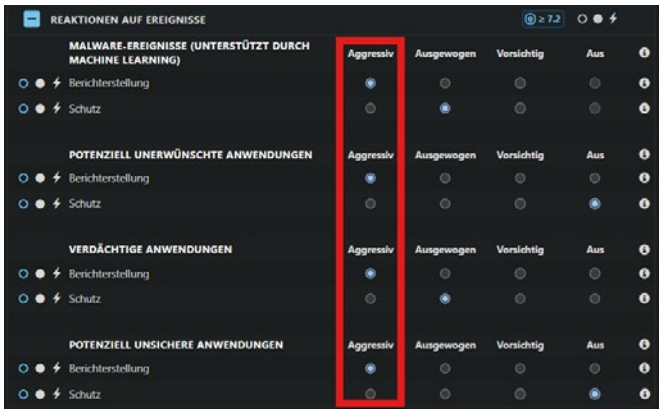
Digital Security
Progress. Protected.

Best Practice für **ESET Endpoint Security for Windows** (Version 12)

Diese Best Practice-Anleitung gilt für ESET Endpoint Security for Windows Version 12. Alle hier gezeigten Vorschläge sind über die erweiterten Optionen (Kurzbefehl: F5) aufrufbar. Es ist möglich, dass sich diese Einstellungsmöglichkeiten in zukünftigen Versionen ändern. Alle Best Practice-Empfehlungen sind mit einer Begründung versehen. Falls ein Vorschlag für Sie nicht relevant ist, können Sie diesen Punkt gerne überspringen.

Vorschlag 1

Via *F5* können Sie die *Erweiterten Schutzfunktionen* erreichen. Aktivieren Sie unter *Schutzfunktionen* die Option *Berichterstattung: Aggressiv*. Dadurch sehen Sie, welche Dateien und Anwendungen ESET empfiehlt zu blockieren. Diese Informationen können Sie anschließend im Bericht *Aktive Ereignisse* einsehen.



Mehr Informationen über *Potenziell unsichere Anwendungen* finden Sie hier:

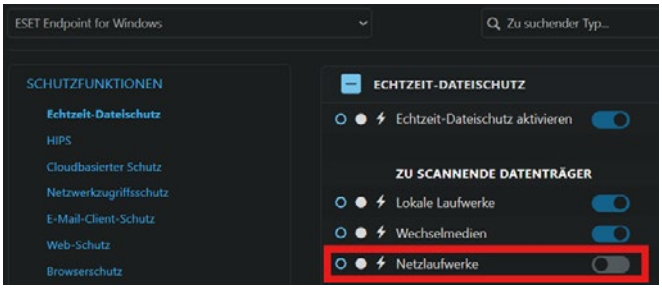
↗https://help.eset.com/glossary/de-DE/unsafe_application.html

Mehr Informationen über *Potenziell unerwünschte Anwendungen* finden Sie hier:

↗https://help.eset.com/glossary/de-DE/unwanted_application.html

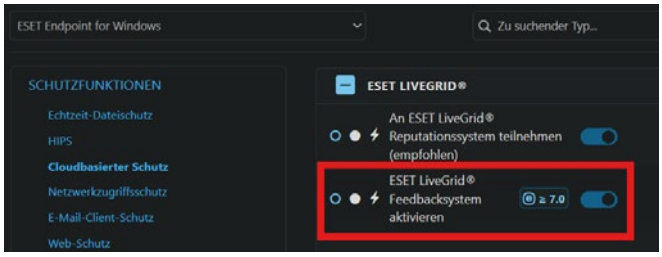
Vorschlag 2

Deaktivieren Sie unter *Echtzeit-Dateischutz* das *Scannen von Netzlaufwerken*. Sie werden in der Regel bereits durch ESET Server Security (für Windows oder Linux) überwacht, sodass ein erneuter Scan bei jedem einzelnen Endpoint nicht erforderlich ist. Dies reduziert die Systemlast und verbessert die Performance, insbesondere beim flächendeckenden Rollout von ESET.

