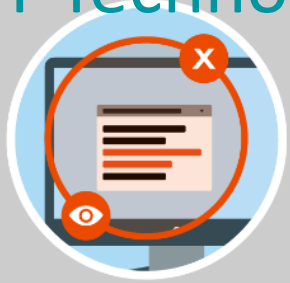
Endpoint Security ESET Module

ESET Technologie

BESTÄNDIG

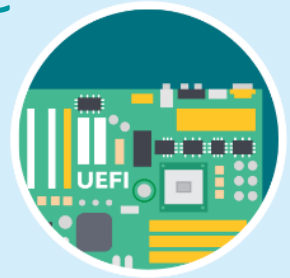


VERHALTENSBASIERTE ERKENNUNG UND BLOCKIERUNG - HIPS

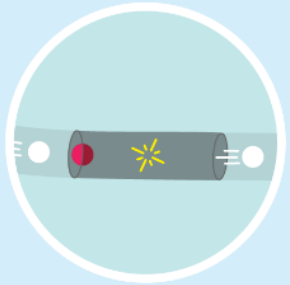
ESET LIVEGRID

MACHINE LEARNING

VOR AUSFÜHRUNG



UEFI SCANNER

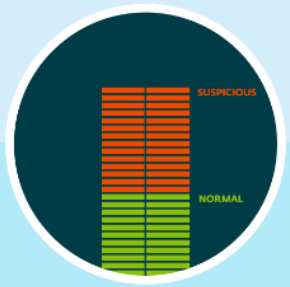


SCHUTZ VOR NETZWERKANGRIFFEN

REPUTATION & CACHE

IN-PRODUCT SANDBOX

DNA ERKENNUNG



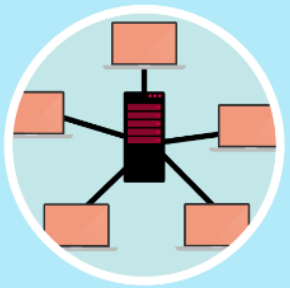
ERWEITERTE SPEICHERPRÜFUNG

RANSOMWARE SHIELD

EXPLOIT BLOCKER

NACH AUSFÜHRUNG

CLOUD-BASIERTER SCHUTZ VOR MALWARE



BOTNET-ERKENNUNG

Reputation and Cache

DNA Detections

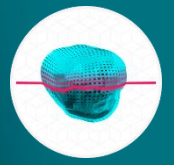
UEFI Scanner

Device Control

Network Attack Protection

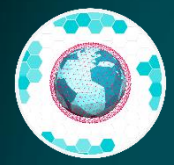
In-product Sandbox

Ransomware Shield

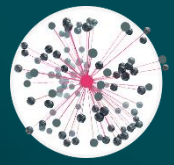


Advanced Memory Scanner

Deep Behavioral Inspection



LiveGrid® Protection



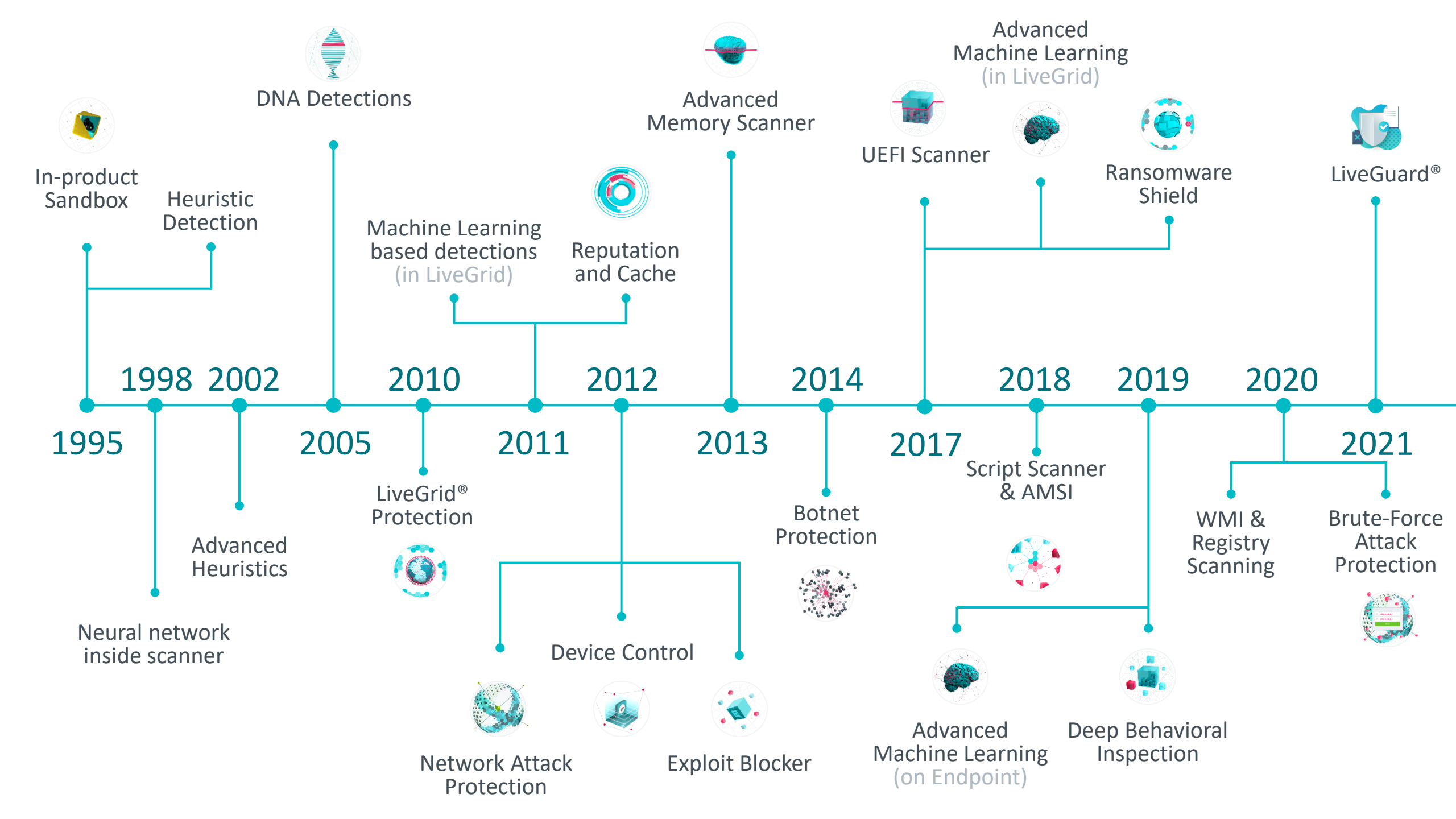
Botnet Protection

Script Scanner & AMSI

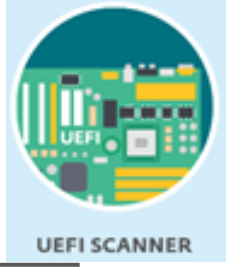
Exploit Blocker

Advanced Machine Learning

- PRE-EXECUTION
- EXECUTION
- POST EXECUTION


1995
In-product Sandbox
1998
Heuristic Detection
Neural network inside scanner
2002
Advanced Heuristics
2005
DNA Detections
2010
Machine Learning based detections (in LiveGrid)
LiveGrid® Protection
2011
Reputation and Cache
2012
Device Control
Network Attack Protection
Exploit Blocker
2013
Advanced Memory Scanner
2014
Botnet Protection
2017
Advanced Machine Learning (in LiveGrid)
UEFI Scanner
2018
Script Scanner & AMSI
Advanced Machine Learning (on Endpoint)
2019
Ransomware Shield
Deep Behavioral Inspection
2020
WMI & Registry Scanning
2021
LiveGuard®
Brute-Force Attack Protection

