LÖSUNGSANSATZ &
PRODUKTÜBERSICHT

DYNAMIC THREAT DEFENSE

Schützen Sie sich vor Zero-Day-Angriffen und Ransomware durch cloudbasiertes Sandboxing

VERFÜGBAR ALS MANAGED SERVICE

TEIL DES MULTI-SECURED ENDPOINT KONZEPTS

ESET.DE | ESET.AT | ESET.CH

Was ist eine **cloudbasierte Sandbox-Analyse?**

Bei einer cloudbasierten Sandbox handelt es sich um eine Testumgebung, in der ein verdächtiger Binärcode isoliert ausgeführt wird. Sein Verhalten wird beobachtet, dokumentiert und automatisch analysiert.

ESET Dynamic Threat Defense ergänzt den Schutz anderer ESET Sicherheitslösungen wie ESET Mail Security und ESET Endpoint Security. Die cloudbasierte Sandboxing-Technologie ist in der Lage, bis dahin unbekannte Bedrohungen, insbesondere Ransomware, noch besser zu erkennen. Die Sandbox besteht aus einer Vielzahl an Sensoren, die statische Codeanalysen, Prüfungen des Arbeitsspeichers, eingehende Analysen über Machine Learning Algorithmen sowie verhaltensbasierte Prüfungen durchführen.

Zwei **gute Gründe**

RANSOMWARE

Spätestens seit Cryptolocker im Jahre 2013 stellt Ransomware eine reale Gefahr für Industrienetzwerke auf der ganzen Welt dar. Dabei ist das Konzept der Ransomware natürlich schon viel länger bekannt. Allerdings erschien die Bedrohung nicht so groß, dass sich Unternehmen ernsthaft mit der Situation auseinandergesetzt hätten.

Das sieht heute schon ganz anders aus: Das Bewusstsein dafür, dass schon ein einziger Ransomware-Angriff durch die Verschlüsselung wichtiger Dateien das gesamte Unternehmen lahmlegen 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. Cloudbasiertes Sandboxing erweitert die Abwehr des Unternehmens um eine zusätzliche Schicht und verhindert, dass Ransomware in einer Produktivumgebung ausgeführt wird.

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 oder einem Datenleck betroffen, sind sie oft überrascht, dass ihre Abwehr scheinbar mühelos durchbrochen werden konnte (vorausgesetzt, der Angriff wird überhaupt bemerkt). 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.

Eine cloudbasierte Sandbox-Analyse ist wesentlich effektiver als andere Technologien, da sie nicht nur das äußere Erscheinungsbild einer potenziellen Bedrohung analysiert, sondern zudem beoachtet, was das Element tut. Somit kann sie wesentlich bessere Entscheidungen bezüglich der Frage treffen, ob es sich eventuell um einen gezielten Angriff oder einen Advanced Persistent Threat (APT) handelt oder ob das Sample ungefährlich ist.

Cloudbasiertes Sandboxing erweitert die Abwehr des Unternehmens um eine zusätzliche Schicht.

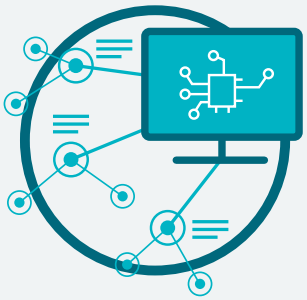
Sie sieht nicht nur das äußere Erscheinungsbild sondern untersucht genau, was eine potenzielle Bedrohung tut.

Die Technologie

Unsere Produkte und Technologien stehen auf 3 Säulen

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.

ESET bietet **einfach mehr**

MEHRSCHICHTIGER SCHUTZ

Bei der Analyse eines Samples durch ESET Dynamic Threat Defense werden zunächst drei verschiedene Machine Learning Modelle verwendet. Anschließend wird das Objekt in einer Sandbox ausgeführt, die das Nutzerverhalten imitiert, um potenzielle Tarnmechanismen zu enthüllen. Danach wird das beobachtete Verhalten über neuronale Netzwerke mit bekannten Verhaltensmustern abgeglichen. Zuletzt nimmt die neueste Version von ESETs Scan Engine die einzelnen Komponenten auseinander und prüft sie auf Auffälligkeiten.

TRANSPARENZ

In den ESET PROTECT Management-Konsolen werden umfangreiche Informationen über alle Samples und deren Herkunft angezeigt. In dieser leicht verständlichen Übersicht sind nicht nur die von ESET Dynamic Threat Defense geprüften Samples enthalten, sondern auch alle Elemente, welche an die cloudbasierte Reputationsdatenbank ESET LiveGrid® gesendet wurden.

