LÖSUNGSANSATZ

ENJOY SAFER TECHNOLOGY™

Endpoint & Server

Umfassender Schutz von Endpoints und Servern für Unternehmen jeder Größe

VERFÜGBAR ALS MANAGED SERVICE

TEIL DES MULTI-SECURED ENDPOINT KONZEPTS

ESET.DE | ESET.AT | ESET.CH

Was ist eine **Endpoint Plattform oder Server Sicherheitslösung?**

Eine Endpoint Sicherheitslösung schützt Endgeräte, indem sie Malware-Angriffe verhindert, schädliche Aktivitäten erkennt und Funktionen zur Untersuchung sowie Behebung von Sicherheitsvorfällen und Meldungen bereitstellt.

Die ESET Server Sicherheitslösungen dienen dazu, die zentralen Server einer Organisation vor Bedrohungen aller Art zu schützen. Unternehmen setzen sich heutzutage einem Risiko aus, wenn entsprechende Lösungen nicht auf die spezifischen Anforderungen der Verarbeitung ausgerichtet sind. Beispiele hierfür sind u.a. die Speicherung von Dateien durch Mitarbeiter auf einem (gemeinsam verwendeten) Netzlaufwerk bzw. Cloud-Speicher oder die E-Mail-basierte Unternehmenskommunikation. Es ist dabei elementar wichtig, dass die eingesetzte Sicherheitslösung auf die Funktionalitäten der Server ausgelegt ist.

Vier **gute Gründe**

RANSOMWARE

Spätestens seit Cryptolocker im Jahre 2013 stellt Ransomware eine reale Gefahr für Industrienetzwerke auf der ganzen Welt dar. Das Bewusstsein dafür, dass schon ein einziger Ransomware-Angriff durch die Verschlüsselung wichtiger Dateien das gesamte Unternehmen stilllegen kann, ist stark gestiegen. Ist ein Unternehmen von Ransomware betroffen, wird oft schnell klar, dass die Wiederherstellung der Daten teuer und teilweise unmöglich ist. Die Zahlung des Lösegeldes erscheint unvermeidbar.

Die ESET Endpoint Sicherheitslösungen bieten einen vielschichtigen Schutz, der das Eindringen von Ransomware in Unternehmensnetzwerk und -kommunikation verhindert und Bedrohungen erkennt, die sich bereits im System befinden. Für Server ist Ransomware eine noch größere Gefahr, da Mitarbeiter die Schadsoftware auf einem Netzlaufwerk abspeichern könnten. Die ESET Server Sicherheitslösungen bieten daher mehrschichtige Schutzebenen, um Ransomware nicht nur zu verhindern, sondern auch zu erkennen, falls sie schon innerhalb einer Organisation existiert.

DATEILOSE ANGRIFFE

Dateilose Malware wird nur im Arbeitsspeicher ausgeführt. Sicherheitslösungen, die allein auf der Analyse von Dateien basieren, können diese nicht erkennen. Bei manchen dateilosen Angriffen werden zudem Anwendungen innerhalb des Betriebssystems genutzt, um einer Erkennung zu entgehen (z.B. Missbrauch von Power-Shell).

Die Endpoint und Server Sicherheitslösungen von ESET erkennen manipulierte oder gekaperte Anwendungen und bieten damit umfassenden Schutz vor dateilosen Angriffen. Zudem wird der Arbeitsspeicher laufend auf verdächtige Prozesse geprüft. Dank dieses mehrschichtigen Ansatzes sind die ESET Sicherheitslösungen in der Lage, selbst neuartige Bedrohungen sicher abzuwehren.

GEZIELTE ANGRIFFE UND DATENLECKS

Die moderne Bedrohungslandschaft entwickelt sich rasant mit ständig neuen Angriffsmethoden und bis dahin unbekannten Schädlingen. Unternehmen müssen stets in der Lage sein, Angriffe (bspw. Zero-Days) auf die eigenen Systeme zu erkennen und schnell zu reagieren. Dafür sind bestimmte Tasks wie die Ausführung von Prüfungen auf allen Firmengeräten notwendig. Außerdem müssen Organisationen unter Umständen ganze Richtlinien anpassen, um sich besser vor zukünftigen Angriffen zu schützen.

Die Endpoint und Server Sicherheitslösungen arbeiten unter anderem mit Daten, die anonymisiert von Endpoints auf der ganzen Welt eingereicht werden. So können selbst neueste Bedrohungen erkannt werden – noch bevor sie sich weltweit verbreiten. Dank cloudbasierter Aktualisierungen stehen die Informationen noch vor dem regulären Update der Erkennungsroutine bereit.

