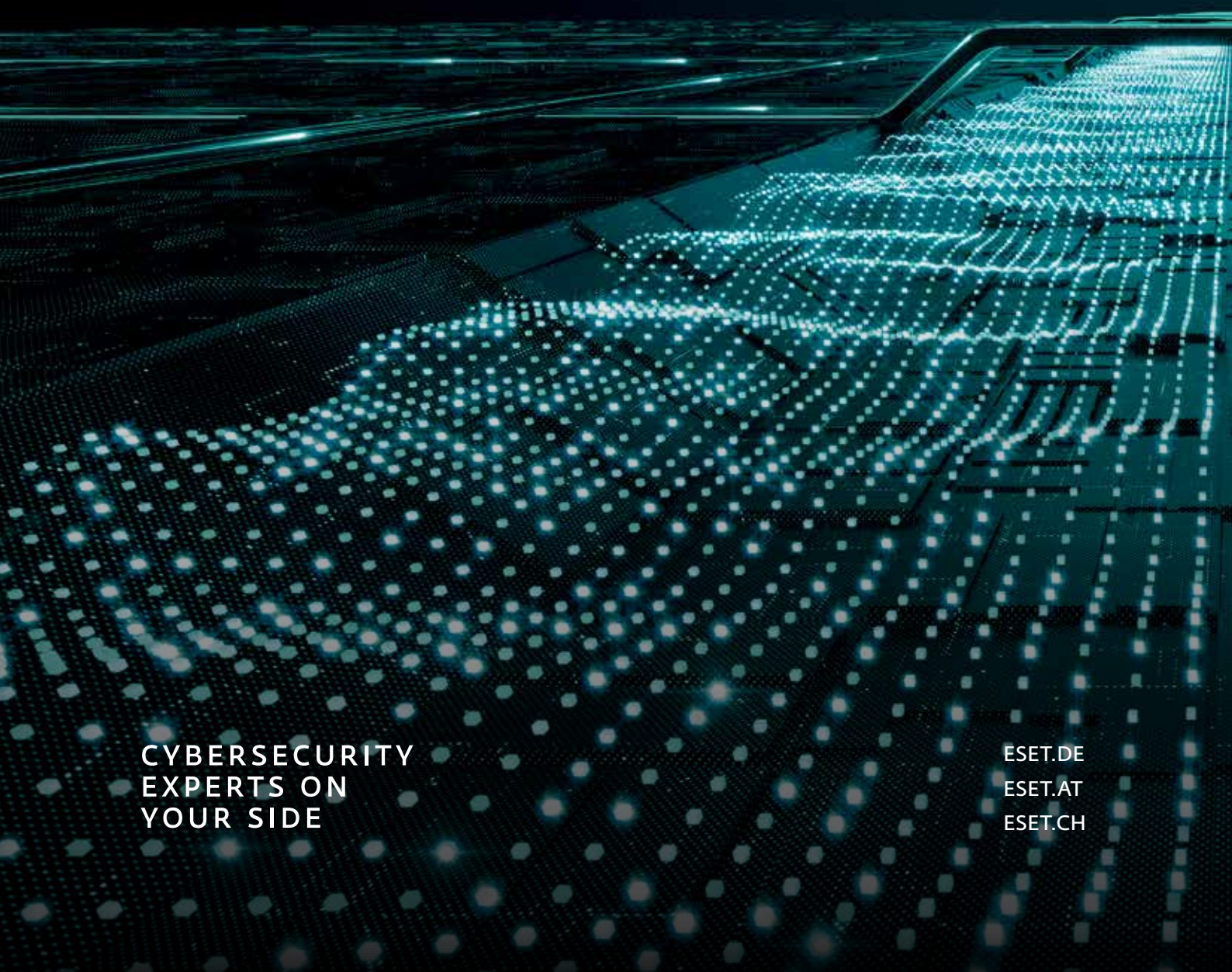
PRODUKTÜBERSICHT

SECURITY
FOR MICROSOFT SHAREPOINT SERVER

Zuverlässiger Schutz für Microsoft SharePoint Server



CYBERSECURITY
EXPERTS ON
YOUR SIDE

ESET.DE
ESET.AT
ESET.CH

Was macht eigentlich eine **Sicherheitslösung für SharePoint?**

Viele Unternehmen setzen aktuell auf SharePoint Server, um die Zusammenarbeit zu erleichtern. Dabei stellen Server, auf denen einzelne Nutzer prinzipiell jede Datei speichern können, ein potenzielles Sicherheitsrisiko für das gesamte Unternehmen dar. Mit einer Security-Lösung für SharePoint schützen Sie unternehmensweit genutzte Server vor Bedrohungen aller Art.

ESET Security für Microsoft Sharepoint bietet höchsten Schutz vor schädlichen Uploads und erwünschten Dateien. Dabei laufen die Server stabil und konfliktfrei weiter, Pop-Ups und Neustarts sind selten. Der Geschäftsbetrieb wird nicht beeinträchtigt.

Drei **gute Gründe**

RANSOMWARE

Spätestens seit Cryptolocker im Jahr 2013 stellt Ransomware eine reale Gefahr für Industrienetzwerke auf der ganzen Welt dar. Dabei ist das Konzept natürlich schon viel länger bekannt. Bisher erschien die Bedrohung jedoch nicht so groß, dass sich Unternehmen ernsthaft mit der Situation auseinandergesetzt hätten. Das hat sich inzwischen geändert: Das Bewusstsein dafür, dass schon ein einziger Ransomware-Angriff durch die Verschlüsselung wichtiger Dateien das gesamte Unternehmen lahmlegen kann, ist stark gestiegen. Betrifft Ransomware Unternehmensgeräte, wird oft schnell klar, dass die Wiederherstellung der Daten teuer und teilweise unmöglich ist. Die Zahlung des Lösegeldes erscheint unvermeidbar.