ÜBERALL VERFÜGBAR

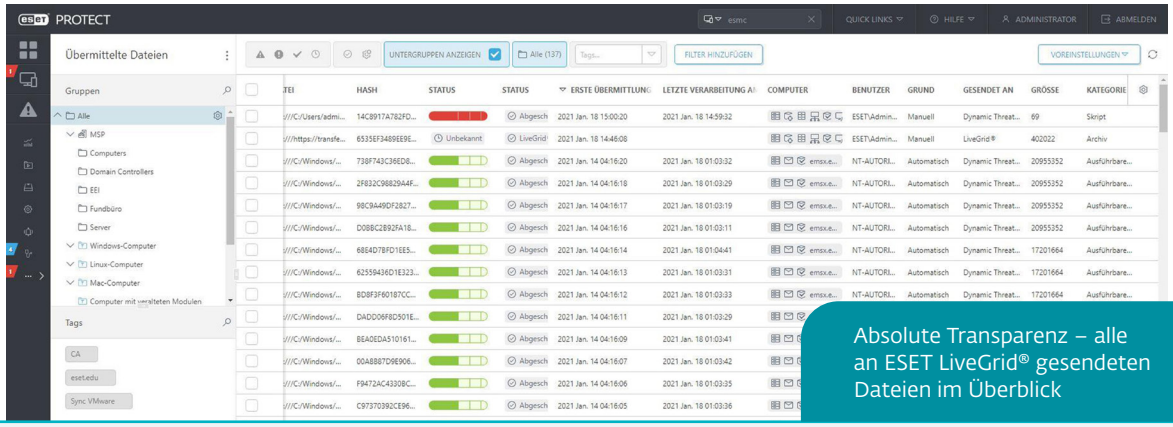
Mobilität ist heute ein Muss – ESET Dynamic Threat Defense bietet deshalb die Möglichkeit, Dateien auch außerhalb des Firmennetzwerks zu scannen. Sollten bösartige Samples erkannt werden, ist automatisch das gesamte Unternehmen geschützt.

EINZIGARTIGE GESCHWINDIGKEIT

Jede Minute zählt. Deshalb werden die meisten Samples in weniger als 5 Minuten analysiert. Wurden Elemente zuvor bereits geprüft, dauert es nur wenige Sekunden, bis alle Geräte in Ihrem Unternehmen geschützt sind.

BEWÄHRT UND ZUVERLÄSSIG

ESET hat eine lange Erfolgsgeschichte. Bereits seit 1987 gehören wir zu den Vorreitern der IT-Security-Branche und arbeiten stets an der Optimierung unserer Sicherheitslösungen. Mehr als 110 Millionen Anwender weltweit vertrauen auf unsere Technologien und auch unabhängige Testinstitute bestätigen immer wieder die Effektivität unserer Produkte bei der Abwehr moderner Bedrohungen.



Absolute Transparenz – alle an ESET LiveGrid® gesendeten Dateien im Überblick

So **funktioniert's**

Ransomware

PROBLEM

Häufig gelangt Ransomware über E-Mails in die Posteingänge ahnungsloser Nutzer.

LÖSUNG

- ✓ Der Admin kann die Anzahl der erkannten Spam-, Malware- oder Phishing-E-Mails überprüfen und analysieren, welche Nutzer am häufigsten von schädlichen E-Mails betroffen sind.
- ✓ Der Admin kann beobachten, an welchen Tagen und zu welchen Zeiten die meisten Spam-E-Mails den Nutzern der Organisation zugestellt werden.
- ✓ Aus den erhobenen Kennzahlen können die Admins direkt Berichte und Empfehlungen an die Führungskräfte vorlegen.

Rollenspezifischer Schutz

PROBLEM

Je nach Position im Unternehmen benötigen Mitarbeiter unterschiedliche Sicherheitseinstellungen. So benötigen Entwickler oder IT-Mitarbeiter völlig andere Rechte als der Leiter einer Niederlassung oder der CEO.

LÖSUNG

- ✓ Legen Sie in ESET Dynamic Threat Defense Policies für einzelne Rechner oder Server an.
- ✓ Wenden Sie die Policies automatisch auf einzelne statische und dynamische Nutzergruppen oder Active Directory Gruppen an.
- ✓ Ändern Sie die Einstellungen eines Nutzers ganz einfach, indem Sie ihn in eine andere Gruppe verschieben.

Unbekannte oder verdächtige Dateien

PROBLEM

Von Zeit zu Zeit erhalten Mitarbeiter oder die IT-Abteilung Dateien, bei denen sie absolut sichergehen wollen, dass sie ungefährlich sind.

LÖSUNG

- ✓ Jeder Nutzer kann aus allen ESET Produkten Samples zur Analyse einreichen.
- ✓ Das fragliche Element wird umgehend von ESET Dynamic Threat Defense analysiert.
- ✓ Wird eine Datei als schädlich identifiziert, werden alle Rechner im Unternehmen automatisch geschützt.
- ✓ IT-Admins erhalten Auskunft über den Nutzer, der das Sample eingereicht hat und ob die Datei als sauber oder schädlich eingestuft wurde.

