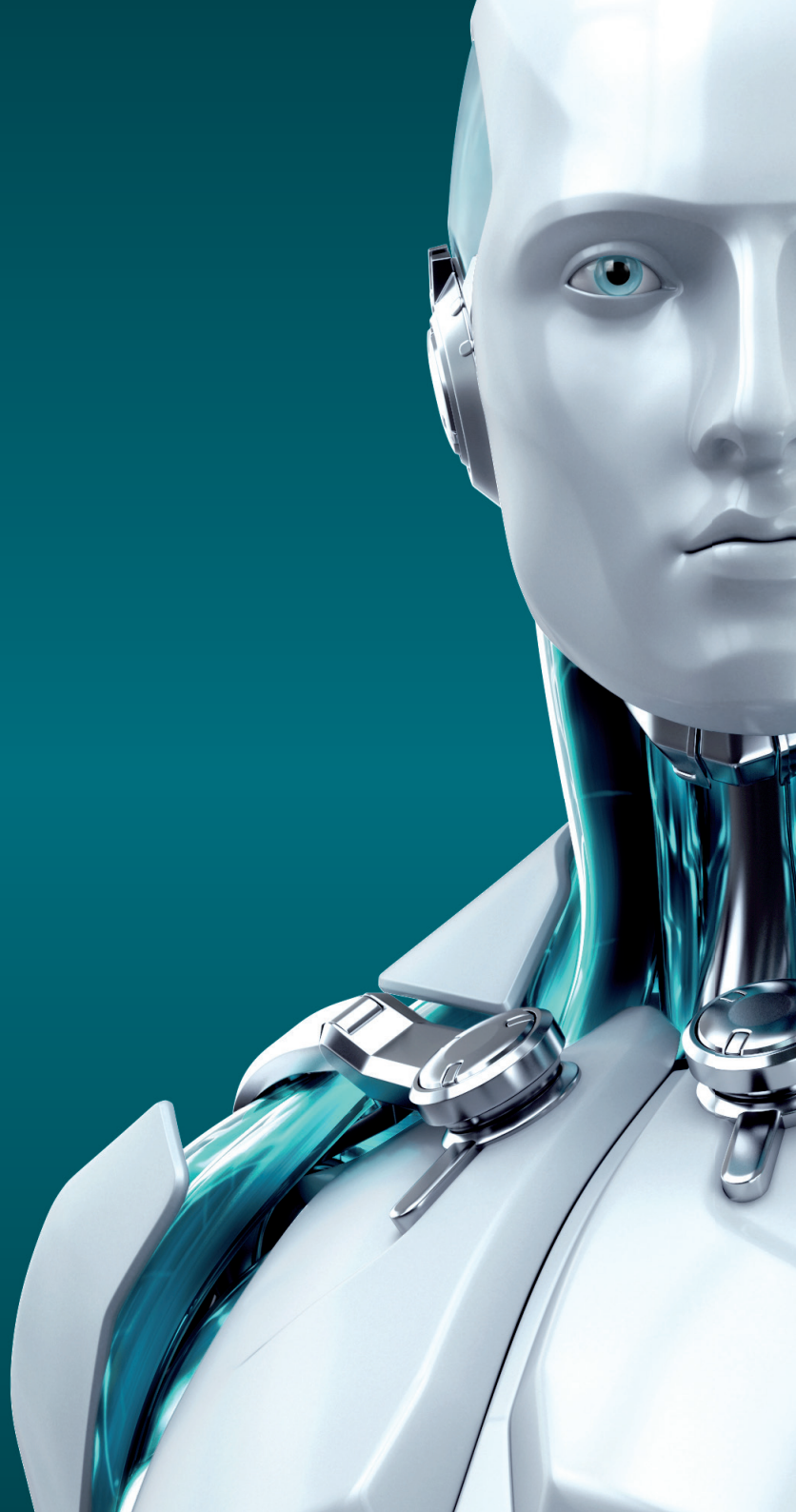
MAIL SECURITY

FOR MICROSOFT EXCHANGE SERVER

BUSINESS

ENJOY SAFER TECHNOLOGY™



MAIL SECURITY

FOR MICROSOFT EXCHANGE SERVER

ESET Mail Security für Microsoft Exchange Server enthält leistungsstarke Antiviren- und Antispam-Technologien, die E-Mail-Bedrohungen schon am Server stoppen.