Gerade zentrale SharePoint-Server, auf die Nutzer mehr oder weniger unkontrolliert Daten hochladen können, sind dabei besonders gefährdet. ESET SharePoint Security verhindert nicht nur, dass Ransomware ins Unternehmen eindringt. Sie entdeckt sogar Ransomware, die sich bereits seit Längerem auf dem Server verborgen hält.

GEZIELTE ANGRIFFE UND DATENLECKS

Die Gefahrenlandschaft im IT-Sektor entwickelt sich ständig weiter. Täglich kommen neue Angriffsmethoden und bisher unbekannte Bedrohungen hinzu. Sind Unternehmen von einem Angriff betroffen, sind sie oft überrascht, dass ihre Abwehr scheinbar mühelos durchbrochen werden konnte. Wird der Angriff schließlich entdeckt, werden Prozesse implementiert, um ähnliche Vorfälle in Zukunft zu vermeiden. Es ist jedoch sehr unwahrscheinlich, dass der nächste Angriff auf genau demselben Weg erfolgt. Die Schutzwirkung der neuen Prozesse ist minimal.

ESET SharePoint Security arbeitet mit weltweit gesammelten Daten zur aktuellen Bedrohungslage und kann so selbst neueste Malware erkennen – noch bevor sie sich verbreitet. Vor allem Server sind beliebtes Ziel von Angreifern, liegen hier doch häufig Daten, die sich gewinnbringend weiterverkaufen lassen. Um Server auch gegenüber solchen häufigen und gezielten Angriffen abzusichern, wird ESET SharePoint Security laufend über die Cloud aktualisiert – ohne auf reguläre Updates warten zu müssen.

DATEILOSE ANGRIFFE

Ein neuartige Malware-Form, sogenannte dateilose Malware, wird nur im Arbeitsspeicher ausgeführt. Abwehrlösungen, die allein auf der Analyse von Dateien basieren, sind nicht in der Lage, diese zu erkennen. Einige dateilose Attacken kapern zudem auf dem Betriebssystem installierte Anwendungen und sind so noch besser getarnt. Typisches Beispiel ist der Missbrauch von PowerShell für Attacken.