BERICHT ZUM DATEIVERHALTEN

STATUS	Bösartig
SHA-1	14C8917A782FD2C26346AFAD8A26C3735E25DC96
GRÖSSE	69B
KATEGORIE	Skript

Erkannte Verhaltensweisen

VERHALTEN	**Malware vor Ausführung erkannt.**
ERKLÄRUNG	Das Sample wurde vor Ausführung als bösartig erkannt.
GUTARTIGE URSACHEN	Das sollte bei sauberen Anwendungen nicht vorkommen.
BÖSARTIGE URSACHEN	Schadsoftware wurde nach ihrer Ausführung vom ESET Prüfmodul erkannt.

ESET Dynamic Threat Defense

Technische Features

AUTOMATISCHER SCHUTZ

Nach der Installation müssen weder Admin noch Endnutzer aktiv werden. Das Endpoint- oder Server-Produkt entscheidet automatisch, ob ein Sample sauber, schädlich oder unbekannt ist. Im letzteren Fall wird das Sample zur weiteren Analyse an ESET Dynamic Threat Defense gesendet. Anschließend wird das Ergebnis für alle Endpoint-Produkte bereitgestellt.

AUF IHREN BEDARF ZUGESCHNITTEN

ESET Dynamic Threat Defense ist ab 5 Seats verfügbar und ermöglicht eine detaillierte Policy-Konfiguration für jeden Rechner. Der Admin kann festlegen, welche Samples eingereicht und welche Aktionen anhand der Ergebnisse ausgeführt werden sollen.

MANUELLER SAMPLE-UPLOAD

Nutzer oder Admins können Samples aus kompatiblen ESET Produkten manuell zur Analyse hochladen und das vollständige Ergebnis einsehen. Mit ESET PROTECT erhalten Admins detaillierte Einblicke zu eingereichten Samples und deren Analyseergebnissen.

SCHUTZ FÜR DATEIEN UND E-MAILS

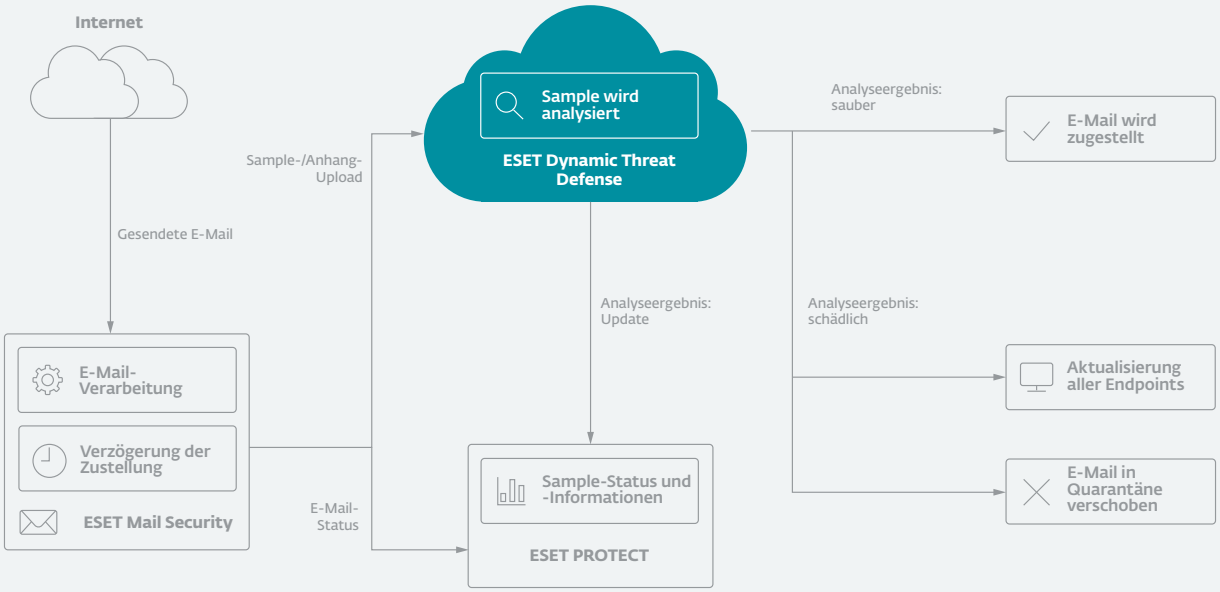
ESET Dynamic Threat Defense funktioniert sowohl mit den Endpoint-Lösungen zur Erkennung infizierter Dateien als auch mit der ESET Mail Security, um schädliche E-Mails von den Posteingängen Ihrer Mitarbeiter fernzuhalten. Für einen reibungslosen Geschäftsbetrieb werden ausschließlich E-Mails von externen Absendern zur Analyse eingereicht. Weiterhin ist ESET Dynamic Threat Defense fester Bestandteil von ESET Cloud Office Security für einen umfassenden Schutz von Microsoft 365 Cloud-Anwendungen.