SPAM UND PHISHING

Im Idealfall gehen Mitarbeiter einer Organisation ihrer Arbeit nach, ohne sich mit dem Aussortieren von Spam-Mails beschäftigen zu müssen. Tatsächlich sind aber mehr als die Hälfte aller eingehenden Nachrichten Spam. Müssten Nutzer all diese E-Mails eigenständig prüfen, wären sie nur schwerlich effektiv.

ESET Mail Security verhindert, dass schädliche Nachrichten in Mitarbeiter-Postfächern landen. Unsere Sicherheitslösung entscheidet zuverlässig, ob es sich bei einer E-Mail um Spam bzw. Phishing handelt oder nicht. Damit wird die Sicherheit Ihrer Organisation gestärkt und gleichzeitig die Effektivität der Mitarbeiter gesteigert.

ESET Endpoint Security filtert effektiv Spam und scannt alle eingehenden E-Mails auf Malware.

Die 3 Säulen **unserer Technologie**

ESET LIVEGRID®

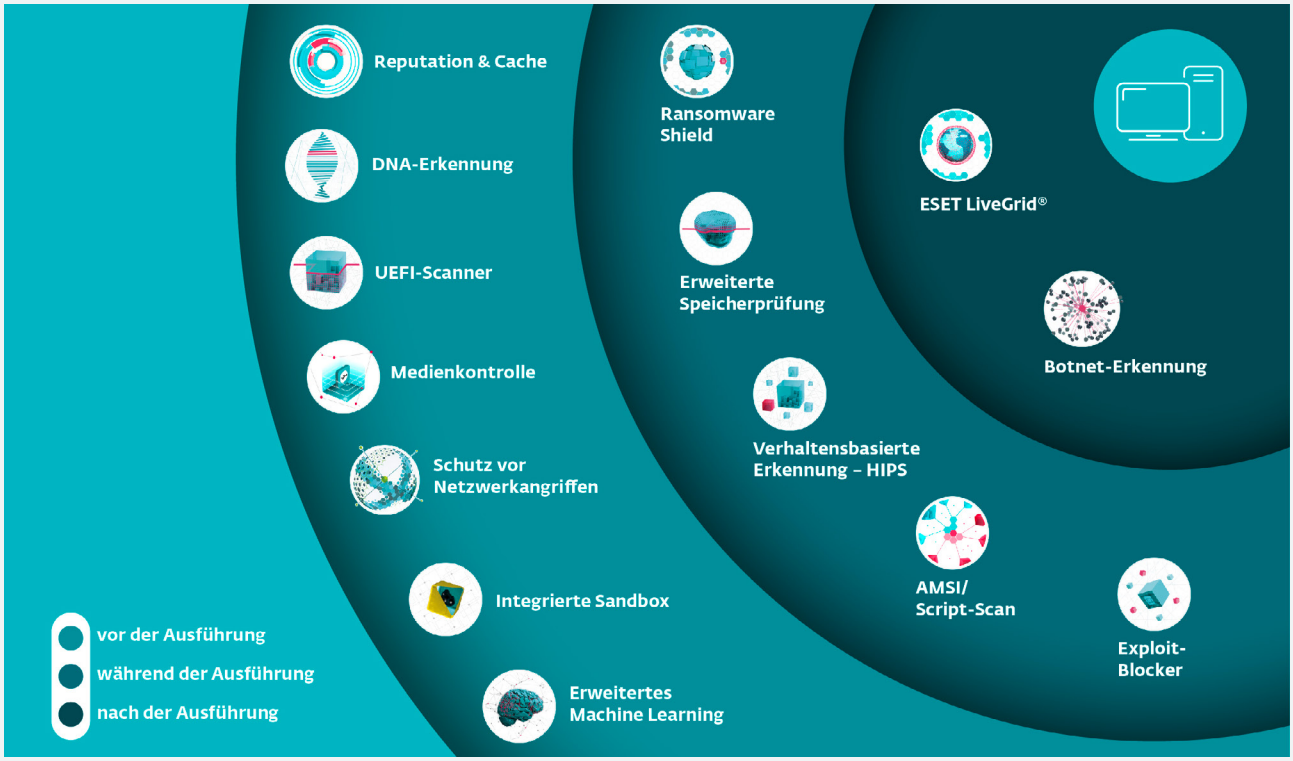
Wird eine Zero-Day-Bedrohung erkannt, wird die Datei zur Verhaltensanalyse an ESET LiveGrid® gesendet, wenn Ihr Einverständnis zur Teilnahme gegeben wurde. Das Ergebnis der Prüfung wird innerhalb weniger Minuten auf allen Endpoints weltweit eingespielt, ohne dass ein Update notwendig ist.