ESET SharePoint Security erkennt manipulierte oder gekaperte Anwendungen und kann so selbst gut getarnte Malware identifizieren. Zusätzlich nutzt es Technologien, die den Arbeitsspeicher laufend auf verdächtige Vorgänge scannen.

ESET SharePoint Security erkennt auch solche Ransomware, die sich seit Längerem im Unternehmensnetzwerk verborgen hält.

Ransomware ist vor allem für zentrale SharePoint-Server, auf die Nutzer Daten hochladen können, eine ernstzunehmende Gefahr.

„Dateilose" Malware wird nur im Arbeitsspeicher ausgeführt. Abwehrlösungen, die allein auf der Analyse von Dateien basieren, können diese nicht erkennen.

„Wir vertrauen seit vielen Jahren auf den ESET Schutz. Die Lösungen tun ganz einfach, was sie tun sollen. ESET steht für uns vor allem für drei Dinge: Zuverlässigkeit, Qualität und Service."

—Jos Savelkoul, Leiter IT-Abteilung; Zuyderland Hospital, Niederlande; 10.000+ Seats

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.

EINZIGARTIGE PERFORMANCE

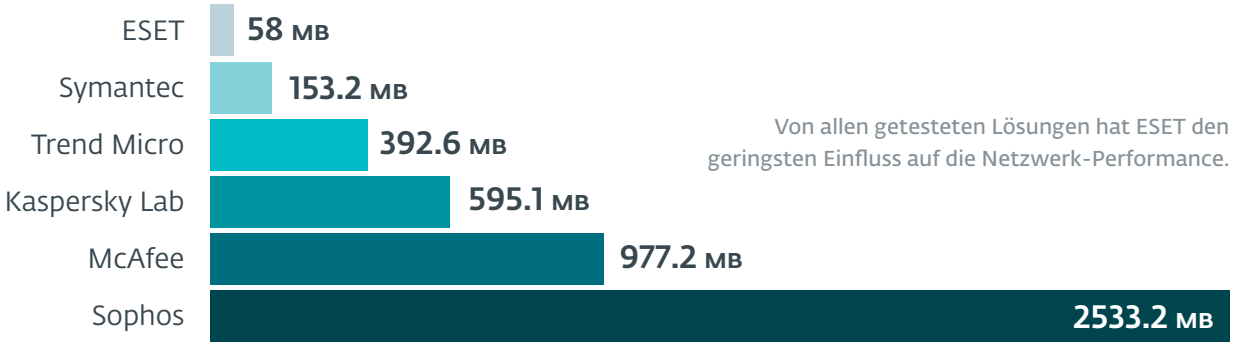
Die Befürchtung vieler Unternehmen, dass sich eine Sicherheitslösung negativ auf die Systemleistung auswirkt, ist unbegründet. Alle ESET Produkte zeichnen sich durch minimalen Ressourcenbedarf aus. Das bestätigen auch immer wieder Tests von unabhängigen Drittanbietern.

DIREKTER DATENBANKZUGRIFF

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

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 akute Bedrohungen reagieren und Abwehrmechanismen gegen neuartige Malware-Trends entwickeln.



Von allen getesteten Lösungen hat ESET den geringsten Einfluss auf die Netzwerk-Performance.

Quelle: AV-Comparatives: Network Performance Test, Business Security Software

„Seit wir ESET im Einsatz haben, hat unser Helpdesk nichts mehr zu tun – zumindest nicht, wenn es um Virus- oder Malware-Probleme geht."