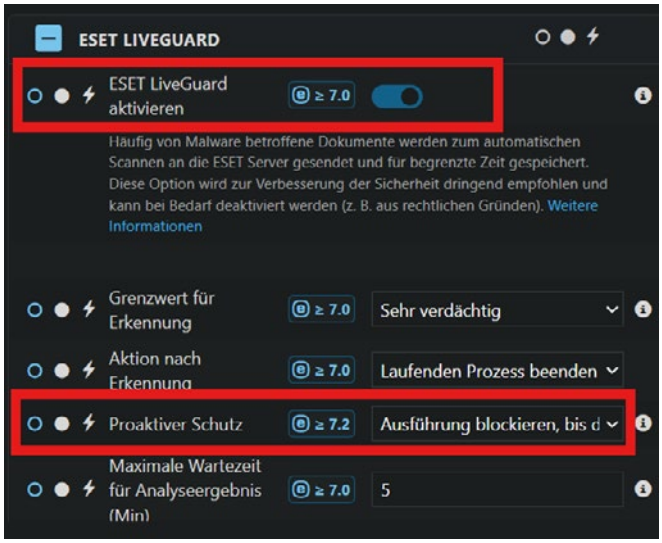


Vorschlag 3

Aktivieren Sie *ESET LiveGuard*, um die Cloud Sandboxing-Technologie zu nutzen. Dafür muss das *ESET LiveGrid®-Feedbacksystem* aktiviert sein. So werden Erkenntnisse über neuartige Malware, die zuerst in Ihrer Umgebung erkannt werden, mit anderen ESET Nutzern weltweit geteilt. Dabei werden ausschließlich Hash-Werte und keinerlei andere Daten übermittelt.



Zusätzlich empfehlen wir, unter *ESET LiveGuard®* den *Proaktiven Schutz* auf *Ausführung blockieren, bis Analyseergebnis vorliegt* zu setzen. Damit schützen Sie sich effektiv vor unbekannter Malware, sogenannten never-seen-before Attacken sowie Zero-Day-Exploits.



Hinweis: Dieses Feature ist in allen ESET PROTECT Business Bundles enthalten, ausgenommen von ESET PROTECT Entry.

Weitere Details zu ESET LiveGuard® finden Sie hier:

↗https://help.eset.com/elga/de-DE/overview.html

Vorschlag 4

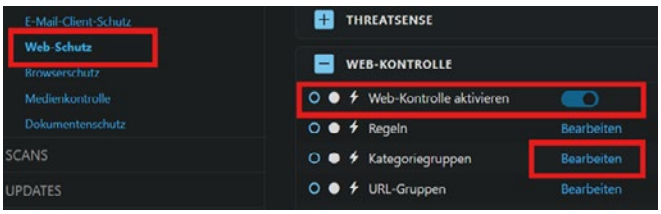
Aktivieren Sie die *Web-Kontrolle*. Dabei handelt es sich um einen DNS-basierten URL-Filter. Auch wenn diese Funktion häufig bereits durch die Firewall abgedeckt wird, bietet diese Einstellung eine zusätzliche Schutzschicht direkt am Endpoint.

Ergänzen Sie unter *Kategoriegruppen* das Feld *Sicherheit und Malware*. So profitieren Sie von den ESET Sensordaten: URLs und IP-Adressen, die als gefährlich eingestuft wurden, werden automatisch blockiert – noch bevor eine Verbindung zur Schadensquelle aufgebaut werden kann.

Weiterführende Informationen zur Web-Kontrolle finden Sie hier:

↗https://help.eset.com/ees/12/de-DE/idh_config_web_control.html

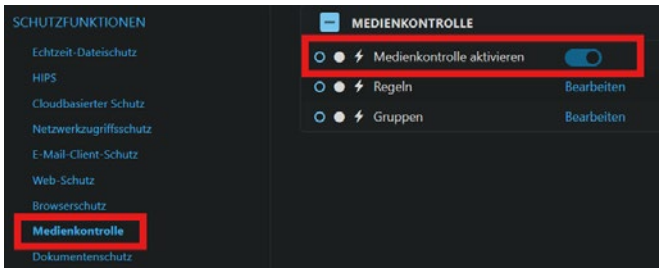
Hinweis: Die Web-Kontrolle ist Bestandteil in allen ESET PROTECT Business Bundles.