MACHINE LEARNING

Die eigens von ESET entwickelte Machine Learning Engine „Augur" nutzt eine Kombination aus neuronalen Netzen und ausgewählten Klassifizierungsalgorithmen zur zuverlässigen Einstufung von Samples als sicher, potenziell unerwünscht oder schädlich.

MENSCHLICHES KNOW-HOW

Dank dem umfassenden Wissen und der langjährigen Erfahrung unserer Sicherheitsexperten sind Sie stets umfassend geschützt.

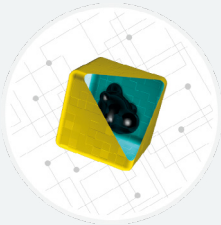


Alle ESET Sicherheitslösungen identifizieren Malware vor, während und nach der Ausführung. Diese ganzheitliche Absicherung durch unsere mehrschichtigen Schutzmechanismen ermöglicht Ihnen den optimalen Schutz für Geräte und Daten.

Unsere eingesetzten **Schutzmodule**

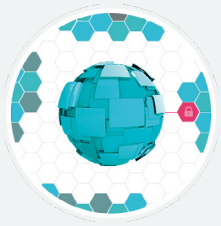
MACHINE LEARNING

Bereits seit 1997 ist Machine Learning (ML) integraler Bestandteil unserer Sicherheitslösungen. Aktuell ist unsere ML-Engine „Augur" in all unseren Sicherheitslösungen enthalten. ML-Algorithmen kommen in Form von konsolidiertem Output und neuronalen Netzen zum Einsatz.



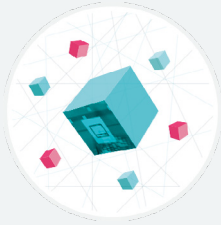
INTEGRIERTE SANDBOX

Malware ist heute oft darauf optimiert, so lange wie möglich im Verborgenen zu agieren. Unsere integrierte Sandbox bildet verschiedene Hardware- und Softwarekomponenten in einer isolierten Umgebung nach. So wird bösartiges Verhalten erkannt, noch bevor es im Netzwerk sichtbar wird.



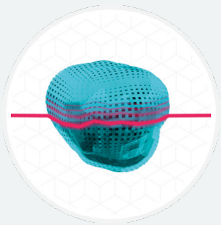
RANSOMWARE SHIELD

Das ESET Ransomware Shield schützt Nutzer umfassend vor allen Arten von Ransomware. Die Technologie überprüft alle ausgeführten Anwendungen und bewertet sie anhand ihres Verhaltens und ihrer Reputation. Prozesse, die typisches Ransomware-Verhalten aufweisen, werden umgehend blockiert.



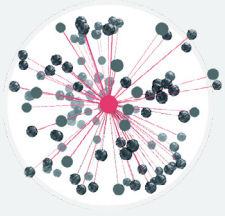
EXPLOIT-BLOCKER

Der Exploit-Blocker beobachtet konstant das Verhalten häufig angegriffener Anwendungen wie Webbrowser, PDF-Reader, E-Mail-Programme, Flash oder Java. Anstatt sich nur auf bestimmte CVE-Kennungen zu beschränken, werden gängige Ausnutzungstechniken berücksichtigt. Wird eine Bedrohung erkannt, wird die entsprechende Anwendung umgehend blockiert.



ERWEITERTE SPEICHERPRÜFUNG

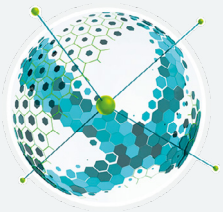
Die Erweiterte Speicherprüfung wehrt getarnte Bedrohungen ab, indem sie verdächtige Prozesse erkennt und blockiert, sobald sie im Arbeitsspeicher ihre schädlichen Funktionen zur Ausführung bereitstellen. Das ermöglicht eine Erkennung dateiloser Malware, die keine dauerhafte Komponente im Dateisystem benötigt und deshalb nicht durch klassische Methoden entdeckt wird.



BOTNET-ERKENNUNG

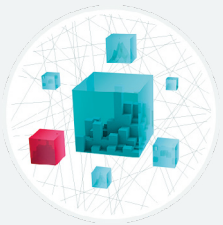
Die ESET Sicherheitslösungen erkennen schädliche Kommunikationen, die für Botnets typisch sind, und identifizieren zugleich die angreifenden Prozesse. Jede erkannte schädliche Kommunikation wird blockiert und dem Nutzer gemeldet.