Unsere Lösung bietet erstklassigen Rundum-Schutz für Ihre Server und Daten. Basierend auf realen Dateitypen können Sie Regeln für spezifische Inhalte erstellen, den Sicherheitsstatus jederzeit überwachen sowie die Konfiguration über den ESET Remote Administrator optimal einstellen.

Effektiver Schutz vor Bedrohungen

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 anonyme Metadaten über ausführbare Dateien und Archive übermittelt.
Antispam und Anti-Phishing	Verhindert effektiv Spam- sowie Phishing-Versuche, ohne dass Einstellungen oder Schwellenwerte manuell konfiguriert werden müssen.
Lokale Quarantäne-Verwaltung	Jeder Mailbox-Nutzer kann über einen eigenständigen Browser die Nachrichten einsehen, die als Spam oder verdächtig eingestuft und in Quarantäne verschoben wurden. Je nach vom Admin festgelegten Rechten kann der Nutzer die Nachrichten hier sortieren, durchsuchen oder bestimmte Aktionen durchführen - für einzelne Nachrichten oder Nachrichten-Gruppen. Die erlaubten Aktionen variieren je nach Grund für die Quarantäne. Es ist möglich, regelmäßig einen Bericht an den Nutzer zu senden, in dem Informationen über die in Quarantäne verschobenen Nachrichten sowie Links zur Ausführung von Aktionen enthalten sind.
On-Demand-Scan der Datenbank	Ermöglicht Ihnen, Server-Ressourcen zu sparen, indem der Administrator bestimmt, welche Datenbanken und Mailboxen überprüft werden sollen. Darüber hinaus kann der Zeitstempel der letzten Änderung einer Nachricht genutzt werden, um die Prüfung weiter einzugrenzen.
Regeln für die Nachrichten-Verarbeitung	Bieten eine Reihe an anpassbaren Regeln für die Verarbeitung einzelner Nachrichten. Zu den Parametern gehören Standardfelder wie Betreff, Sender, Text und Nachrichten-Header sowie vorherige Ergebnisse von Spam- und Antiviren-Prüfungen. Beschädigte oder Passwort-geschützte Archive werden automatisch erkannt. Anhänge werden intern überprüft, um den tatsächlichen Dateityp zu ermitteln.
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.
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.
Medienkontrolle	Erlaubt dem Admin, Medien wie CDs/DVDs und USB Geräte 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.

Komplexe Umgebungen komfortabel verwalten

Unabhängig von Snapshots	ESET-Updates und Programm-Module können an anderen Orten als den Standard-Pfaden abgelegt werden. So bleiben sie auch dann aktuell, wenn eine virtuelle Maschine auf einen vorherigen Snapshot zurückgesetzt wird.
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 Mail 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.
ESET Shared Local Cache	Vermeidet die wiederholte Prüfung mehrfach vorhandener Dateien, indem er die Metadaten bereits gescannter und als ungefährlich eingestufter Dateien in eine Whitelist einträgt. Bei Prüfungen fragt das auf dem System installierte ESET-Produkt beim Shared Local Cache an, ob die Datei bereits gescannt wurde und überspringt gegebenenfalls deren Prüfung. Befindet sich der Shared Local Cache auf einem Virtualisierungssystem, gibt es nur minimale Verzögerungen durch die Netzwerkkommunikation, was für eine optimale Performance sorgt.
Unterstützung für WMI (Windows Management Instrumentation)	Bietet die Möglichkeit, mithilfe des Windows Management Instrumentation Frameworks die Schlüsselfunktionen der ESET Mail Security zu überwachen. Dadurch kann der ESET Mail Server problemlos in Managementsysteme anderer Anbieter und SIEM-Software wie Microsoft System Center Operations Manager, Nagios und weitere integriert werden.

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.
Kleine Updates der Virendefinitionen	Reguläre Updates und Aktualisierungen werden in kleinen Paketen heruntergeladen und schrittweise ausgeführt. Das schont Systemressourcen und Internetbandbreite - ohne merkliche Auswirkungen auf die Geschwindigkeit der gesamten Netzwerk-Infrastruktur und Server oder auf Speicherplatz und CPU der Endpoints.
Modulare Installation	Ermöglicht, die zu installierenden Komponenten individuell auszuwählen – unabhängig von einer lokalen oder einer Installation per ESET Remote Administrator unter anderem: • Echtzeit-Dateischutz • Web- und E-Mail-Schutz • Medienkontrolle • Grafische Benutzeroberfläche (GUI) • ESET Log Collector
Zentrale Verwaltung	ESET Mail Security kann 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.
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.

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

Artikelnummer: M_Print2017_08
Stand: Februar 2017