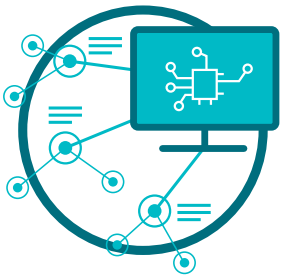
— Adam Hoffman, Manager IT-Infrastruktur; Mercury Engineering, Irland; 1.300 Seats

Die Technologie

Unsere Produkte und Technologien stehen auf 3 Säulen

ESET LIVEGRID®

Wird eine Zero-Day Bedrohung wie z.B. Ransomware erkannt, wird die Datei zur Verhaltensanalyse an unser Cloudsystem LiveGrid® gesendet. 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.

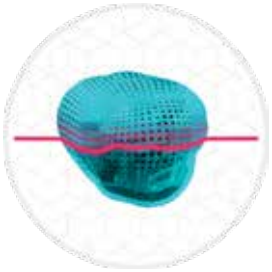
MENSCHLICHES KNOW-HOW

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

Ein einzelner Verteidigungsmechanimus reicht angesichts der komplexen Bedrohungslage bei weitem nicht aus. Deshalb sind alle ESET Endpoint Produkte in der Lage, Malware vor, während und nach der Ausführung zu erkennen.

MACHINE LEARNING

Bereits seit 1997 ist Machine Learning integraler Bestandteil unserer Sicherheitslösungen. Aktuell ist unsere ML-Engine „Augur" in allen unseren Produkten enthalten und sorgt zusammen mit allen anderen ESET Technologien für höchsten Schutz. ML-Algorithmen kommen in Form von konsoldiertem Output und neuronalen Netzen zum Einsatz.



TIEFENSCAN

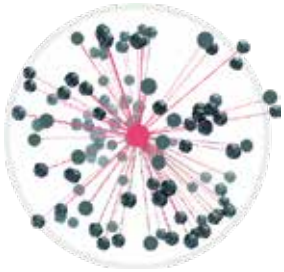
ESET überwacht das Verhalten potentiell schädlicher Anwendungen und erkennt gefährliches Verhalten sofort, sobald es sich im Arbeitsspeicher zeigt. Dateilose Malware kommt ohne persistente Komponenten auf dem Rechner aus und kann so nicht mit konventionellen Methoden entdeckt werden. Nur ein Scan des Arbeitsspeichers kann derartige Malware erkennen und unschädlich machen.

RANSOMWARE SHIELD

ESET Ransomware Shield schützt Nutzer umfassend vor allen Arten von Ransomware. Diese Schutzschicht überwacht und analysiert Anwendungen und kategorisiert sie entsprechend ihres Verhaltens und ihrer Reputation. So werden Prozesse blockiert, die für Ransomware typisches Verhalten zeigen.

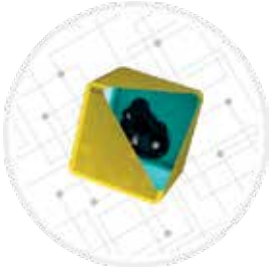
EXPLOIT BLOCKER

ESETs Exploit Blocker überwacht typische Ziele für Exploit-Attacken (Browser, PDF-Reader, E-Mail-Clients, Flash, Java etc.). Dabei wird insbesondere auch das Verhalten von Anwendungen beobachtet, nicht bloß CVE-Kennungen abgeglichen. Wird eine Gefahr erkannt, wird die Anwendung sofort blockiert.



BOTNET-SCHUTZ

ESET Produkte erkennen Kommunikationsmuster, die auf den Missbrauch des Rechners durch Botnets hindeuten und können dann die verursachenden Prozesse identifizieren. Jede verdächtige Kommunikation wird geblockt und dem Nutzer gemeldet.



INTEGRIERTE SANDBOX

Malware ist heute vielfach darauf optimiert, so lange wie möglich im Verborgenen zu agieren. Unsere integrierte Sandbox erkennt das verborgene, bösartige Verhalten schon bevor es im Netzwerk sichtbar wird. Die ESET Produkte können hiermit verschiedene Hard- und Software-Komponenten nachahmen und das verdächtige Sample in einer isolierten virtuellen Umgebung ausführen.