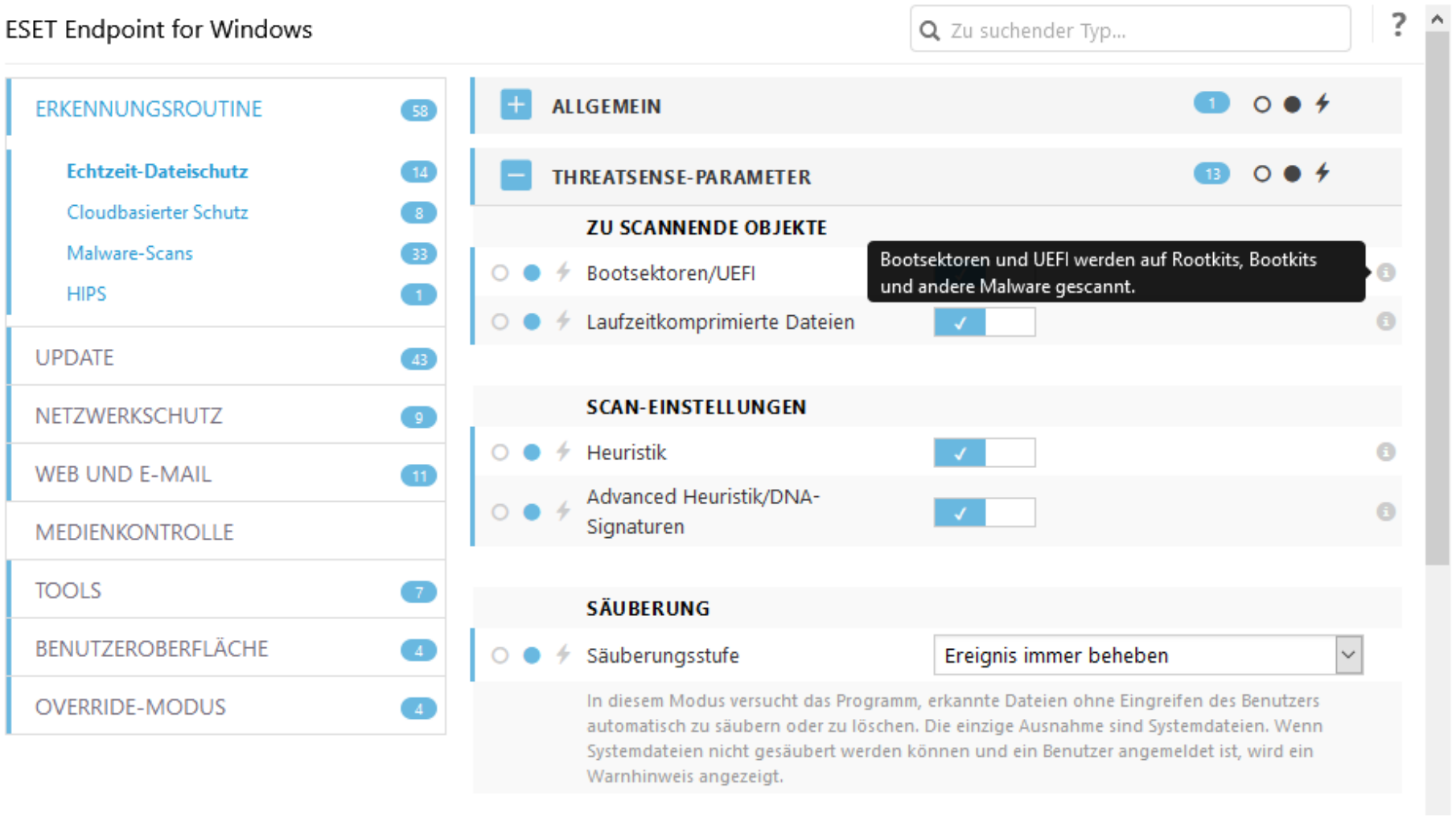
Modul – UEFI Scanner



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.