Vorschlag 5

Aktivieren Sie die *Medienkontrolle*, um die Kontrolle über alle USB-Schnittstellen zu behalten. Bitte beachten Sie, dass nach der Aktivierung ein Neustart empfohlen wird – dieser wird jedoch nicht automatisch erzwungen.

Die Medienkontrolle kann zunächst eingeschaltet und die entsprechenden Regeln können zu einem späteren Zeitpunkt definiert werden.



Mehr Informationen zur Medienkontrolle gibt es hier:

↗https://help.eset.com/ees/12/de-DE/idh_config_devmon_rule_dlg.html?idh_config_devmon.html

Falls Sie USB- oder andere externe Geräte sperren, filtern oder Zugriffsrechte anpassen möchten, finden Sie hier eine entsprechende Anleitung:

↗https://help.eset.com/ees/12/de-DE/idh_config_devmon_rule_edit_dlg.html

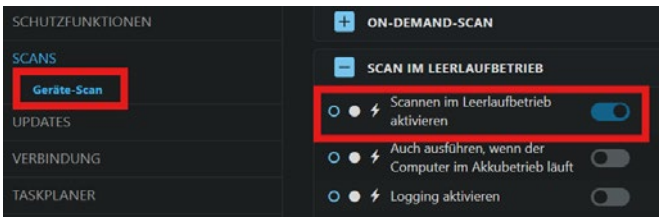
Hinweis: Die Medienkontrolle ist Bestandteil in allen ESET PROTECT Business Bundles.

Vorschlag 6

Aktivieren Sie *Scannen im Leerlaufbetrieb*, damit ein Scan automatisch durchgeführt wird, sobald der Rechner nicht aktiv genutzt wird.

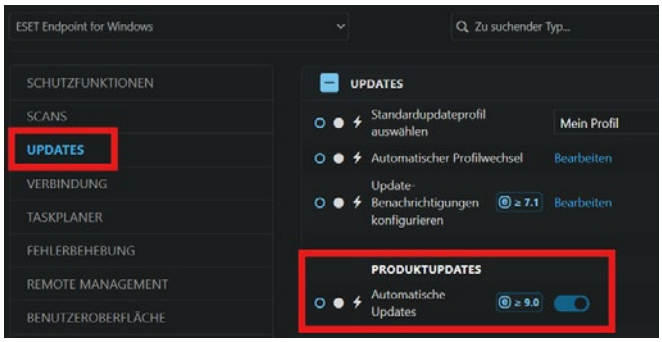
Weitere Details finden Sie hier:

↗https://help.eset.com/ees/12/de-DE/idh_config_idle_scan.html



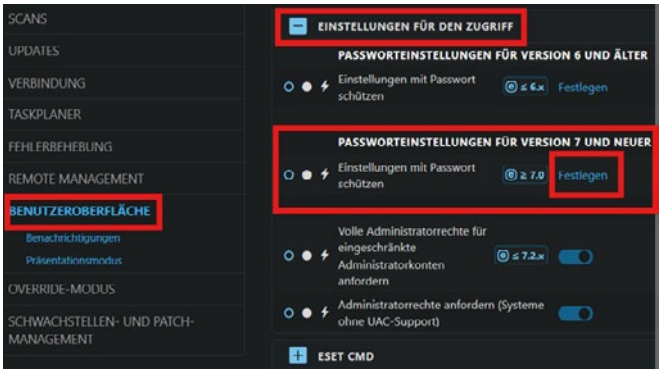
Vorschlag 7

Aktivieren Sie die automatischen Updates, um sicherzustellen, dass Feature-Updates regelmäßig installiert werden. Dadurch bleibt Ihre Endpoint Security for Windows immer auf dem neuesten Stand und Sie können neue Funktionen sofort nutzen.