DNA-KENNUNGEN

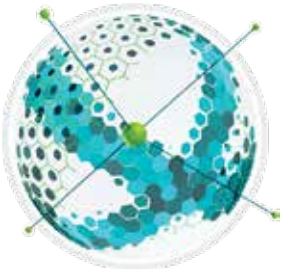
Die Erkennung basiert auf ganz konkreten Hashes sowie den ESET DNA-Kennungen – umfangreiche Definitionen verdächtigen Verhaltens und von Malware-Eigenschaften. Angreifer sind mittlerweile sehr gut darin, Schadcode zu modifizieren oder eine Entdeckung durch andere Methoden für lange Zeit zu verhindern. Was sie jedoch nicht ändern können, ist das Verhalten von Objekten. Genau dies macht sich die ESET DNA-Erkennung zunutze und erkennt Schadsoftware anhand ihres Verhaltens.

AMSI/SCRIPT-SCAN

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

VERHALTENSBASIERTE ERKENNUNG – HIPS

ESETs Host Based Intrusion Prevention System überwacht die Systemvorgänge und erkennt verdächtiges Verhalten anhand im Voraus festgelegter Regeln. Der integrierte Abwehrmechanismus verhindert zudem, dass der verdächtige Prozess ausgeführt wird.

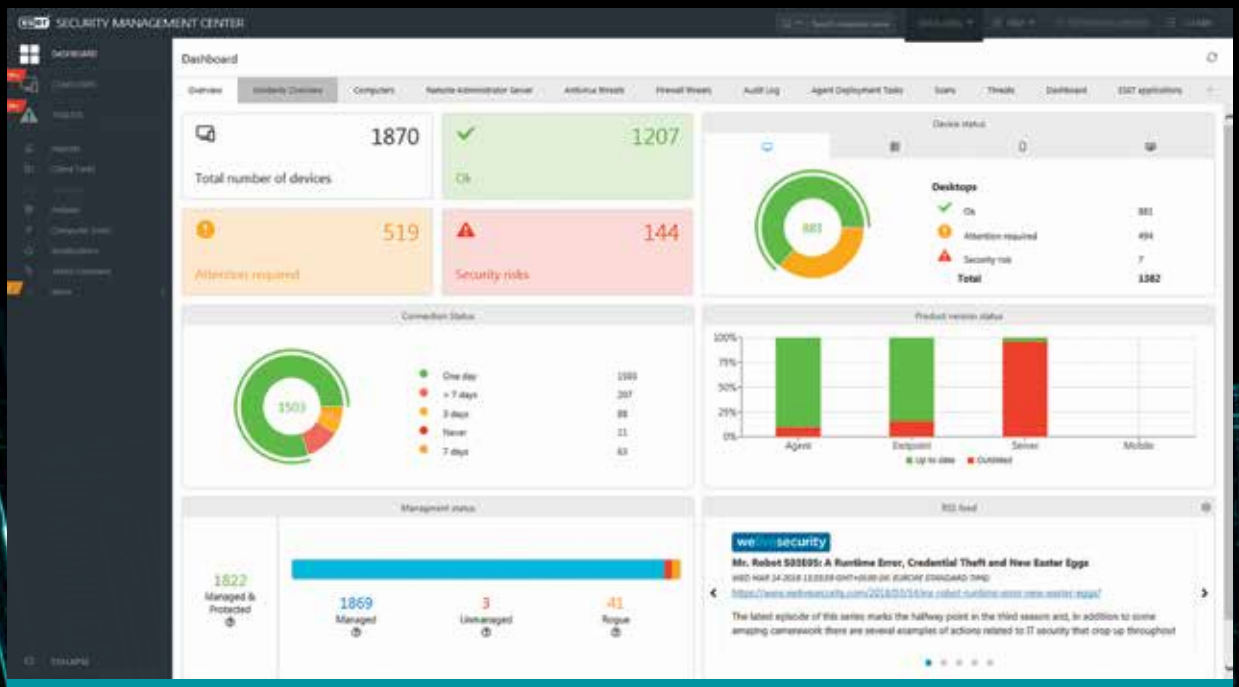


SCHUTZ VOR NETZWERKANGRIFFEN

Die ESET Produkte prüfen bereits auf Netzwerkebene. Dies erhöht den Schutz gegenüber Malware, Netzwerkangriffen und Exploits, für die noch kein Patch existiert.