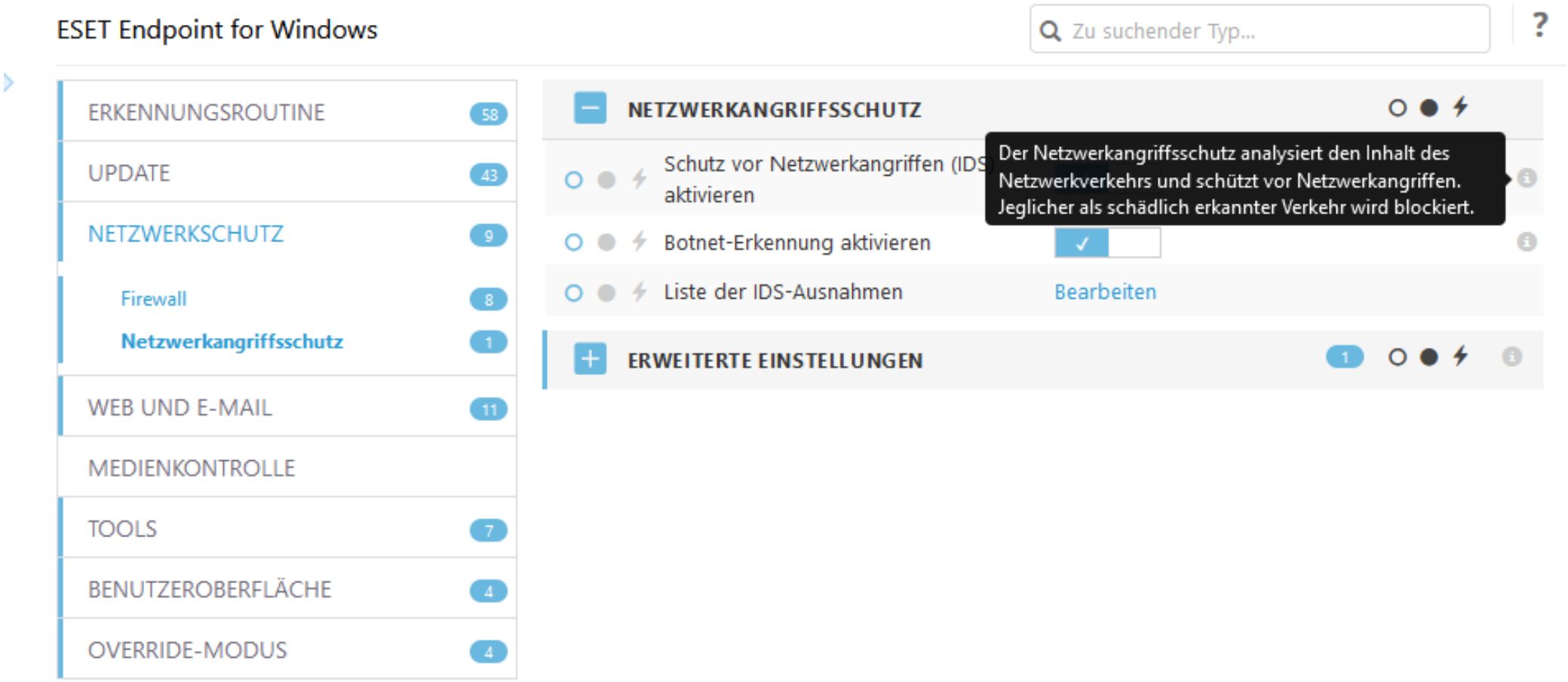
Modul – UEFI Scanner



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



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.

