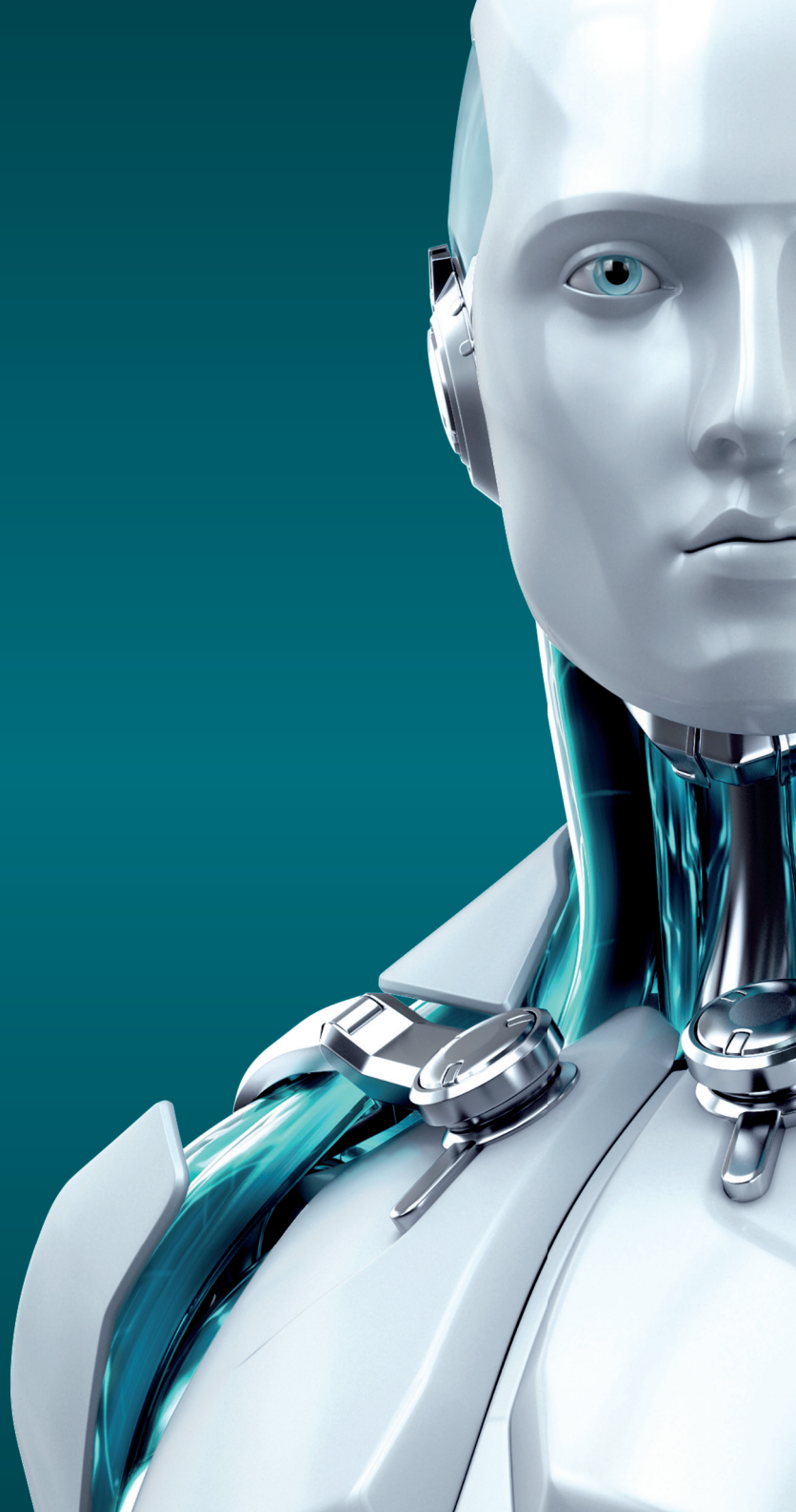
# ENDPOINT SECURITY

FOR WINDOWS

BUSINESS

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ENJOY SAFER TECHNOLOGY™



# ENDPOINT SECURITY
FOR WINDOWS

ESET Endpoint Security kombiniert unsere vielfach ausgezeichnete ESET NOD32®-Technologie mit individuellen Konfigurationsmöglichkeiten und bietet dadurch den optimalen Schutz - ganz nach Ihren Bedürfnissen.

Der geringe Ressourcenverbrauch, die optimierte Unterstützung virtueller Umgebungen sowie der optionale Cloud-basierte Scan sorgen für einen reibungslosen Systembetrieb.