„Am meisten sticht der starke technische Vorsprung gegenüber anderen Produkten am Markt hervor. ESET bietet zuverlässige Sicherheit, sodass ich jederzeit an jedem beliebigen Projekt arbeiten kann und weiß, dass unsere Computer zu 100 Prozent geschützt sind."

— Fiona Garland, Business Analyst Group IT;
Mercury Engineering, Irland; 1.300 Seats



Security Management Center

Mit dem ESET Security Management Center für Windows und Linux verwalten Sie alle ESET Lösungen komfortabel auf einen Blick. Das Security Management Center lässt sich dabei lokal installieren oder als virtuelle Applikation importieren.

„ESET erfüllt all unsere Ansprüche: Zuverlässige Technologie, sehr gute Erkennungsraten, und professioneller Support."

— Ernesto Bonhoure, Manager IT-Infrastruktur; Hospital Alemán, Argentinien, 1.500+ Seats

Use Cases

Dateilose Attacken

Use Case: Dateilose Malware ist verhältnismäßig neu und kann nicht mit herkömmlichen Methoden erkannt werden, agiert sie doch allein im Arbeitsspeicher.

DIE LÖSUNG

- ✓ Der Tiefenscan erkennt und blockiert Schadsoftware, sobald sie im Arbeitsspeicher aktiv wird.
- ✓ Erscheint ein Sample verdächtig, kann ESET Security für Microsoft SharePoint es an ESETs cloudbasierte Sandbox, ESET Dynamic Threat Defense, senden. So ist sichergestellt, dass Gefahren als solche erkannt und Fehlalarme vermieden werden.
- ✓ Die Erkennung und Analyse von Gefahren wird zudem durch den Upload von Daten in ESET Threat Intelligence erheblich beschleunigt.

Zero-Day-Bedrohungen

Use Case: Zero-Day-Bedrohungen sind für Unternehmen besonders besorgniserregend, da sie nicht wissen, wie sie auf diese bisher unbekannten Gefahren reagieren sollen.

DIE LÖSUNG

- ✓ ESET Threat Intelligence stellt Informationen zu den neuesten Bedrohungen und gezielten Angriffen zur Verfügung und hilft so, selbst unbekannte Bedrohungen zu erkennen.
- ✓ Mithilfe von Heuristiken und Machine Learning-Algorithmen sind die ESET Endpoint-Lösungen in der Lage, auch bisher komplett unbekannte Gefahren zu identifzieren.
- ✓ Mithilfe des cloud-basierten Systems ESET LiveGrid sind Sie selbst vor neuesten Gefahren geschützt – und das ohne auf Updates warten zu müssen.

Ransomware

Use Case: Ransomware ist für viele Unternehmen eine ernstzunehmende Bedrohung, gegenüber der sie sich besonders absichern möchten. Zudem wollen sie die Gewissheit, dass Netzlaufwerke und SharePoint-Datenbanken vor Verschlüsselung durch Dritte geschützt sind.

DIE LÖSUNG

- ✓ Sobald eine Datei auf den SharePoint Server hochgeladen wird, wird sie von ESET geprüft und als gutartig, schädlich oder verdächtig eingestuft.
- ✓ Der Schutz vor Netzwerkangriffen blockiert Exploits bereits auf Netzwerkebene und kann Ihr Unternehmen so vor Ransomware-Angriffen schützen.
- ✓ Unsere Mehrschichttechnologie ist mit einer Sandbox ausgestattet, die selbst gut getarnte Malware anhand ihres Verhaltens identifiziert.
- ✓ Mithilfe des cloud-basierten Systems ESET LiveGrid sind Sie selbst vor neuesten Gefahren geschützt – unabhängig von regulären Updates.
- ✓ Alle Produkte sind mit einem Ransomware Shield ausgestattet und schützen so vor der Verschlüsselung von Daten durch Kriminelle.