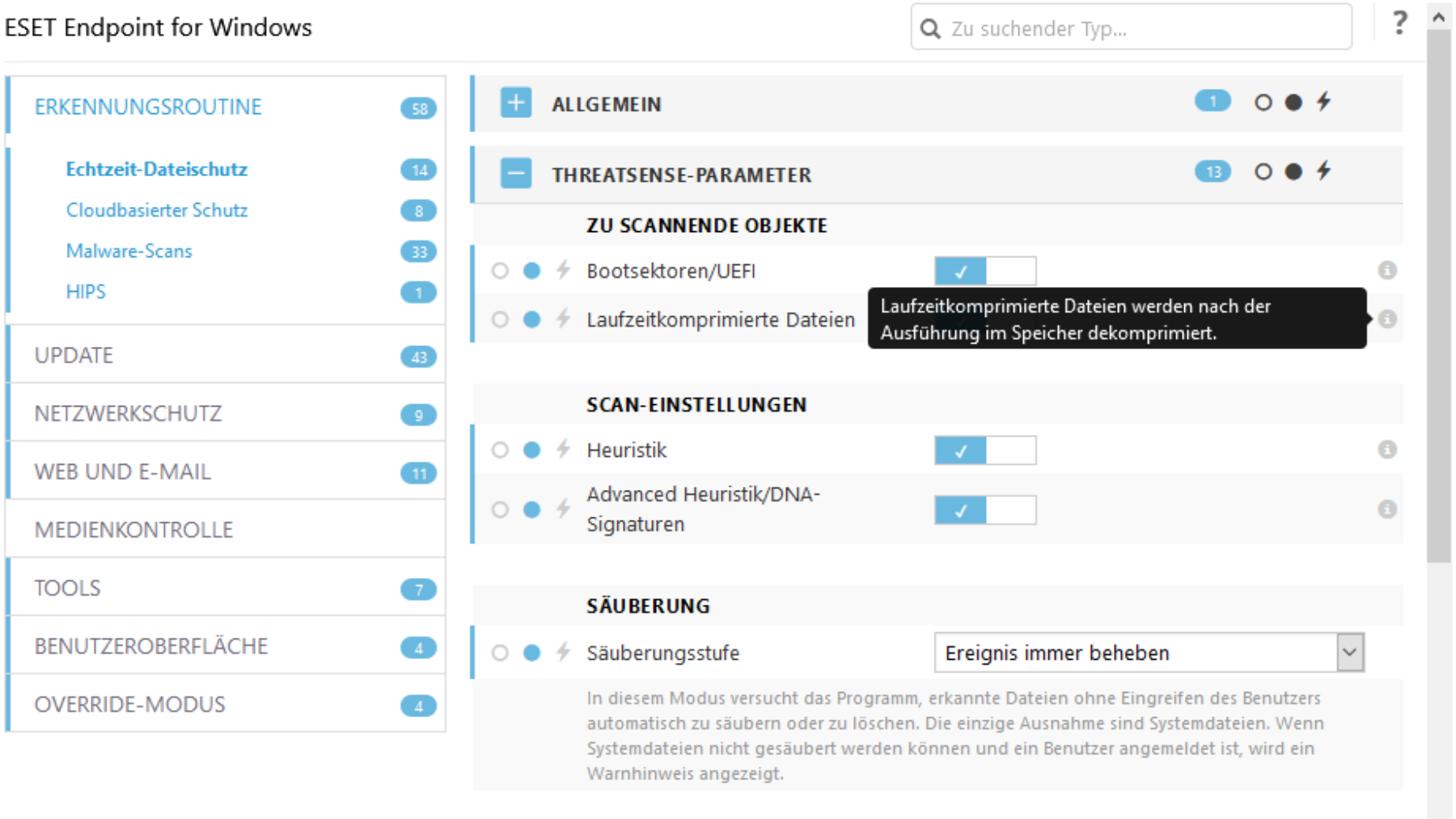
Modul – In Product Sandboxing

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

IN-PRODUCT SANDBOX

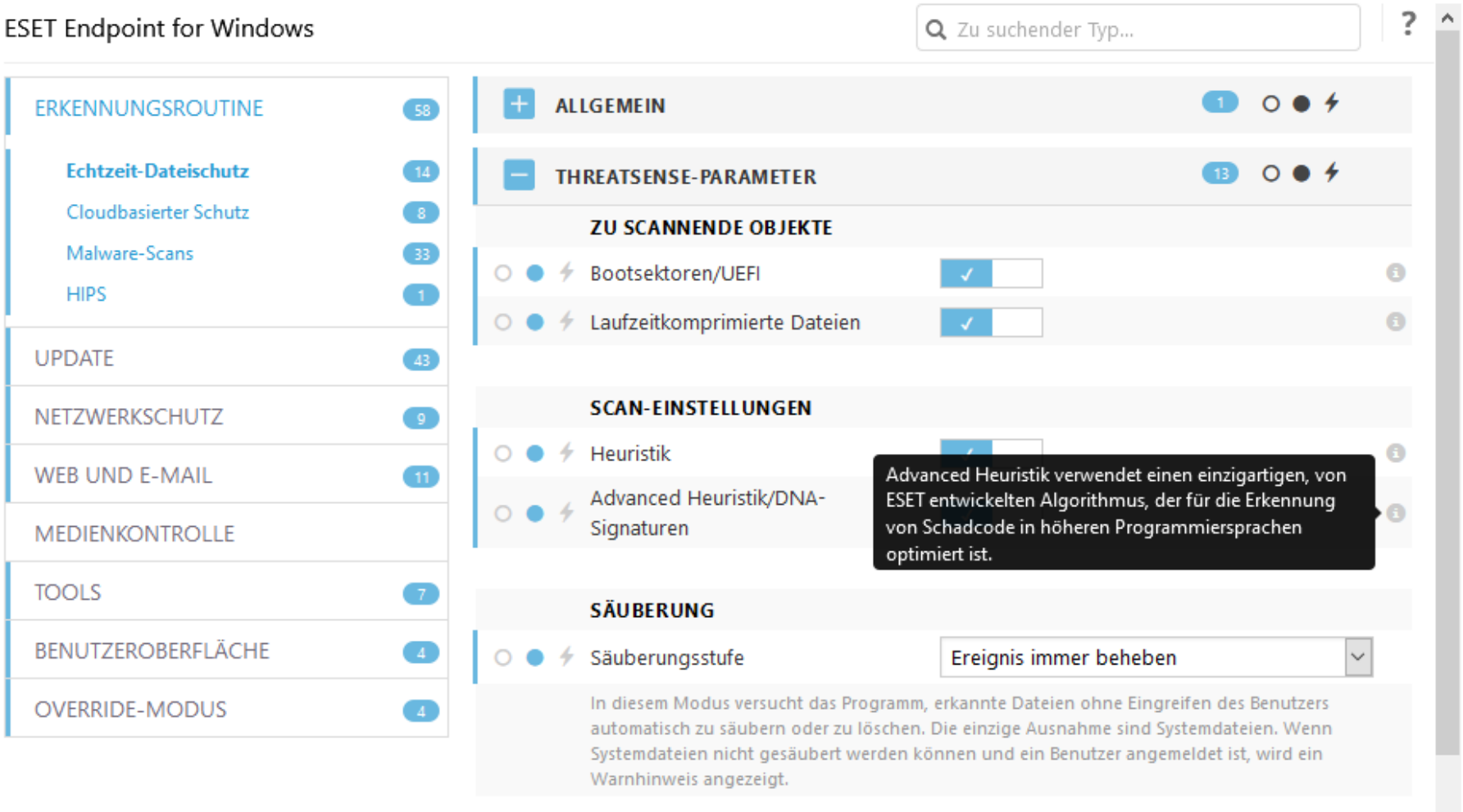


Modul – DNA Erkennung

Die Erkennungsarten reichen von sehr spezifischen Hashes bis hin zu ESET DNA-Erkennungen, einer komplexen Definition von bösartigen 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 bösartiges Verhalten hindeuten.