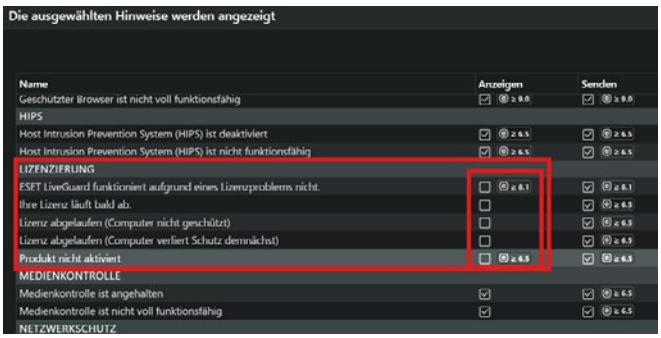
Vorschlag 8

Schützen Sie den Zugriff auf die Einstellungen in der Benutzeroberfläche mit einem Passwort, um eine unerwünschte Deinstallation der Endpoint Security zu verhindern.



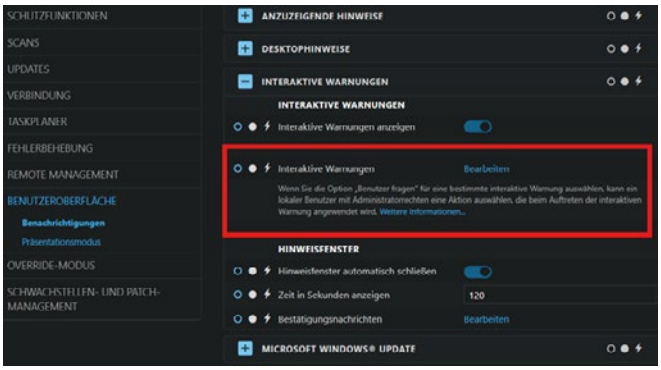
Vorschlag 9

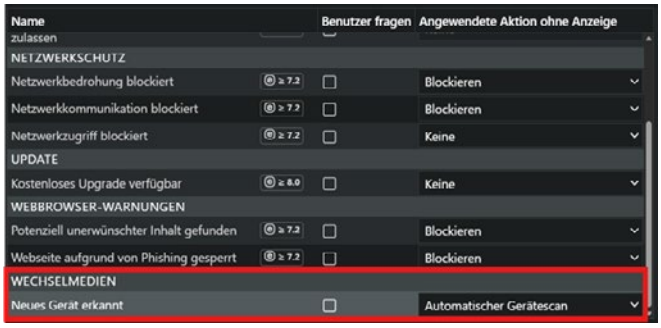
Deaktivieren Sie alle lizenzbezogenen Statusmeldungen für den Nutzer, indem Sie die entsprechenden Häkchen entfernen. So werden diese Meldungen nicht mehr in der Programmoberfläche angezeigt.



Vorschlag 10

Entfernen Sie den Haken bei *Benutzer fragen* unter *Wechselmedien* und *Neues Gerät erkannt*. Dadurch wird das Scannen aller USB-Sticks und sonstiger Speichermedien aktiviert. Mit der Option *Automatischer Geräte-Scan* startet der Scan sofort, sobald ein USB-Gerät oder Speichermedium angeschlossen wird. Der Scanvorgang kann jederzeit vom Nutzer unterbrochen werden. Wenn Sie eine Unterbrechung durch den Nutzer verhindern möchten, wählen Sie *Erzwungener Geräte-Scan*.





Weitere Informationen zu den verschiedenen Scan-Optionen finden Sie hier:

↗https://help.eset.com/ees/12/de-DE/idh_config_rem_media_amon.html

Vorschlag 11

Aktivieren Sie das Schwachstellen- und Patch-Management (ESET Vulnerability & Patch Management).

Hinweis: Dieses Feature ist exklusiv in der Cloud-Version von ESET PROTECT enthalten und nur Bestandteil in den Cloud Business Bundles **ESET PROTECT Complete** und **ESET PROTECT Elite**.

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Endpoint Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN

BVB 09 CHAMPION PARTNER

Seit 2019 ein starkes Team
auf dem Platz und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal
www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel
„IT Security made in EU" verliehen

ISO 9001 SGS
ISO/IEC 27001 SGS

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2022 zertifiziert

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

500.000+
Geschützte Unternehmen

176
Länder & Regionen

11
Forschungs- und Entwicklungszentren weltweit