Über ESET

ESET ist einziger „Challenger“ in Gartners Magic Quadrant for Endpoint Protection Platforms.*

Seit mehr als 30 Jahren ist ESET® Vorreiter in der IT-Security-Branche und schützt sowohl Unternehmen als auch Privatleute auf der ganzen Welt. ESET ist und bleibt inhabergeführt. Wir haben keine offenen Forderungen oder Kredite und können so stets das tun, was wir für das Beste für unsere Kunden halten.

ESET IN ZAHLEN

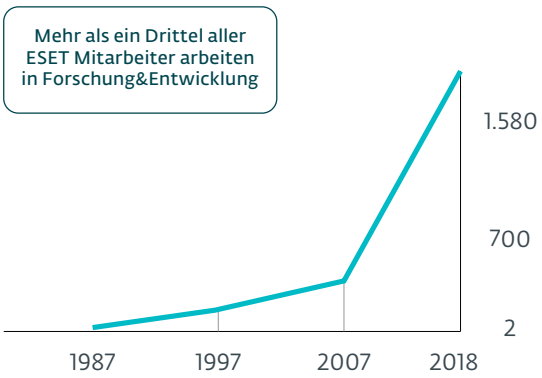
110+ Mio.
Nutzer weltweit

400k+
Business-kunden

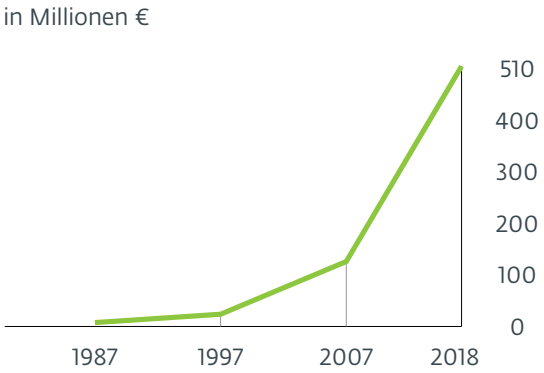
200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

ESET MITARBEITER



ESET ERLÖSE



*Gartner wirbt für keine der erwähnten Anbieter, Produkte oder Dienstleistungen. Gartners Publikationen basieren auf den Meinungen seiner Forschungseinrichtungen und sollten nicht als Fakten ausgelegt werden. Gartner lehnt jede ausdrückliche oder implizierte Gewährleistung in Bezug auf diese Untersuchung ab, einschließlich der Gewährleistung der Marktgängigkeit oder der Eignung für einen bestimmten Zweck.

ZUFRIEDENE KUNDEN

HONDA

Seit 2011 durch ESET geschützt

Lizenz 3x verlängert, 2x erweitert

Canon

Canon Marketing Japan Group

Seit 2016 durch ESET geschützt

Mehr als 14.000 Endpoints

Allianz Suisse

Seit 2016 durch ESET geschützt

Mehr als 4.000 Postfächer

T

ISP Security Partner seit 2008

2 Millionen Kunden

AUSZEICHNUNGEN

CRN 2019 Bester Hersteller

Produkt des Jahres ESET Endpoint Security

Endpoint Protection Plattform (Epp) – GOLD – Readers' Choice Security Insider AWARD 2018