Modul – DNA Erkennung



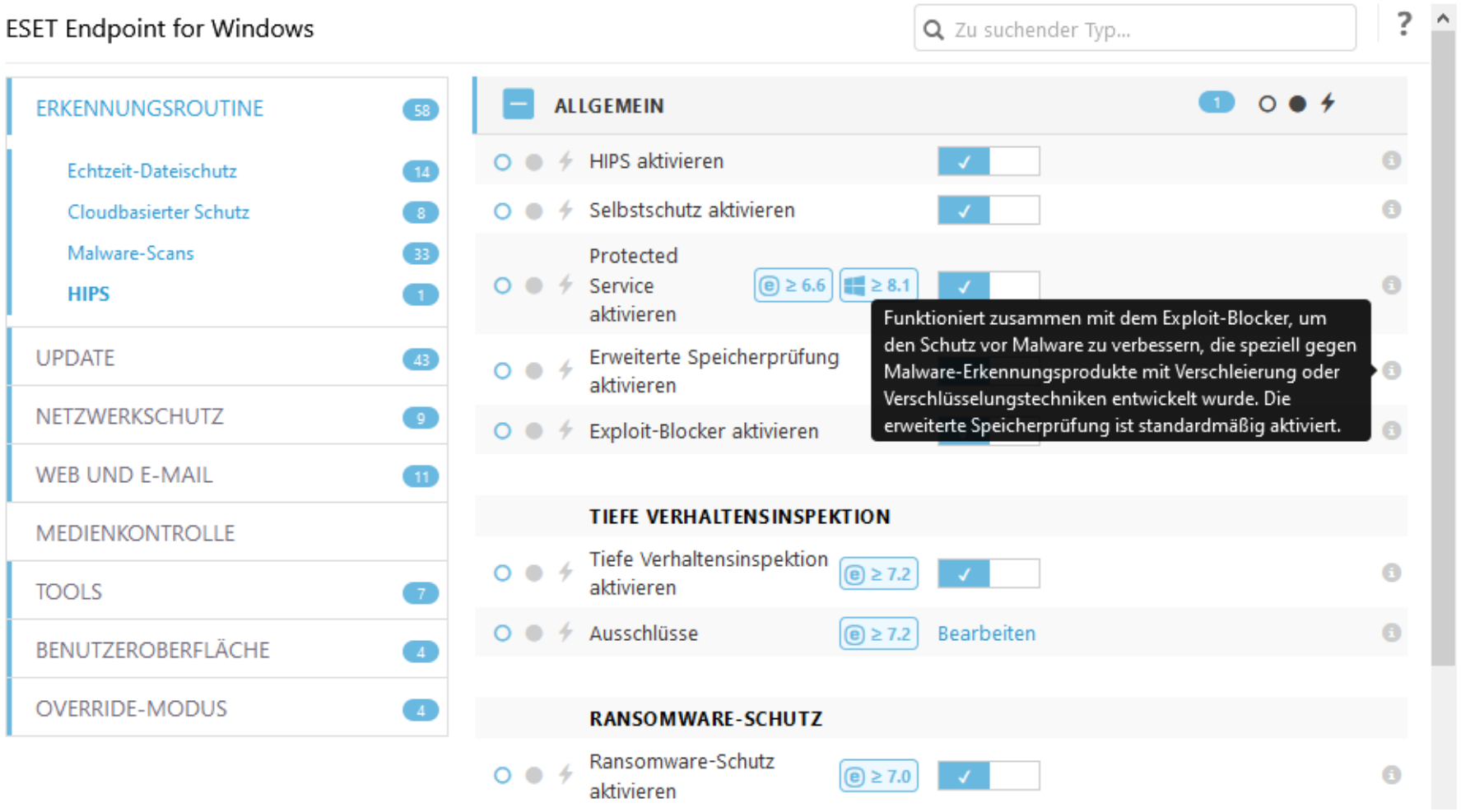
DNA ERKENNUNG

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

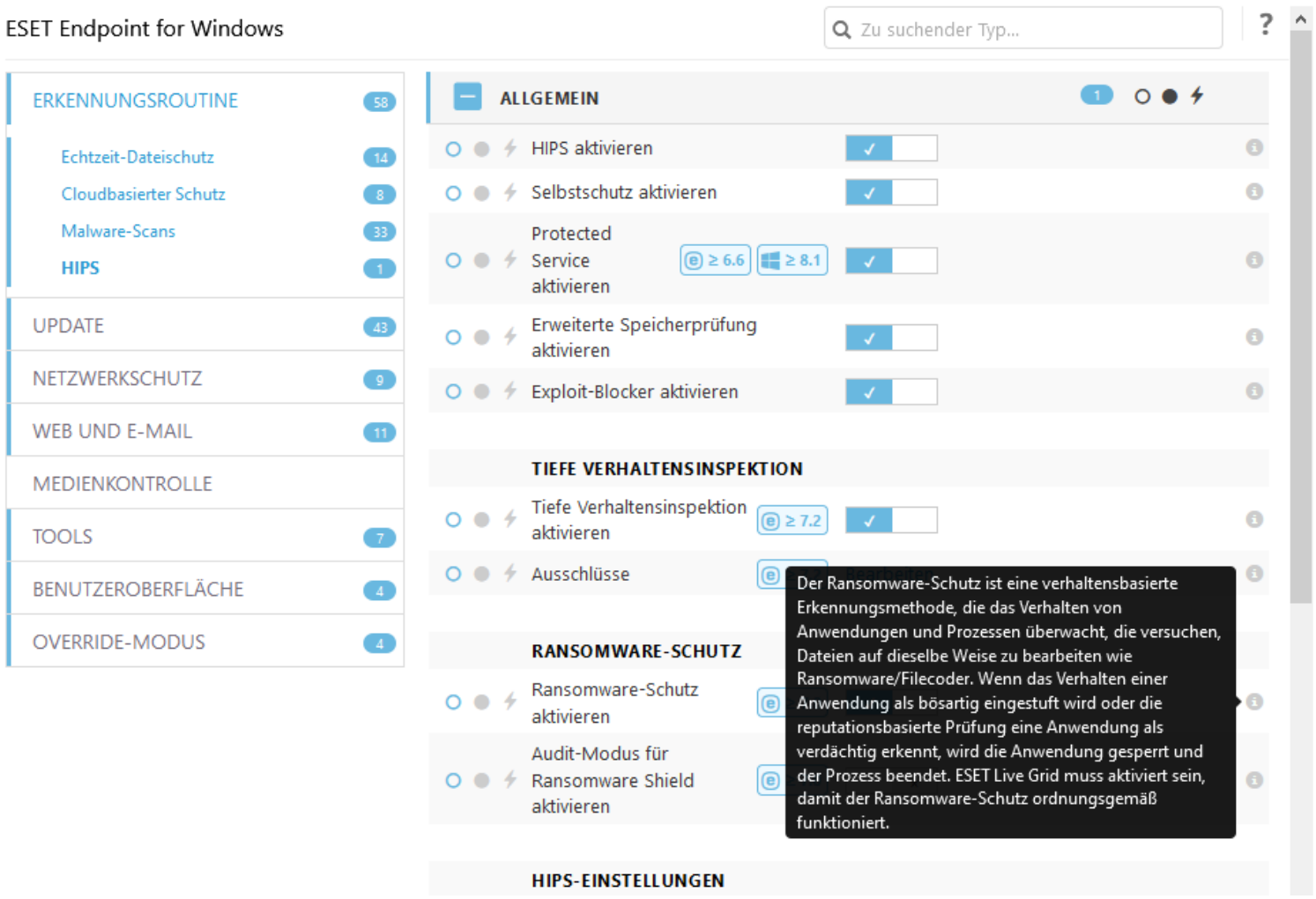


Modul – Ransomware Shield

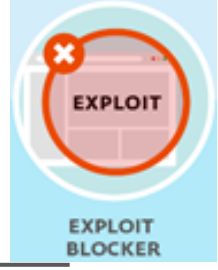
Der Ransomware-Schutz ist eine verhaltensbasierte Erkennungstechnik und überwacht das Verhalten von Anwendungen und Prozessen, die versuchen, Ihre persönlichen Daten so zu verändern, wie dies für Ransomware oder Filecoder üblich ist. Wenn das Verhalten einer Anwendung als bösartig erkannt wird oder eine 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



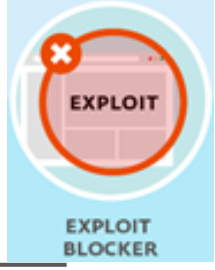
Modul – Exploit Blocker



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
- UPDATE 43
- NETZWERKSCHUTZ 9
- WEB UND E-MAIL 11
- MEDIENKONTROLLE
- TOOLS 7
- BENUTZEROBERFLÄCHE 4
- OVERRIDE-MODUS 4