„Eine komplexe IT-Sicherheitslösung muss einwandfrei funktionieren und dennoch einfach zu bedienen sein. Diesen Spagat schafft ESET vorbildlich.“

— Stefan Pistorius, Gruppenleiter EDV Service und Administration bei kohlpharma

So funktioniert **ESET Dynamic Threat Defense**

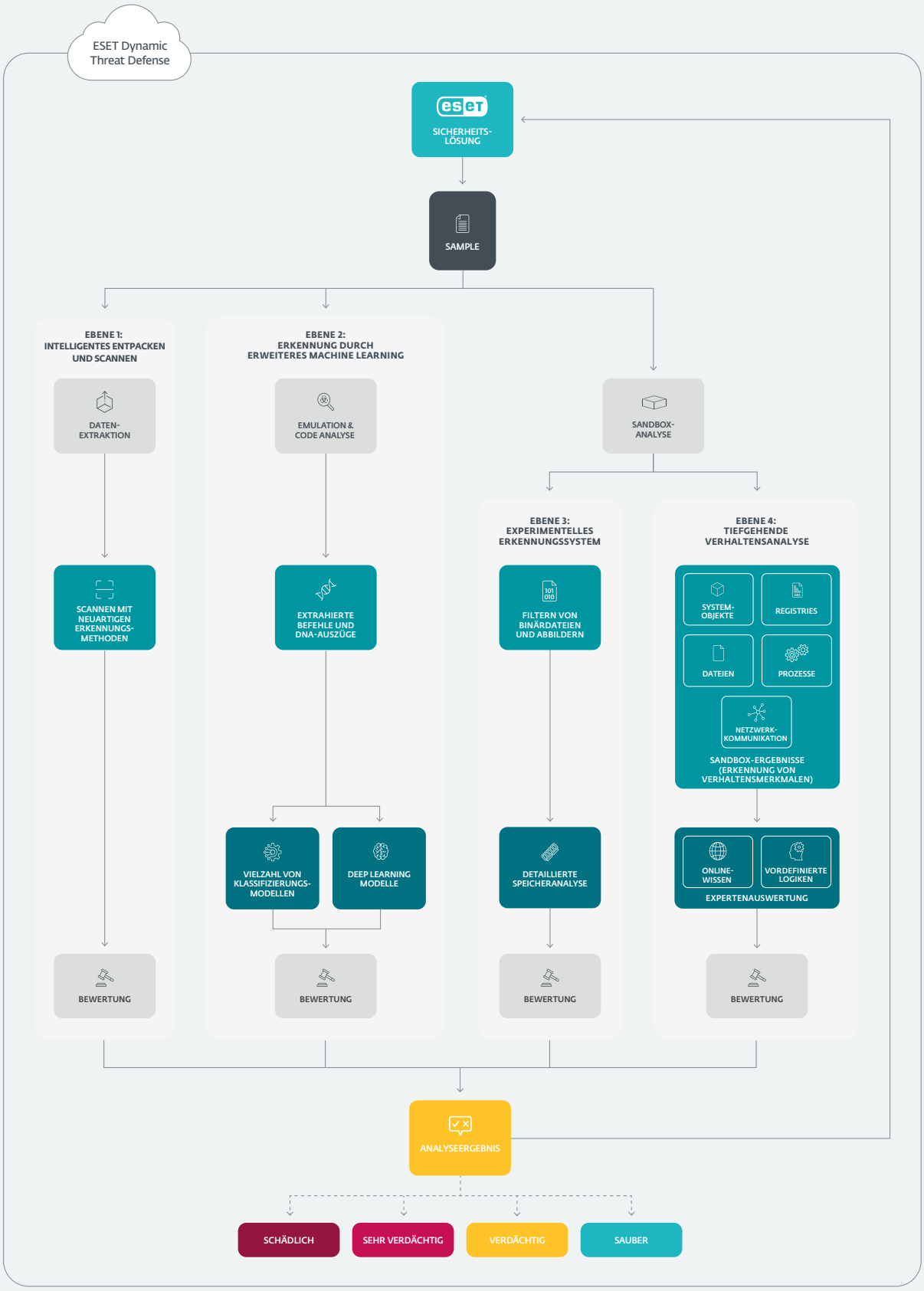
am Beispiel ESET Mail Security



„ESET wäre die Idealbesetzung eines Spielers bei uns: starkes Pressing gegen Hacker, überzeugende Defensive gegen Malware und ein vorausschauendes Spiel mit Überblick."

— Stephan Horst, Abteilungsleiter IT Borussia Dortmund

Cloud-Analyse **im Detail**



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