Mit dem komplett neuen, anwenderfreundlichen Remote Administrator Tool haben Sie stets alles im Blick.

## Endpoint-Schutz

| | |
|---|---|
| **Antivirus und Antispyware** | Eliminiert alle Arten an Bedrohungen wie Viren, Rootkits, Würmer und Spyware.<br><br>**Optional Cloud-basierte Scans:**<br>Für eine bessere Erkennungsleistung und schnellere Prüfungen werden bekannte Dateien in einer cloud-basierten Reputationsdatenbank auf eine Black- oder Whitelist gesetzt.<br>Hierbei werden lediglich anonymisierte Metadaten über ausführbare Dateien und Archive an diese Datenbank übermittelt. |
| **Optimiert für virtuelle Umgebungen** | Der ESET Shared Local Cache speichert Metadaten über bereits geprüfte Dateien und vermeidet somit Mehrfachscans. Insbesondere bei virtuellen Umgebungen kann dies die Systemlast erheblich reduzieren.<br>ESET-Updates und Programm-Module können an anderen Orten als den Standard-Pfaden abgelegt werden (z.B. in Netzwerkfreigaben). So bleiben sie auch dann aktuell, wenn eine virtuelle Maschine auf einen vorherigen Snapshot zurückgesetzt wird. |
| **Host-Based Intrusion Prevention System (HIPS)** | Erlaubt Ihnen das Erstellen von Regeln für die Registry, Prozesse, Anwendungen und Dateien.<br>Schützt Sie vor unautorisierten Vorgängen und erkennt Bedrohungen basierend auf dem Systemverhalten. |
| **Exploit Blocker** | Blockiert gezielt Angriffe von getarnter Malware und wehrt Attacken auf Webbrowser, PDF-Reader und andere Anwendungen ab.<br>Der Exploit Blocker überwacht verdächtige Prozesse und zeigt auch bei unbekannten Bedrohungen wie Zero-Day-Angriffen volle Abwehrleistung. |
| **Erweiterte Speicherprüfung** | Entdeckt verschlüsselte oder getarnte Malware, die einer Erkennung durch klassische Methoden entgeht. Dazu werden verdächtige Prozesse überwacht und blockiert, sobald sie im Arbeitsspeicher ihre schädlichen Funktionen zur Ausführung bereitstellen. |
| **Client Antispam** | Filtert effektiv Spam und scannt alle eingehenden E-Mails auf Malware.<br>Native Unterstützung für Microsoft Outlook (POP3, IMAP, MAPI). |
| **Plattformübergreifender Schutz** | ESET-Sicherheitslösungen erkennen zuverlässig Windows-, macOS- sowie Linux-Bedrohungen und bieten somit noch besseren Schutz in Multi-Plattform-Umgebungen. |

## Schutz vor Datendiebstahl

| | |
|---|---|
| **Web-Kontrolle** | Anhand von vordefinierten Kategorien wie „Gaming", „Soziale Netzwerke" oder „Shopping" lassen sich Zugriffe auf Webseiten problemlos beschränken.<br>Sie können gemäß der Unternehmensrichtlinien Regeln für Nutzergruppen erstellen. Die Einstellung „Zulassen und Warnen" benachrichtigt den Nutzer über eine gesperrte Webseite und gibt ihm die Möglichkeit, protokollierten Zugriff zu erhalten. |
| **Anti-Phishing** | Schützt Nutzer vor gefälschten oder manipulierten Webseiten, die auf persönliche Daten wie Benutzernamen, Passwörter oder Bankinformationen zugreifen wollen. |
| **Zwei-Wege-Firewall** | Schützt Ihr Unternehmensnetzwerk vor unautorisierten Zugriffen und Datendiebstahl.<br>Legen Sie vertrauenswürdige Netzwerke fest und aktivieren Sie für alle anderen Verbindungen wie öffentliche Hotspots eine restriktivere Konfiguration. |
| **Schwachstellenprüfung** | Verbessert die Erkennung von Common Vulnerabilities and Exposures (CVEs) in weit verbreiteten Protokollen wie SMB, RPC und RDP.<br>Schützt vor Angriffen auf Schwachstellen, für die noch kein Update/Patch bereitgestellt wurde. |
| **Botnet-Erkennung** | Schützt Sie vor Botnet-Malware und verhindert, dass Ihre Endpoints für Spam- sowie Netzwerkangriffe missbraucht werden. |
| **Medienkontrolle** | Erlaubt dem Admin, Medien wie CDs/DVDs und USBs gezielt zu blockieren. Für Nutzergruppen lassen sich problemlos Regeln im Rahmen der Unternehmensrichtlinien festlegen.<br>Es gibt die Möglichkeit, das Medium zu sperren, schreibgeschützt darauf zuzugreifen oder den Nutzer zu warnen. Zudem kann der Zugriff auf das Medium protokolliert werden. |

