUNG

☐ ☒ ☐ ☐ Säuberungsstufe

Ereignis immer beheben

In diesem Modus versucht das Programm, erkannte Dateien ohne Eingreifen des Benutzers automatisch zu säubern oder zu löschen. Die einzige Ausnahme sind Systemdateien. Wenn Systemdateien nicht gesäubert werden können und ein Benutzer angemeldet ist, wird ein Warnhinweis angezeigt.

Modul – Schutz vor Netzwerkangriffen

Der Netzwerkangriffsschutz ist eine Erweiterung der Firewall und verbessert die Erkennung von Exploits für bekannte Schwachstellen auf der Netzwerkebene. Durch die Bereitstellung von Erkennungsmethoden für verbreitete Exploits in häufig genutzten Protokollen wie SMB, RPC und RDP bietet er eine weitere wichtige Schutzebene gegen die Verbreitung von Malware, Angriffe aus dem Netzwerk und das Ausnutzen von Sicherheitslücken, für die noch kein Patch herausgegeben oder installiert wurde.

Modul – Schutz vor Netzwerkangriffen



ESET Endpoint for Windows

🔍 Zu suchender Typ...



ERKENNUNGSRoutine	58
UPDATE	43
NETZWERKSCHUTZ	9
Firewall	8
Netzwerkangriffsschutz	1
WEB UND E-MAIL	11
MEDIENKONTROLLE	
TOOLS	7
BENUTZEROBERFLÄCHE	4
OVERRIDE-MODUS	4

NETZWERKANGRIFFSSCHUTZ ○ ● ⚡

☐ ☒ ⚡

 Schutz vor Netzwerkangriffen (IDS)
aktivieren ?

☐ ☒ ⚡

 Botnet-Erkennung aktivieren ✓ ?

☐ ☒ ⚡

 Liste der IDS-Ausnahmen Bearbeiten

+ ERWEITERTE EINSTELLUNGEN 1 ○ ● ⚡ ?

Der Netzwerkangriffsschutz analysiert den Inhalt des Netzwerkverkehrs und schützt vor Netzwerkangriffen. Jeglicher als schädlich erkannter Verkehr wird blockiert.

Modul – Reputation & Cache

Vor der Prüfung von Dateien oder URLs fragen unsere Produkte beim lokalen Cache an, ob das Objekt bereits als schädlich oder sicher eingestuft wurde. Hierdurch werden unnötige Mehrfachscans ungefährlicher Objekte vermieden und Prüfungen beschleunigt.

Anschließend wird bei der Überprüfung der Objekte zunächst deren eindeutiger „Fingerabdruck“ (Hash) mit der Reputationsdatenbank ESET LiveGrid® abgeglichen. D.h. es wird ermittelt, ob das Objekt schon irgendwo anders aufgetaucht und als schädlich bekannt ist. Dies steigert die Effektivität der Prüfung und ermöglicht zudem eine schnellere Bereitstellung wichtiger Informationen über aktuelle Bedrohungen.

Modul – In Product Sandboxing

Laufzeitkomprimierte Dateien – Im Unterschied zu Standardarchiven werden laufzeitkomprimierte Dateien nach dem Starten im Arbeitsspeicher dekomprimiert.

Neben statischen laufzeitkomprimierten Dateiformaten (UPX, yoda, ASPack, FSG usw.) kann die Prüfung durch Code-Emulation viele weitere SFX-Typen erkennen.

Modul – In Product Sandboxing

ESET Endpoint for Windows

Zu suchender Typ...



ERKENNUNGSROUTINE

58

Echtzeit-Dateischutz

14

Cloudbasierter Schutz

8

Malware-Scans

33

HIPS

1

UPDATE

43

NETZWERKSCHUTZ

9

WEB UND E-MAIL

11

MEDIENKONTROLLE

TOOLS

7

BENUTZEROBERFLÄCHE

4

OVERRIDE-MODUS

4

+ ALLGEMEIN

1

- THREATSENSE-PARAMETER

13

ZU SCANNENDE OBJEKTE

☐ ☒ ☐ Bootsektoren/UEFI



☐ ☒ ☐ Laufzeitkomprimierte Dateien

Laufzeitkomprimierte Dateien werden nach der Ausführung im Speicher dekomprimiert.