WICHTIGER HINWEIS: Integrierte Technologien sind teilweise produktspezifisch.



SCHUTZ VOR NETZWERKANGRIFFEN

Die ESET Sicherheitslösungen nehmen bereits auf Netzwerkebene Prüfungen vor. Das stärkt den Schutz vor Malware und verhindert über das Netzwerk ausgeführte Angriffe sowie Ausnutzungsversuche von Schwachstellen, für die noch kein Patch bereitgestellt wurde.



VERHALTENSBASIERTE ERKENNUNG – HIPS

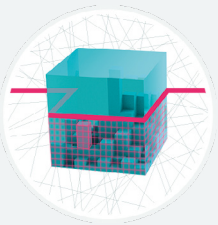
Das Host-based Intrusion Prevention System (HIPS) von ESET beobachtet die Systemaktivitäten und erkennt verdächtiges Systemverhalten anhand vordefinierter Regeln. Werden solche Aktivitäten identifiziert, verhindert der Selbstschutzmechanismus des Moduls die Ausführung der entsprechenden Programme oder Prozesse.

SECURE BROWSER

Dient der Absicherung von Unternehmensressourcen dank einer speziellen Schutzschicht. Diese konzentriert sich auf den Zugriff kritischer Daten innerhalb des Intranet und der Cloud durch den verwendeten Browser. Secure Browser bietet einen erweiterten Speicherschutz für den Browser-Prozess, und ermöglicht es Administratoren, weitere URLs hinzuzufügen, die geschützt werden sollen.

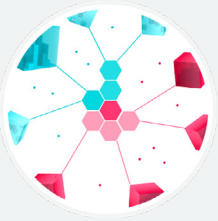
DNA-ERKENNUNGEN

Die ESET Scan Engine erkennt schädliche Objekte anhand verschiedener Kriterien – anhand des eindeutigen „Fingerabdrucks“ (Hash) oder sogenannter DNA Erkennungen, die auf komplexen Definitionen von Verhaltensmustern und anderen Malware-Charakteristika basieren.



UEFI-SCANNER

ESET ist der erste IT-Security-Anbieter, der einen Mechanismus zum Schutz des Unified Extensible Firmware Interface (UEFI) implementiert hat. Der UEFI-Scanner prüft Systeme mit UEFI-Bootumgebung noch vor dem Start des Betriebssystems und gewährleistet dadurch die Sicherheit und Integrität der Firmware. Bei Auffälligkeiten wird der Nutzer umgehend informiert.



AMSI/SCRIPT-SCAN

Die ESET Sicherheitslösungen verwenden AMSI (Antimalware Scan Interface) für noch besseren Schutz von Nutzern, Daten und Anwendungen. Zusätzlich nutzen sie das in Windows integrierte Sicherheitsmodul, durch das nur vertrauenswürdiger, signierter Code ausgeführt und Code Injection-Angriffe verhindert werden.

WICHTIGER HINWEIS: Integrierte Technologien sind teilweise produktspezifisch.

ESET **bietet einfach mehr**

MEHRSCHICHTIGER SCHUTZ

Mit der Kombination aus mehrschichtiger Technologie, Machine Learning und menschlichem Know-how genießen unsere Kunden optimalen Schutz. Dank regelmäßiger Optimierungen gewährleisten unsere Technologien stets den perfekten Mix aus maximaler Erkennung und Performance – bei minimalen Fehlalarmen.

CLOUDBASIERTE SICHERHEIT

Wird eine Zero-Day-Bedrohung wie z.B. Ransomware erkannt, wird die Datei zur Verhaltensanalyse an unser cloudbasiertes Reputationssystem ESET LiveGrid® gesendet, wenn Ihr Einverständnis zur Teilnahme gegeben wurde. Das Ergebnis der Prüfung wird innerhalb weniger Minuten auf allen Endpoints weltweit eingespielt, ohne dass ein Update notwendig ist. Mit der ergänzenden Sicherheitslösung ESET Dynamic Threat Defense bieten wir darüber hinaus zusätzlichen Schutz in Form von Cloud-Sandboxing.