ALLGEMEIN 1

- HIPS aktivieren
- Selbstschutz aktivieren
- Protected Service aktivieren ≥ 6.6 ≥ 8.1
- Erweiterte Speicherprüfung aktivieren
- Exploit-Blocker aktivieren

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

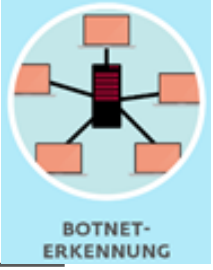
TIEFE VERHALTENSINSPEKTION

- Tiefe Verhaltensinspektion aktivieren ≥ 7.2
- Ausschlüsse ≥ 7.2 Bearbeiten

RANSOMWARE-SCHUTZ

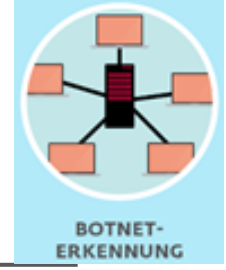
- Ransomware-Schutz aktivieren ≥ 7.0

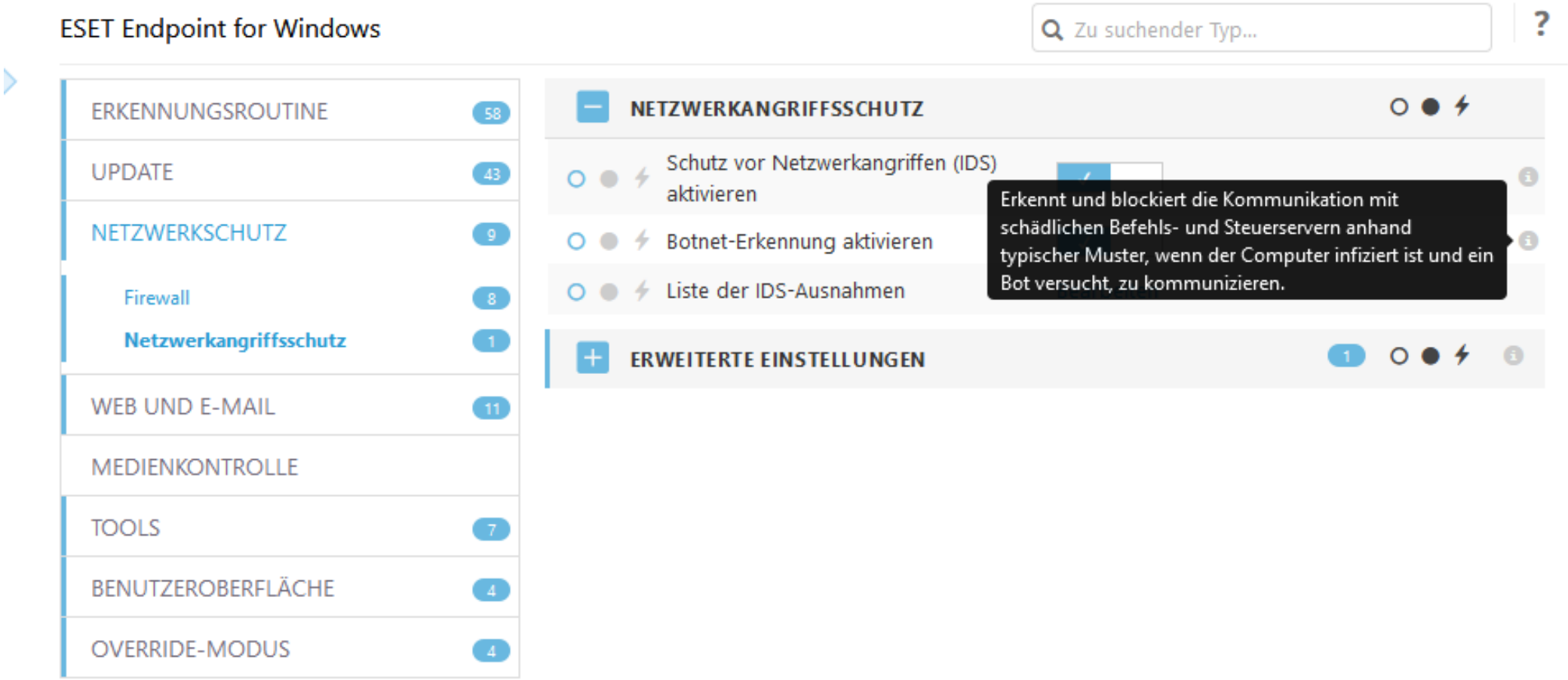
Modul – Botnet Erkennung



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





Vielen Dank für die Aufmerksamkeit

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ENJOY SAFER TECHNOLOGY™