SCAN-EINSTELLUNGEN

☐ ☒ ☐ Heuristik



☐ ☒ ☐ Advanced Heuristik/DNA-Signaturen



SÄUBERUNG

☐ ☒ ☐ Säuberungsstufe

Ereignis immer beheben



In diesem Modus versucht das Programm, erkannte Dateien ohne Eingreifen des Benutzers automatisch zu säubern oder zu löschen. Die einzige Ausnahme sind Systemdateien. Wenn Systemdateien nicht gesäubert werden können und ein Benutzer angemeldet ist, wird ein Warnhinweis angezeigt.

Modul – DNA Erkennung

Die Erkennungsarten reichen von sehr spezifischen Hashes bis hin zu ESET DNA-Erkennungen, einer komplexen Definition von böartigen Verhaltensweisen und Eigenschaften von Schadsoftware. Während ein Angreifer den Schadcode relativ leicht ändern oder verschleiern kann, lässt sich das Verhalten von Objekten nicht so einfach ändern. Die ESET DNA-Erkennungen machen sich dieses Prinzip zunutze.

Wir führen eine tiefgehende Codeanalyse durch, extrahieren „Gene“ für das Verhalten des Codes und gleichen sie mit ESET DNA-Erkennungen auf potenziell verdächtigen Code ab, egal ob auf dem Datenträger oder im Arbeitsspeicher von laufenden Prozessen. DNA-Erkennungen können bekannte Proben von Schadsoftware, neue Varianten einer bekannten Familie von Schadsoftware oder unbekannte Schadsoftware anhand von Genen erkennen, die auf ein böartiges Verhalten hindeuten.

Modul – DNA Erkennung

ESET Endpoint for Windows



ERKENNUNGSROUTINE

58

Echtzeit-Dateischutz

14

Cloudbasierter Schutz

8

Malware-Scans

33

HIPS

1

UPDATE

43

NETZWERKSCHUTZ

9

WEB UND E-MAIL

11

MEDIENKONTROLLE

TOOLS

7

BENUTZEROBERFLÄCHE

4

OVERRIDE-MODUS

4



ALLGEMEIN

1



THREATSENSE-PARAMETER

13



ZU SCANNENDE OBJEKTE



Bootsektoren/UEFI



Laufzeitkomprimierte Dateien



SCAN-EINSTELLUNGEN



Heuristik



Advanced Heuristik/DNA-Signaturen



Advanced Heuristik verwendet einen einzigartigen, von ESET entwickelten Algorithmus, der für die Erkennung von Schadcode in höheren Programmiersprachen optimiert ist.

SÄUBERUNG



Säuberungsstufe



Ereignis immer beheben



In diesem Modus versucht das Programm, erkannte Dateien ohne Eingreifen des Benutzers automatisch zu säubern oder zu löschen. Die einzige Ausnahme sind Systemdateien. Wenn Systemdateien nicht gesäubert werden können und ein Benutzer angemeldet ist, wird ein Warnhinweis angezeigt.

Modul – Erweiterte Speicherprüfung

Die erweiterte Speicherprüfung bietet im Zusammenspiel mit dem Exploit-Blocker stärkeren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung und/oder Verschlüsselung zu entgehen. In Fällen, in denen herkömmliche Emulation oder Heuristik eine Bedrohung eventuell nicht aufspüren, kann die erweiterte Speicherprüfung verdächtiges Verhalten identifizieren und Bedrohungen erkennen, wenn sie sich im Arbeitsspeicher manifestieren. Diese Lösung kann selbst gegen stark verschleierte Malware wirkungsvoll agieren.

Anders als der Exploit-Blocker sucht die erweiterte Speicherprüfung nach ausgeführter Malware. Damit ist das Risiko verbunden, dass vor der Erkennung einer Bedrohung bereits schädliche Aktivitäten durchgeführt wurden; falls jedoch andere Erkennungsmethoden versagt haben, bietet sie eine zusätzliche Schutzebene.