VERTRAUEN UND STABILITÄT

ESET ist seit über 30 Jahren als Hersteller von Sicherheitslösungen am Markt und schützt betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach getesteten sowie ausgezeichneten mehrschichtigen Technologie vor Bedrohungen aller Art. Unsere Produkte haben sich bewährt und schützen mittlerweile über 110 Millionen Nutzer weltweit. Zudem schützen wir mit den ESET Technologien über eine Milliarde Menschen bei der täglichen Nutzung ihrer Internetbrowser.

EINZIGARTIGE PERFORMANCE

Die Befürchtung vieler Unternehmen, dass sich eine Sicherheitslösung negativ auf die Systemleistung auswirkt, ist unbegründet. Alle ESET Sicherheitslösungen zeichnen sich durch minimalen Ressourcenbedarf aus. Das bestätigen auch immer wieder Tests von unabhängigen Drittanbietern.

WELTWEIT FÜR SIE DA

ESET verfügt über ein globales Netzwerk an Niederlassungen sowie Forschungs- und Entwicklungszentren, die Produkte sind in mehr als 200 Ländern und Regionen verfügbar. So können wir frühzeitig auf Bedrohungen reagieren und Abwehrmechanismen gegen neuartige Malware-Trends entwickeln.

ESET Endpoint Sicherheitslösungen

ESET Endpoint Security for Windows/macOS/Android

ESET Endpoint Antivirus for Windows/macOS/Linux

ESET Endpoint Sicherheitslösungen
Technische Features

MALWARE-SCHUTZ

Schützt Endpoints vor Gefahren aller Art. Für eine bessere Erkennungsleistung und schnellere Prüfungen werden bekannte Dateien in einer cloudbasierten Reputationsdatenbank auf eine Black- oder Whitelist gesetzt. Hierbei werden lediglich anonymisierte Metadaten über ausführbare Dateien und Archive an diese Datenbank übermittelt.

WEB-KONTROLLE*

Anhand von vordefinierten Kategorien wie „Gaming“, „Soziale Netzwerke“ oder „Shopping“ lassen sich Zugriffe auf Webseiten einfach beschränken. 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.

CLIENT ANTI-SPAM*

Filtert effektiv Spam und scannt alle eingehenden E-Mails auf Malware. Native Unterstützung für Microsoft Outlook (POP3, IMAP, MAPI).

PLATTFORM-ÜBERGREIFENDE UNTERSTÜTZUNG

Die ESET Endpoint Sicherheitslösungen unterstützen alle gängigen Betriebssysteme, einschließlich Windows, macOS, Linux und Android. Über eine Web-Konsole lassen sich alle Produkte bequem zentral verwalten. Zudem unterstützt das Tool das komplette Mobile Device Management (MDM) von Android- und iOS-Geräten.

ZWEI-WEGE- FIREWALL*

Schützt Ihr Unternehmensnetzwerk vor unautorisierten Zugriffen und Datendiebstahl. Legen Sie vertrauenswürdige Netzwerke fest und aktivieren Sie für alle anderen Verbindungen wie öffentliche Hotspots eine restriktivere Konfiguration.

MEDIENKONTROLLE

Erlaubt dem Admin, Medien wie CDs/DVDs und USBs gezielt zu blockieren. Für Nutzergruppen lassen sich simpel 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.

GERINGE SYSTEMBELASTUNG

ESET Endpoint Sicherheitslösungen bieten bewährten Schutz und schonen dabei Systemressourcen. Durch den geringen Ressourcenbedarf der Produkte können auch ältere Systeme einfach weiter genutzt werden.

MULTIPLE LOGFORMATE

Lässt Sie Logs in gängigen Formaten speichern – CSV, Textdatei oder Windows Ereignisprotokoll. Die Logs werden außerdem zur Weiterverarbeitung, z.B. per externem SIEM Tool, am Endpoint gespeichert.

* gilt ausschließlich für ESET Endpoint Security

ESET Endpoint Sicherheitslösungen profitieren von proaktiven und intelligenten Technologien, die optimal ineinander greifen und so den perfekten Mix aus maximaler Erkennung und Performance bei minimalen Fehlalarmen gewährleisten.

ESET Server Sicherheitslösungen

ESET Server Security

- ESET Server Security for Microsoft Windows Server
- ESET Server Security for Linux

ESET Server Sicherheitslösungen
Technische Features

MALWARE-SCHUTZ FÜR SERVER

Bietet Echtzeit-Scan sämtlicher servergespeicherten Daten. Der Selbstschutz verhindert die Deaktivierung der Software durch Malware und unberechtigte Zugriffe. Die fortschrittliche LiveGrid®-Technologie von ESET vereint Geschwindigkeit, Präzision und geringste Systembelastung.

