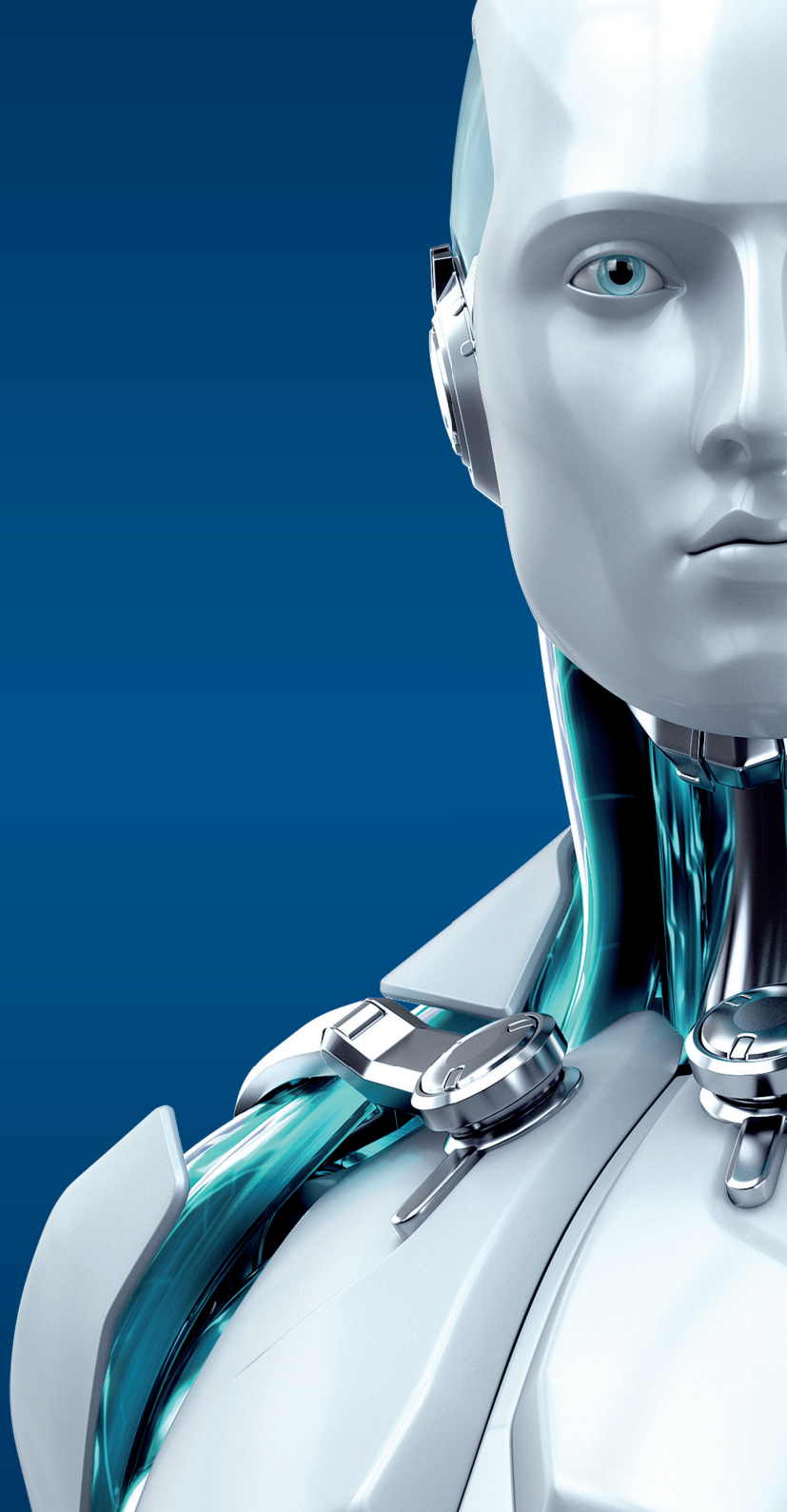
FILE SECURITY

FÜR MICROSOFT WINDOWS SERVER

ENJOY SAFER TECHNOLOGY™



FILE SECURITY
FÜR MICROSOFT WINDOWS SERVER

ESET File Security für Microsoft Windows® Server bietet einen erstklassigen Schutz für Unternehmensdaten auf Ihren File Servern.

Dank der vielfach ausgezeichneten ESET NOD32®-Technologie gewährleistet die Lösung eine schnelle Erkennung sowie einen reibungslosen Systembetrieb und sorgt damit für optimale Sicherheit.

Durch den geringen Ressourcenverbrauch bleiben Ihnen mehr Speicherplatz und CPU-Leistung für die eigentlichen Aufgaben. Ausführliche und verständliche Logs sowie Meldungen über Ihren Netzwerk- und Systemstatus verschaffen Ihnen stets den vollen Überblick.