Modul – Erweiterte Speicherprüfung

ESET Endpoint for Windows

Zu suchender Typ...

?

^

ERKENNUNGSROUTINE

58

Echtzeit-Dateischutz

14

Cloudbasierter Schutz

8

Malware-Scans

33

HIPS

1

UPDATE

43

NETZWERKSCHUTZ

9

WEB UND E-MAIL

11

MEDIENKONTROLLE

TOOLS

7

BENUTZEROBERFLÄCHE

4

OVERRIDE-MODUS

4

ALLGEMEIN

1

○

●

⚡

○ ● ⚡ HIPS aktivieren

✓

i

○ ● ⚡ Selbstschutz aktivieren

✓

i

○ ● ⚡ Protected

Service

aktivieren

Ⓜ ≥ 6.6

Ⓜ ≥ 8.1

✓

i

○ ● ⚡ Erweiterte Speicherprüfung
aktivieren

Funktioniert zusammen mit dem Exploit-Blocker, um den Schutz vor Malware zu verbessern, die speziell gegen Malware-Erkennungsprodukte mit Verschleierung oder Verschlüsselungstechniken entwickelt wurde. Die erweiterte Speicherprüfung ist standardmäßig aktiviert.

i

○ ● ⚡ Exploit-Blocker aktivieren

i

TIEFE VERHALTENSINSPEKTION

○ ● ⚡ Tiefe Verhaltensinspektion
aktivieren

Ⓜ ≥ 7.2

✓

i

○ ● ⚡ Ausschlüsse

Ⓜ ≥ 7.2

Bearbeiten

i

RANSOMWARE-SCHUTZ

○ ● ⚡ Ransomware-Schutz
aktivieren

Ⓜ ≥ 7.0

✓

i



Modul – Ransomware Shield

Der Ransomware-Schutz ist eine verhaltensbasierte Erkennungstechnik und überwacht das Verhalten von Anwendungen und Prozessen, die versuchen, Ihre persönlichen Daten so zu verändern, wie dies für Ransomware oder Filecoder üblich ist. Wenn das Verhalten einer Anwendung als bösartig erkannt wird oder eine Anwendung bei einem reputationsbasierten Scan als verdächtig eingestuft wird, wird entweder die Anwendung gesperrt und der Prozess beendet, oder der Benutzer wird gefragt, ob er die Anwendung blockieren oder erlauben möchte

Für den ordnungsgemäßen Betrieb des Ransomware-Schutzes muss ESET LiveGrid® aktiviert sein.

Modul – Ransomware Shield

ESET Endpoint for Windows

Zu suchender Typ...

ERKENNUNGSRoutine

58

Echtzeit-Dateischutz

14

Cloudbasierter Schutz

8

Malware-Scans

33

HIPS

1

UPDATE

43

NETZWERKSCHUTZ

9

WEB UND E-MAIL

11

MEDIENKONTROLLE

TOOLS

7

BENUTZEROBERFLÄCHE

4

VERRIDE-MODUS

4

ALLGEMEIN

1

HIPS aktivieren

✓

Selbstschutz aktivieren

✓

Protected Service aktivieren

≥ 6.6

≥ 8.1

✓

Erweiterte Speicherprüfung aktivieren

✓

Exploit-Blocker aktivieren

✓

TIEFE VERHALTENSINSPEKTION

Tiefe Verhaltensinspektion aktivieren

≥ 7.2

✓

Ausschlüsse

RANSOMWARE-SCHUTZ

Ransomware-Schutz aktivieren

Audit-Modus für Ransomware Shield aktivieren

HIPS-EINSTELLUNGEN

Der Ransomware-Schutz ist eine verhaltensbasierte Erkennungsmethode, die das Verhalten von Anwendungen und Prozessen überwacht, die versuchen, Dateien auf dieselbe Weise zu bearbeiten wie Ransomware/Filecoder. Wenn das Verhalten einer Anwendung als bösartig eingestuft wird oder die reputationsbasierte Prüfung eine Anwendung als verdächtig erkennt, wird die Anwendung gesperrt und der Prozess beendet. ESET Live Grid muss aktiviert sein, damit der Ransomware-Schutz ordnungsgemäß funktioniert.

eset ENJOY SAFER TECHNOLOGY™



Modul – Exploit Blocker

Der Exploit-Blocker sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab. Er überwacht das Verhalten von Prozessen auf verdächtige Aktivitäten, die auf einen Exploit hinweisen könnten.