PLATTFORM-ÜBERGREIFENDER SCHUTZ

ESET Server Security unterstützt gängige Betriebssysteme und Plattformen, z.B. Windows Server, Microsoft 365, OneDrive, Linux und Microsoft Azure. Dadurch wird die Ausbreitung von Malware von einem Betriebssystem auf ein anderes verhindert. Über eine Web-Konsole lassen sich alle Produkte bequem zentral verwalten.

REIBUNGSLOSER SYSTEMBETRIEB

ESET Server Security identifiziert Nutzerkonten bei Zugriffsversuchen und schützt per Passwort vor Deinstallation. Erkennt automatisch Serverrollen und schließt kritische Serverdateien wie Datenbanken und Paging-Files vom On-Access-Scan aus, was die Systemlast erheblich verringert.

CLUSTER SUPPORT

ESET Server Sicherheitslösungen bieten die Möglichkeit, mehrere Produkte in einem Cluster miteinander zu verbinden und zu verwalten. So lassen sich Konfigurationen, Benachrichtigungen, Greylisting-Datenbanken usw. austauschen. Zudem werden Windows Failover Cluster und Network Load Balancing Cluster unterstützt.

GERINGE SYSTEMBELASTUNG

Schont Systemressourcen und lässt mehr Kapazitäten für die eigentlichen Serveraufgaben.

ESET Server Security bietet einen erweiterten Schutz für alle allgemeinen Server, Netzwerk-Dateispeicher und Mehrzweck-Server. Besonderes Augenmerk liegt dabei darauf, dass die Server stabil und konfliktfrei sind, um Wartungen auf ein Minimum zu beschränken und die Geschäftskontinuität sicherzustellen.

ESET Mail Sicherheitslösungen

ESET Mail Security

- ESET Mail Security for Microsoft Exchange Server
- ESET Mail Security for IBM Domino

ESET Mail Security Sicherheitslösungen
Technische Features

ANTI-SPAM

Unsere inhouse entwickelte, mehrfach ausgezeichnete Engine stoppt Spam-Nachrichten noch bevor sie den Nutzer erreichen. Verhindert zudem Backscatter-Mails und bietet SMTP-Schutz sowie SPF- und DKIM-Validierung.

ANTI-MALWARE

Der zweite Schutzmechanismus der ESET Mail Security schützt Ihre Nutzer vor verdächtigen oder schädlichen E-Mail-Anhängen.

CLUSTER SUPPORT

ESET Server Sicherheitslösungen bieten die Möglichkeit, mehrere Produkte in einem Cluster miteinander zu verbinden und zu verwalten. So lassen sich Konfigurationen, Benachrichtigungen, Greylisting-Datenbanken usw. austauschen. Zudem werden Windows Failover Cluster und Network Load Balancing Cluster unterstützt.

ANTI-PHISHING

Verhindert das Öffnen von Phishing-Seiten, indem E-Mail-Inhalte und die Betreffzeile auf URLs geprüft werden. Erkannte URLs werden mit einer Datenbank abgeglichen und entsprechend der Bewertungsregeln als schädlich oder harmlos eingestuft.

PRÜFUNG VON HYBRIDEN MICROSOFT 365 UMGEBUNGEN

Unterstützt Unternehmen, die Microsoft Exchange in hybriden Umgebungen verwenden.

GESCHWINDIGKEIT

Sicherheitslösungen für Mailserver müssen vor allem zwei Anforderungen erfüllen: Leistungsfähigkeit und Stabilität. Unternehmen sind auf eine störungsfreie Verarbeitung ihrer E-Mails angewiesen. ESET stellt ein 64-Bit-Produkt bereit, das dank Clustering in Unternehmen jeder Größe eine optimale Performance gewährleistet.

REGELN

Über das einfach zu verstehende Regelsystem können Administratoren die Bedingungen für den E-Mail-Filter und die durchzuführenden Aktionen manuell definieren.

QUARANTÄNE-MANAGEMENT

Nutzer erhalten automatisch Benachrichtigungen über Spam-Mails, die in Quarantäne verschoben wurden und können diese Nachrichten eigenständig verwalten und Folgeschritte einleiten.

CLOUD-SANDBOXING SUPPORT FÜR EXCHANGE

Steigern Sie zusätzlich das Schutzniveau Ihrer Exchange Server durch unser cloudbasierte Sandbox, die neue und bisher unbekannte Bedrohungen (bspw. Zero-Days, Ransomware) analysiert. Diese Erweiterung bedarf einer eigenen Lizenz.