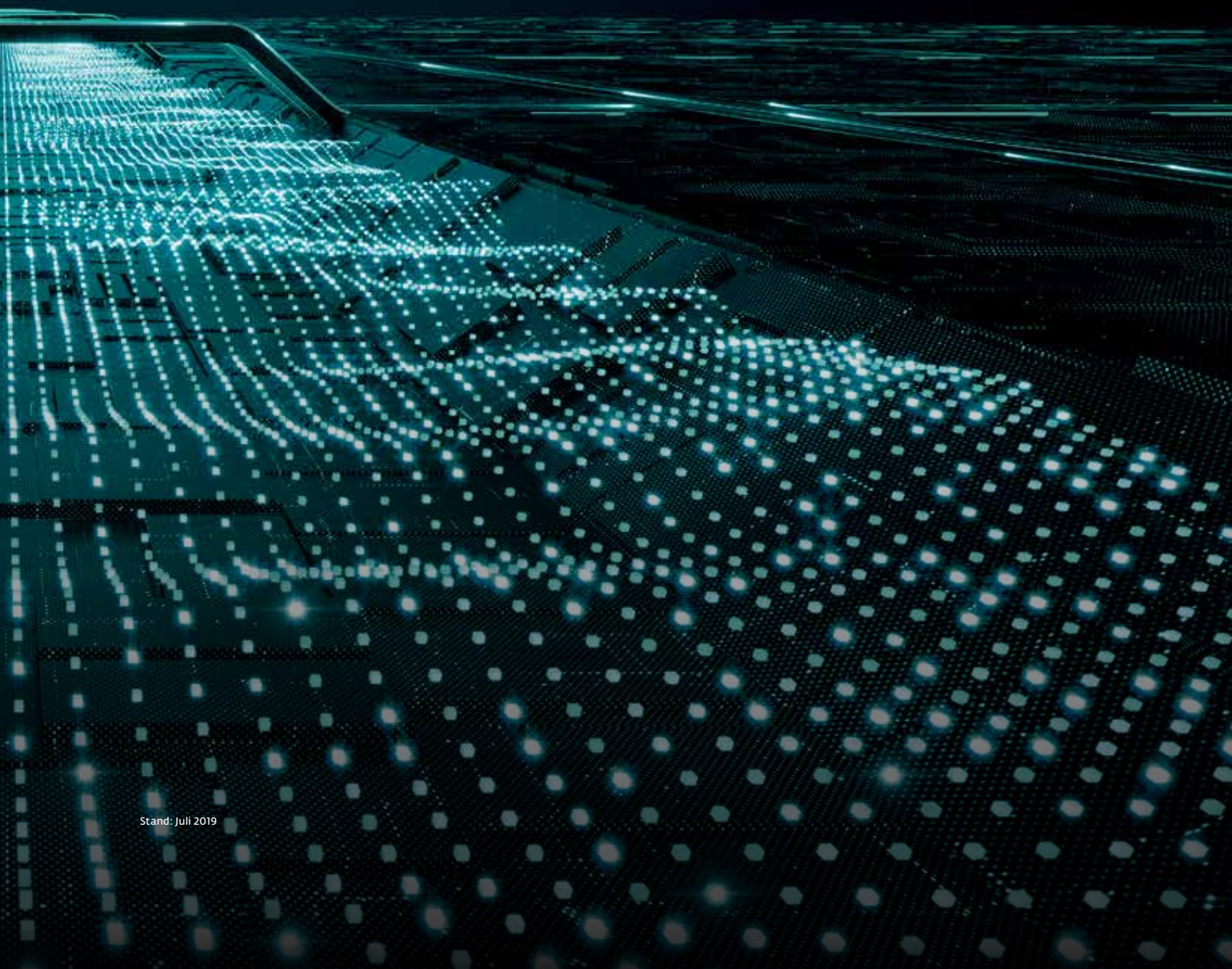
„Angesichts der guten Schutz- und Verwaltungs-Funktionen sowie der globalen Reichweite des Supports sollte ESET bei Ausschreibungen von großen Unternehmen für IT-Sicherheitslösungen immer in die engere Wahl genommen werden."

KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018

ENJOY SAFER TECHNOLOGY™

ESET.DE | ESET.AT | ESET.CH



Stand: Juli 2019