Wenn der Exploit-Blocker einen verdächtigen Prozess identifiziert, kann er ihn sofort anhalten und Daten über die Bedrohung erfassen, die dann an das ESET LiveGrid®-Cloudsystem gesendet werden. Diese Daten werden im ESET-Virenlabor analysiert und genutzt, um alle Anwender besser vor unbekannten Bedrohungen und neuesten Angriffen durch Malware, für die noch keine Erkennungssignaturen vorhanden sind, zu schützen.

Modul – Exploit Blocker

ESET Endpoint for Windows

 Zu suchender Typ...

ERKENNUNGSROUTINE 58

Echtzeit-Dateischutz 14

Cloudbasierter Schutz 8

Malware-Scans 33

HIPS 1

ALLGEMEIN 1

HIPS aktivieren ☒

Selbstschutz aktivieren ☒

Protected

Service aktivieren Windows ≥ 6.6 Windows ≥ 8.1 ☒

Erweiterte Speicherprüfung aktivieren ☒

Exploit-Blocker aktivieren ☒

TIEFE VERHALTENSINSPEKTION

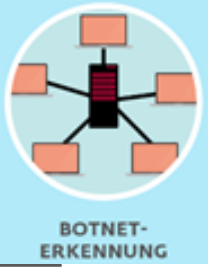
Tiefe Verhaltensinspektion aktivieren Windows ≥ 7.2 ☒

Ausschlüsse Windows ≥ 7.2 [Bearbeiten](#)

RANSOMWARE-SCHUTZ

Ransomware-Schutz aktivieren Windows ≥ 7.0 ☒

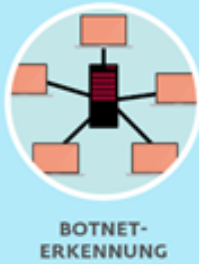
Bietet zusätzlichen Schutz für Anwendungen, die anfällig für Exploits sind, wie Webbrowser, PDF-Anzeigeprogramme, E-Mail-Clients und MS Office-Komponenten.



Modul – Botnet Erkennung

Der Botnetzschutz analysiert Kommunikationsprotokolle im Netzwerk, um Malware zu erkennen. Botnetz-Schadsoftware ändert sich häufig im Gegensatz zu den Netzwerkprotokollen, die in den vergangenen Jahren kaum geändert wurden. Mit dieser neuen Technologie überwindet ESET Malware, die sich vor Erkennung schützt und versucht, Ihren Computer mit dem Botnetz zu verbinden.

Modul – Botnet Erkennung



ESET Endpoint for Windows



ERKENNUNGSROUTINE

58

UPDATE

43

NETZWERKSCHUTZ

9

Firewall

8

Netzwerkangriffsschutz

1

WEB UND E-MAIL

11

MEDIENKONTROLLE

TOOLS

7

BENUTZEROBERFLÄCHE

4

OVERRIDE-MODUS

4



NETZWERKANGRIFFSSCHUTZ



Schutz vor Netzwerkangriffen (IDS)
aktivieren



Botnet-Erkennung aktivieren



Liste der IDS-Ausnahmen

Erkennt und blockiert die Kommunikation mit schädlichen Befehls- und Steuerservern anhand typischer Muster, wenn der Computer infiziert ist und ein Bot versucht, zu kommunizieren.



ERWEITERTE EINSTELLUNGEN

1



Vielen Dank für die Aufmerksamkeit

30

30 YEARS OF
CONTINUOUS
IT SECURITY
INNOVATION



ENJOY SAFER TECHNOLOGY™