ESET Mail Security bietet eine zusätzliche Sicherheitsschicht für Organisationen, die den Host selbst schützen und so verhindern möchten, dass Bedrohungen jemals die Posteingänge ihrer Nutzer erreichen.

ESET SharePoint Sicherheitslösung

ESET Security for Microsoft SharePoint Server

ESET SharePoint Sicherheitslösung
Technische Features

PERFORMANCE

ESET Security for Microsoft SharePoint basiert auf einem 64-Bit-Kern und enthält DLL-Module, die den RAM Speicher effizienter verwenden, schnellere Startzeiten der Endgeräte garantieren und ermöglichen, dass zukünftige Windows-Updates nativ unterstützt werden.

DIREKTER DATENBANKZUGRIFF

Bei Bedarf können Dateien direkt vom Datenbankserver geladen und so das SharePoint-Objektmodell umgangen werden. Die Performance wird dadurch nachhaltig verbessert.

CLUSTER SUPPORT

ESET Server Sicherheitslösungen bieten die Möglichkeit, mehrere Produkte in einem Cluster miteinander zu verbinden und zu verwalten. So lassen sich Konfigurationen, Benachrichtigungen, Greylisting-Datenbanken usw. austauschen. Zudem werden Windows Failover Cluster und Network Load Balancing Cluster unterstützt.

ESET Security for Microsoft SharePoint Server bietet höchsten Schutz vor schädlichen Uploads und unerwünschten Dateien. Dabei laufen die Server stabil und konfliktfrei weiter.

Lösungen für Endpoints und Server
So funktioniert‘s

RANSOMWARE

Ransomware ist für viele Unternehmen eine ernstzunehmende Bedrohung, vor der sie sich besonders gut schützen möchten.

Lösung

- ✓ Der Schutz vor Netzwerkangriffen blockiert Exploits bereits auf Netzwerkebene und verhindert dadurch eine Infizierung der Systeme mit Ransomware.
- ✓ Alle ESET Sicherheitslösungen verfügen über eine integrierte Sandbox, die selbst gut getarnte Malware anhand ihres Verhaltens identifiziert.
- ✓ Das Ransomware Shield ist Bestandteil aller ESET Sicherheitslösungen und schützt Nutzer zuverlässig vor Verschlüsselungstrojanern.

ZERO-DAYS

Zero-Day-Angriffe sind für Unternehmen besonders besorgniserregend, da es schwierig ist, sich vor noch unbekannten Gefahren zu schützen.

Lösung

- ✓ Mithilfe von Heuristiken und Machine Learning sind die ESET Sicherheitslösungen in der Lage, auch bislang unbekannte Gefahren zu identifzieren.
- ✓ Dank unserer 13 Forschungs- und Entwicklungszentren weltweit können wir schnell auf aufkommende Bedrohungen reagieren.
- ✓ Dank dem cloudbasierten Schutz vor Malware sind Nutzer umgehend vor neuartigen Bedrohungen geschützt, ohne auf das nächste Update der Erkennungsroutine warten zu müssen.