## Scan- und Update-Optionen

| | |
|---|---|
| **Tiefenprüfung im Leerlauf** | Tiefenprüfungen können während des Computer-Leerlaufs ausgeführt werden.<br>Das beschleunigt spätere Scans, da der lokale Cache aktualisiert und erweitert wird. |
| **Erste Prüfung nach der Installation** | Ermöglicht, automatisch einen On-Demand-Scan 20 Minuten nach der Installation durchzuführen. Für starken Schutz von Anfang an. |
| **Update Rollback** | Lässt Sie zu einem vorherigen Stand der Module zurückkehren.<br>Verzögerte Updates sind bei Bedarf möglich, z.B. als temporäres Rollback oder manuelles Update. |
| **Verzögerte Updates** | Bietet die Möglichkeit, drei verschiedene Arten von Updates zu beziehen. Reguläre Updates, Test-Updates (enthalten Beta-Updates für Tests vor dem finalen Release) und verzögerte Updates (zwölf Stunden später, für unternehmenskritische Systeme). |
| **Lokaler Update-Mirror** | Spart die Bandbreite der Unternehmensanbindung durch das einmalige Herunterladen der Updates in einen Mirror-Ordner.<br>Mitarbeiter im Außendienst empfangen die Updates direkt von den ESET Update Servern, auch wenn der lokale Mirror nicht verfügbar ist.<br>Geschützte (HTTPS) Kommunikation wird unterstützt. |

## Unterstützte Betriebssysteme:

Microsoft Windows® 10, 8.1, 8, 7, Vista, XP sowie deren Embedded Versionen

KOSTENLOSER TECHNISCHER SUPPORT

Unsere deutschsprachigen IT-Spezialisten stehen Ihnen bei Fragen gern mit Rat und Tat zur Seite.

# Usability

| | |
|---|---|
| **RIP & Replace** | Während der Installation der ESET-Endpoint-Lösungen können Rückstände zuvor genutzter Sicherheitsprodukte gründlich entfernt werden.<br>Unterstützt 32- und 64-Bit-Systeme. |
| **Anpassbare Benutzeroberfläche** | Die Sichtbarkeit der grafischen Oberfläche lässt sich nach Bedarf anpassen: Vollständig, Minimal, Manuell oder Still. Die ESET-Software kann beim Nutzer komplett ausgeblendet werden, einschließlich Taskleistensymbol oder Benachrichtigungsfenster.<br>Nach vollständigem Ausblenden der GUI wird der „Egui.exe" Prozess überhaupt nicht ausgeführt, was den Ressourcenverbrauch reduziert. |
| **ESET License Administrator** | Gibt Ihnen per Web-Browser die volle Übersicht über Ihre Lizenzen. Sie können sämtliche Lizenzen zentral und in Echtzeit verwalten, auch ohne ESET Remote Administrator. |
| **Für Touchscreens geeignet** | ESET-Endpoint-Produkte unterstützen Touchscreens sowie hochauflösende Displays.<br>Dafür wurde die gesamte Benutzeroberfläche neu konzipiert und gestaltet.<br>Häufig genutzte Funktionen sind im Menü schnell zur Hand. |
| **Geringe Systembelastung** | ESET-Endpoint-Produkte bieten bewährten Schutz und schonen dabei Systemressourcen.<br>Durch den geringen Ressourcenbedarf der Produkte können auch ältere Systeme problemlos weiter genutzt werden. Im Akku-Modus wird die Laufzeit von Laptops erhöht. |
| **Unterstützung von rechts-nach-links-Sprachen** | Unterstützt jetzt auch von rechts nach links geschriebene Landessprachen wie Arabisch. |
| **Zentrale Verwaltung** | Alle ESET-Endpoint-Produkte können mit dem ESET Remote Administrator verwaltet werden. Über eine einzige webbasierte Management-Konsole können Sie Tasks aufsetzen und ausführen, Policies erstellen und alle Meldungen einsehen, um den Überblick über die Netzwerksicherheit zu behalten. Der Remote Administrator kann unter Windows oder Linux installiert werden und steht als Virtuelle Appliance bereit. |



www.eset.de
www.eset.at
www.eset.ch

Artikelnummer: M_Print2017_16
Stand: August 2017