Schutz für Ihren File Server

Antivirus und Antispyware	Eliminiert alle Arten von Bedrohungen wie Viren, Rootkits, Würmer und Spyware. **Optional Cloud-basierte Scans:** Für eine bessere Erkennungsleistung und schnellere Prüfungen werden bekannte Dateien in einer Cloud-basierten Reputationsdatenbank auf eine Black- oder Whitelist gesetzt. Hierbei werden lediglich anonymisierte Metadaten über ausführbare Dateien und Archive 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. Modul-Updates und die Signaturdatenbank können an anderen Orten als den Standard-Pfaden abgelegt werden (z.B. in Netzwerkfreigaben). So bleiben ESET-Updates auch dann aktuell, wenn eine virtuelle Maschine auf einen vorherigen Snapshot zurückgesetzt wird.
Prüfung des Hyper-V Speichers	Prüft Microsoft Windows® Server mit Hyper-V-Rolle auf Malware, ohne dass ein separates Antiviren-Produkt auf den gehosteten virtuellen Maschinen installiert werden muss. Scannt die Inhalte der Festplatte ohne Systembeeinträchtigungen und erstellt basierend auf den Scan-Ergebnissen gesonderte Reports. Prüfungen können auch auf ausgeschalteten virtuellen Maschinen durchgeführt werden, was eine bessere Performance, geringeren Speicherverbrauch und weniger CPU-Auslastung gewährleistet.
Exploit Blocker	Blockiert gezielt Angriffe von getarnter Malware und wehrt Attacken auf Webbrowser, PDF-Reader und andere Anwendungen ab. 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.
Nativer Clustering-Support	Die Sicherheitslösung kann so konfiguriert werden, dass Einstellungen automatisch kopiert werden, wenn sie in einer Cluster-Umgebung installiert wird. Mithilfe eines Assistenten können mehrere installierte Instanzen der ESET File Security problemlos in einem Cluster miteinander verbunden und gemeinsam verwaltet werden. So müssen geänderte Einstellungen nicht manuell auf andere Systeme in dem Cluster übertragen werden.
Storage Scan	Ermöglicht eine On-Demand-Prüfung von verbundenem Network Attached Storage (NAS). In Kombination mit dem im Netzwerk installierten ESET Shared Local Cache wird die Anzahl der Zugriffe auf die Netzwerk-Laufwerke erheblich reduziert.
ESET Specialized Cleaners	Im Interface finden Sie spezielle Cleaner für besonders hartnäckige und schwer zu bereinigende Malware.
Host-Based Intrusion Prevention System (HIPS)	Erlaubt Ihnen das Erstellen von Regeln für die Registry, Prozesse, Anwendungen und Dateien. Schützt Sie vor unautorisierten Vorgängen und erkennt Bedrohungen basierend auf dem Systemverhalten.

Schutz vor Datendiebstahl

Anti-Phishing	Schützt Nutzer vor gefälschten oder manipulierten Webseiten, die auf persönliche Daten wie Benutzernamen, Passwörter oder Bankinformationen zugreifen wollen.
Medienkontrolle	Erlaubt dem Admin, Medien wie CDs/DVDs und USBs gezielt zu blockieren. Für Nutzergruppen lassen sich problemlos Regeln im Rahmen der Unternehmensrichtlinien festlegen. 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. Das beschleunigt spätere Scans, da der lokale Cache aktualisiert und erweitert wird.
Update Rollback	Lässt Sie zu einem vorherigen Stand der Signaturdatenbank und der Module zurückkehren. 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. Mitarbeiter im Außendienst empfangen die Updates direkt von den ESET Update Servern, auch wenn der lokale Mirror nicht verfügbar ist. Geschützte (HTTPS) Kommunikation wird unterstützt.

KOSTENLOSER TECHNISCHER SUPPORT

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

Usability

Ausschluss von Prozessen	Der Admin kann Prozesse definieren, die vom Echtzeit-Schutzmodul ignoriert werden. Alle Datei-Operationen, die diesen Prozessen zugeordnet werden, gelten automatisch als sicher. So können störende oder überflüssige Scans vermieden werden - zum Beispiel bei Backups oder beim Verschieben von virtuellen Maschinen. Ausgeschlossene Prozesse können sogar auf unsichere Dateien oder Objekte zugreifen, ohne eine Warnmeldung auszulösen.
Unterstützung für WMI (Windows Management Instrumentation)	Bietet die Möglichkeit, mithilfe des Windows Management Instrumentation Frameworks die Schlüsselfunktionen der ESET File Security zu überwachen. Dadurch kann der ESET File Server problemlos in Managementsysteme anderer Anbieter und SIEM-Software wie Microsoft System Center Operations Manager, Nagios und weitere integriert werden.
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. 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.
Modulare Installation	Erlaubt Ihnen, die zu installierenden Komponenten festzulegen: • Echtzeit-Dateischutz • Web-Protokoll-Filterung • Medienkontrolle • Grafische Benutzeroberfläche (GUI) • E-Mail-Client-Schutz • ESET Log Collector • ESET SysInspector • ESET SysRescue • Offline-Hilfe
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.
ESET Log Collector	Ein hilfreiches Tool, das alle notwendigen Logs für die Fehleranalyse sammelt und in einem Archiv abspeichert. Dieses Archiv kann per E-Mail gesendet oder im Netzwerk abgelegt werden, erleichtert den technischen Support und beschleunigt die Fehlerbehebung.

Artikelnummer: M_Print2015_03
Stand: Oktober 2015