DATEILOSE ANGRIFFE

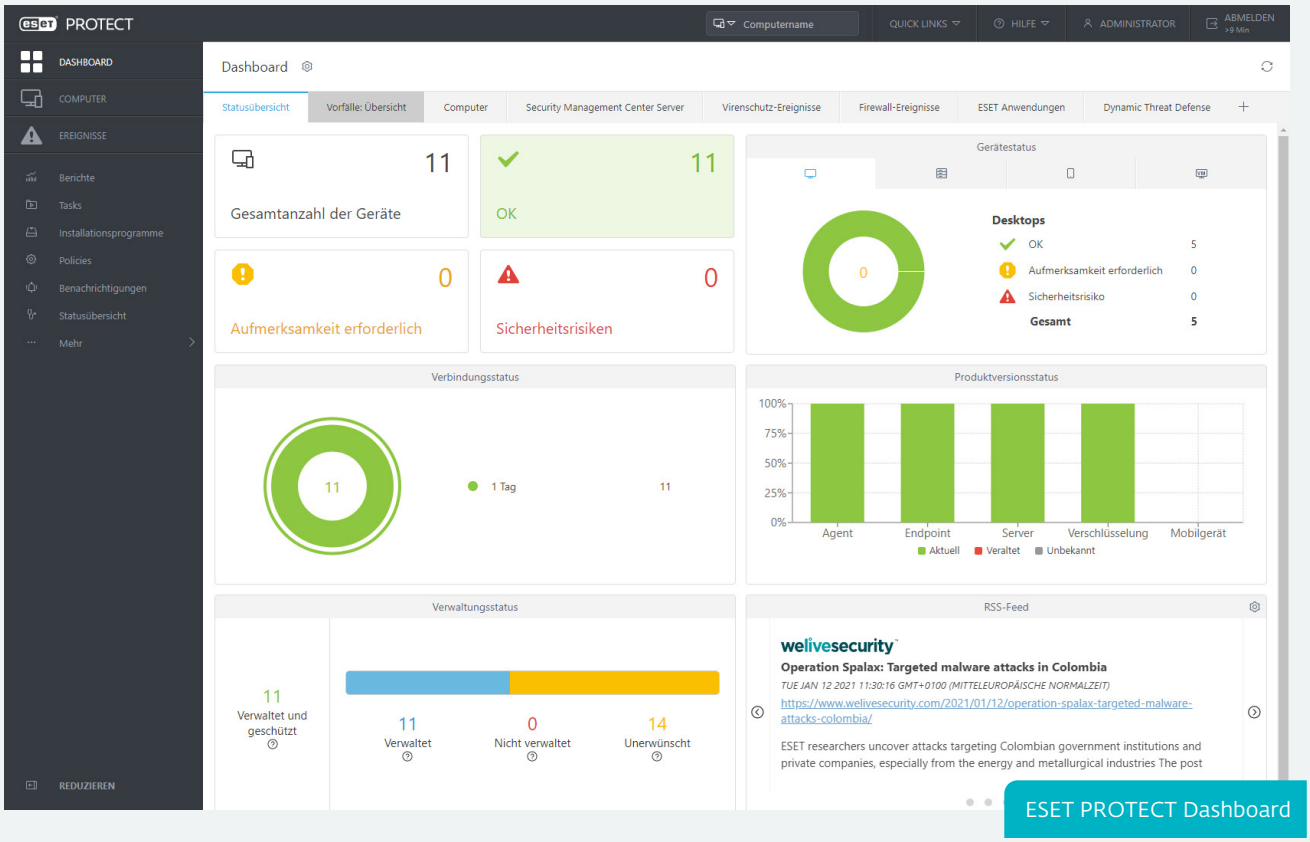
Dateilose Malware ist verhältnismäßig neu und wird nur im Arbeitsspeicher ausgeführt. So entgeht sie einer Erkennung durch herkömmliche Methoden.

Lösung

- ✓ Die Erweiterte Speicherprüfung erkennt und blockiert Schadsoftware, sobald sie im Arbeitsspeicher aktiv wird.
- ✓ Zur Klärung, ob eine potenzielle Bedrohung vorliegt, gibt es die Möglichkeit, ein Sample in die Cloud-Sandbox ESET Dynamic Threat Defense hochzuladen. Das Verhalten der Malware wird beobachtet, dokumentiert und automatisch analysiert.
- ✓ Mit der Kombination aus mehrschichtiger Technologie, Machine Learning und menschlichem Know-how genießen unsere Kunden optimalen Schutz.

ESET PROTECT

Die Management-Konsole ESET PROTECT bietet einen kompletten Überblick über alle Endpoints in Echtzeit innerhalb und außerhalb Ihrer Organisation und gewährleistet so ein vollständiges Security Management sowie umfassendes Reporting für alle gängigen Betriebssysteme. Behalten Sie die Übersicht über alle ESET Lösungen ohne räumliche Grenzen und die volle Kontrolle über Ihre IT-Sicherheit von der Vermeidung und Erkennung potenzieller Gefahren bis hin zur Reaktion auf Vorfälle über alle Plattformen hinweg – ob Desktops, Server oder Mobilgeräte. ESET PROTECT steht sowohl cloudbasiert als auch On-Premises zur Verfügung.



ESET PROTECT Dashboard

Über ESET

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

Unsere Endpoint Detection and Response Lösungen und Frühwarnsysteme wie Threat Intelligence Services ergänzen das Angebot im Hinblick auf Forensik sowie gezieltem Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Repudationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ZUFRIEDENE KUNDEN

BVB 09 Champion Partner

Seit 2019 ein starkes Team
auf dem Feld und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

T

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Security made in EU
Trust Seal www.teletrust.de/itsmie

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

CERTIFIED ISO 9001:2015 COMPANY
CERTIFIED ISO 27001:2013 COMPANY

Unsere Lösungen sind nach
Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Nutzer weltweit

400k+
Business-Kunden

200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

welivesecurity by ESET

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH