PRODUKTÜBERSICHT

ESET PROTECT

Die Management-Konsole für die zentrale Verwaltung Ihrer Systeme

VERFÜGBAR ALS MANAGED SERVICE

TEIL DER ZERO TRUST SECURITY-STRATEGIE

ESET 100% Made in EU IT-Security

ESET.DE | ESET.AT | ESET.CH

WAS IST
SECURITY MANAGEMENT?

Die Management-Konsole ESET PROTECT bietet einen kompletten Überblick über alle Endpoints in Echtzeit innerhalb und außerhalb einer Organisation. Sie gewährleistet so ein vollständiges Security Management und umfassendes Reporting für alle Betriebssysteme.

Behalten Sie die Übersicht über alle installierten ESET Lösungen ohne räumliche Grenzen und die volle Kontrolle über Ihre IT-Sicherheit. Vermeiden und erkennen Sie Schwachstellen sowie andere potenzielle Gefahren und reagieren Sie umgehend auf Vorfälle über alle Plattformen hinweg – ob Desktops, Server oder Mobilgeräte. ESET PROTECT steht sowohl cloudbasiert als auch On-Premises zur Verfügung.

ESET **BIETET EINFACH MEHR**

Prävention bis Reaktion

Das Management unserer Lösungen in einer Konsole vereint: ESET PROTECT deckt von der Bedrohungserkennung über präventive Maßnahmen bis hin zu einer vollständigen Endpoint Detection and Response-Lösung (EDR) die Bedürfnisse Ihrer Organisation ab. Unsere mehrschichtige Technologie sorgt dabei für ein höchstmögliches Schutzlevel.

Vorfälle mit nur einem Klick beheben

Über das Dashboard erhalten IT-Admins einen umfassenden Überblick zu Sicherheitsvorfällen und können damit die Situation schnell einschätzen sowie darauf reagieren. Mit nur einem Klick können bspw. Ausschlüsse festgelegt, Dateien zur weiteren Analyse eingereicht oder Scans gestartet werden. Ausschlüsse können nach Bedrohungsname, URL, Hash oder einer Kombination dieser Kriterien festgelegt werden.

Rollenbasierte Zugriffskontrolle

Der Zugriff auf die Konsole ist durch eine Multi-Faktor-Authentifizierung geschützt. Darüber hinaus ist sie mit einem erweiterten Role-Based Access Control System ausgestattet. Dabei können Administratoren und Nutzern der Konsole bestimmte Netzwerkbereiche und Objektgruppen zugewiesen sowie granulare Berechtigungsstufen festgelegt werden.

MSP Ready

Als Managed Service Provider können Sie in ESET PROTECT eine unbegrenzte Anzahl von Mandanten hinzufügen. Dabei werden MSP-Lizenzen automatisch erkannt und mit den Lizenzservern synchronisiert. Zudem bietet die Konsole zusätzliche Features wie z.B. die Installation/Löschung von Drittanbieter-Anwendungen, das Ausführen von Skripten, Remote-Befehle, die Auflistung von laufenden Prozessen oder Hardware-Konfigurationen.

Dynamisches und anpassbares Reporting

ESET PROTECT bietet mehr als 170 sofort nutzbare Berichte und ermöglicht eine individuelle Anpassung anhand von mehr als 1.000 Datenpunkten. Die erstellten Berichte können nach Bedarf konfiguriert und anschließend in regelmäßigen Abständen generiert sowie per E-Mail zugestellt werden.

Automatisierung über dynamische Gruppen

Computer können je nach definierten Kriterien oder aktuellem Gerätestatus dynamischen Gruppen zugeordnet werden. Bei Änderungen der Gruppenzugehörigkeit können automatische Tasks ausgeführt werden, z.B. Prüfungen, Richtlinienänderungen oder Installation bzw. Deinstallation von Software.

Automatischer VDI Support

Über einen Hardware-Erkennungsalgorithmus werden die Maschinen anhand ihrer Hardware zuverlässig identifiziert. Das ermöglicht eine automatisierte Nachbildung nicht-persistenter Hardware-Umgebungen. Die Virtual Desktop Infrastructure (VDI) Unterstützung von ESET erfordert dabei keine manuellen Eingriffe.

Individuelle Benachrichtigungen

Das Benachrichtigungssystem beinhaltet einen Editor, über den Sie Meldungen ganz nach Ihrem Bedarf anpassen können, um ausschließlich gewünschte Informationen zu erhalten.

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.

DIE OBJEKTIVEN VORTEILE **EINER CLOUD-KONSOLE**

In wenigen Minuten einsatzbereit

Mit einer Cloud-Konsole schützen Sie Ihre Endpoints – ohne räumliche Grenzen – in kürzester Zeit. Sparen Sie wertvolle Ressourcen, die sonst für die Planung und Durchführung von Installationen notwendig waren, öffnen Sie Ihren Account und legen direkt los.

Niedrige Betriebskosten (TCO)

Der Wechsel von einer On-Premises-Konsole auf eine Cloud-Konsole bringt spürbare Vorteile mit sich. Für die cloudbasierte Variante werden keine eigenen Server benötigt. Damit entfallen auch Wartung, Upgrades, Patches oder Backups. Fehleranfällige, wiederkehrende Aufgaben entfallen dadurch und setzen wertvolle Ressourcen frei. Zudem entfallen z.B. Energie- und Lizenzkosten.

Immer auf dem aktuellen Stand

Die Aktualisierung der Konsole auf die neueste Version wird im Hintergrund automatisch durchgeführt, ohne dass Sie aktiv werden müssen. Somit profitiert Ihre Organisation jederzeit von den neuesten Komponenten und Features. Der optimale Schutz für Sie als Kunden ist somit jederzeit gewährleistet.

Überall und jederzeit verfügbar

Über Ihren favorisierten Webbrowser haben Sie die Möglichkeit auf die Cloud-Konsole zuzugreifen. Im Gegensatz zur On-Premises-Konsole sind dafür allerdings weder Firewall-Ausschlüsse noch komplizierte VPN-Einrichtungen erforderlich. Dabei können Sie sich auf die Sicherheit unserer Infrastruktur und eine maximale Verfügbarkeit verlassen.

Effizienter Support

Da die Cloud-Konsole stets auf dem aktuellen Stand ist, können die ESET Experten schnellere und effizientere Hilfe bieten. Schließlich sind Recherchen zum Versionsstand und der Installationsumgebung in diesem Fall nicht notwendig.

WICHTIGER HINWEIS

Bei allen Vorteilen, die eine cloudbasierte Konsole bietet, haben wir ein allgemeines Verständnis dafür, dass einige Organisationen eine derartige Lösung nicht einsetzen dürfen, können oder wollen. ESET PROTECT ist daher auch weiterhin mit derselben Lizenz als On-Premises-Version nutzbar. Sollten Sie zu einem späteren Zeitpunkt in die Cloud migrieren wollen, ist dies ebenfalls möglich.

SO **FUNKTIONIERT'S**

Ransomware

Ein Nutzer öffnet eine schädliche E-Mail mit einer neuen Art von Ransomware.

LÖSUNG

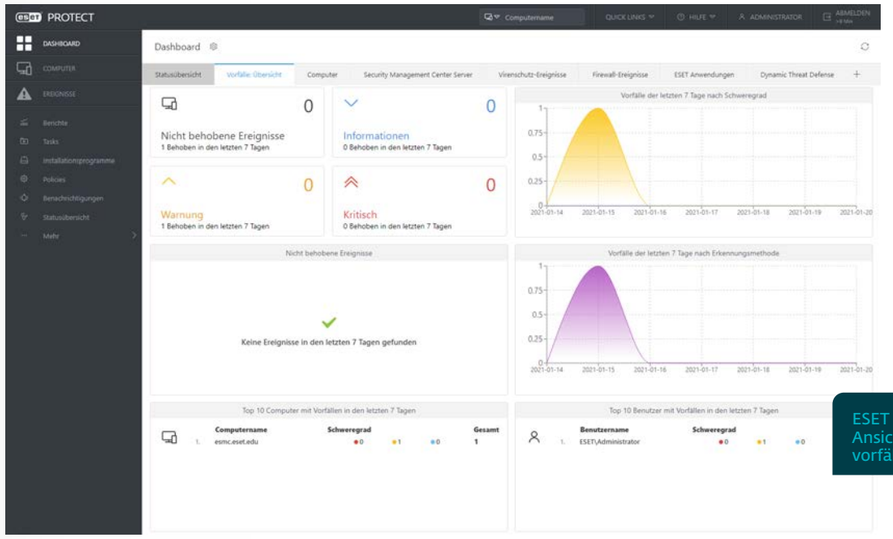
- ✓ Ihre IT-Abteilung erhält per E-Mail und SIEM-Tool die Meldung, dass auf einem bestimmten Computer eine neue Bedrohung erkannt wurde.
- ✓ Mit nur einem Klick wird auf dem infizierten Rechner eine Prüfung gestartet.
- ✓ Mit einem weiteren Klick wird die Datei an ESET LiveGuard® Advanced übermittelt.
- ✓ Nach erfolgreicher Abwehr der Bedrohung werden automatisch alle entsprechenden Warnungen in ESET PROTECT gelöscht.

Entwickler

Programmierer, die auf ihrem Firmenrechner mit Code arbeiten, können durch die Kompilierung von Software möglicherweise Fehlalarme erzeugen.

LÖSUNG

- ✓ Ihre IT-Abteilung erhält per E-Mail und SIEM-Tool die Meldung, dass eine neue Bedrohung erkannt wurde.
- ✓ Der Meldung ist zu entnehmen, dass die Bedrohung auf dem Computer eines Entwicklers gefunden wurde.
- ✓ Mit einem Klick wird die Datei an ESET LiveGuard® Advanced übermittelt, um zu bestätigen, dass sie nicht schädlich ist.
- ✓ Die IT-Abteilung erstellt wiederum mit nur einem Klick einen Ausschluss und verhindert damit künftige Fehlalarme in diesem Umfeld.



ESET PROTECT Dashboard — Ansicht der Sicherheitsvorfälle

VDI-Bereitstellungen

Nicht-persistente Hardware-Umgebungen müssen in der Regel manuell aufgesetzt werden und sind für die IT-Abteilung ein Albtraum in Sachen Reporting und Transparenz.

LÖSUNG

- ✓ Mit dem Deployment eines Master Images auf bereits vorhandene Computer in ESET PROTECT berichten diese auch nach einer kompletten Umstrukturierung weiterhin an ihre bisherige Instanz.
- ✓ In den Ausgangszustand zurückgesetzte Maschinen verursachen keine Duplikate, sondern werden zu einem Datensatz zusammengefasst.
- ✓ Bei der Bereitstellung von nicht-persistenten Images können Sie den jeweiligen Agenten integrieren. Bei der Erstellung einer neuen Maschine mit einem anderen Hardware-Fingerabdruck wird dann automatisch ein neuer Eintrag in ESET PROTECT angelegt.

Inventarisierung von Hard- und Software

Unternehmen sollten wissen, welche Software auf den Firmenrechnern installiert ist und wie alt die Computer sind.

LÖSUNG

- ✓ Werfen Sie einen Blick in das Softwareverzeichnis Ihrer Geräte, um jedes Stück Software und die aktuelle Versionsnummer aufzuspüren.
- ✓ Lassen Sie sich Hardware-Details anzeigen, z.B. Gerät, Hersteller, Modell, Seriennummer, Prozessor, RAM oder Festplattenkapazität und vieles mehr.
- ✓ Ganzheitliche Berichte sorgen jederzeit für einen aktuellen Überblick über Ihre Organisation. So fällen Sie Budgetentscheidungen nicht nur auf Basis valider Daten sondern auf Wunsch sogar nach Hersteller und Modellnummern.

Beseitigung von unerwünschter Software

Ihre IT-Abteilung sollte umgehend über die Installation nicht genehmigter Software benachrichtigt werden und angemessen darauf reagieren können.

LÖSUNG

- ✓ Richten Sie in ESET PROTECT für alle eine dynamische Gruppe ein, die nach einer spezifischen Software Ausschau hält.
- ✓ Erstellen Sie eine Meldung, die die IT-Abteilung informiert, sobald ein Computer das Kriterium erfüllt.
- ✓ Richten Sie in ESET PROTECT einen Task zur Software-Deinstallation ein, der automatisch ausgeführt wird, sobald ein Computer das Kriterium der dynamischen Gruppe erfüllt.
- ✓ Richten Sie eine Nutzerbenachrichtigung ein, die auf dem Bildschirm des Users erscheint und ihn informiert, dass er mit der Installation der Software einen Regelverstoß begangen hat.

TECHNISCHE **FEATURES**

Optimale Übersicht

Alle ESET Endpoint-Lösungen können direkt von ESET PROTECT aus verwaltet werden. Mit inbegriffen sind Workstations, Mobilgeräte, Server sowie die Betriebssysteme Windows, macOS, Linux und Android.

Flexible Installation

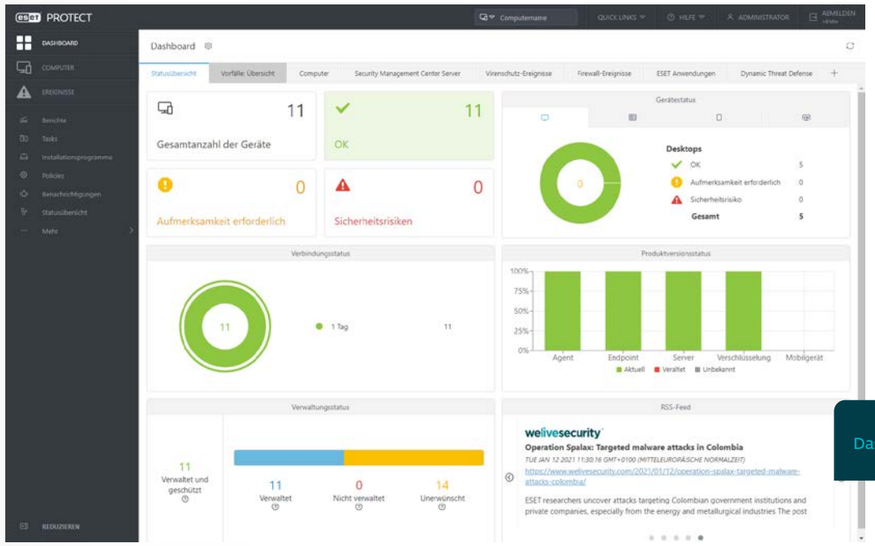
Die On-Premises-Version von ESET PROTECT kann auf Windows, Linux oder als virtuelle Appliance installiert werden. Nach der Installation erfolgt die gesamte Verwaltung über eine Web-Konsole, auf die dann von jedem Gerät bzw. Betriebssystem unkompliziert zugegriffen werden kann.

Multimandatenfähigkeit

Es können verschiedene Nutzer und Berechtigungsgruppen erstellt werden, um limitierte und maßgeschneiderte Zugriffsrechte auf die Management-Konsolen von ESET PROTECT zu gewähren.

Unterstützung von SIEM und SOC

ESET PROTECT komplettiert Ihre SIEM-Lösung (Security Information and Event Management) und kann Log-Informationen in den verbreiteten Formaten JSON und LEEF ausgeben, sodass eine Integration in Ihr SOC (Security Operations Center) möglich wird.



Dashboard von ESET PROTECT

TECHNISCHE **FEATURES**

Starke Festplattenverschlüsselung

Die Full Disk Encryption ist nativ in ESET PROTECT verfügbar und verwaltet die Verschlüsselung von Geräten unter Windows und macOS (FileVault). So gelingt es Organisationen, Daten in Ruhe effektiv zu schützen, gesetzliche Regularien zu erfüllen und Ihren Compliance-Anforderungen gerecht zu werden.

Cloud Sandboxing

Die Implementierung unserer leistungsstarken Cloud Sandbox (ESET LiveGuard® Advanced) ermöglicht eine schnelle und effektive Analyse von bisher unbekannten Bedrohungen wie Zero Day Malware, Ransomware und APTs.

Inventarisierung von Hard- und Software

Mit ESET PROTECT behalten Sie den Überblick über alle installierten Applikationen und die eingesetzten Geräte in Ihrer Organisation.

Granulare Policy-Verwaltung

Organisationen können für ein Gerät oder eine Nutzergruppe mehrere Richtlinien erstellen und Policies für vererbte Berechtigungen verschachteln. Darüber hinaus lassen sich die Policy-Einstellungen nutzerspezifisch konfigurieren, sodass diverse Einstellungen für den Nutzer gesperrt werden können.

Gefahrensuche und -abwehr

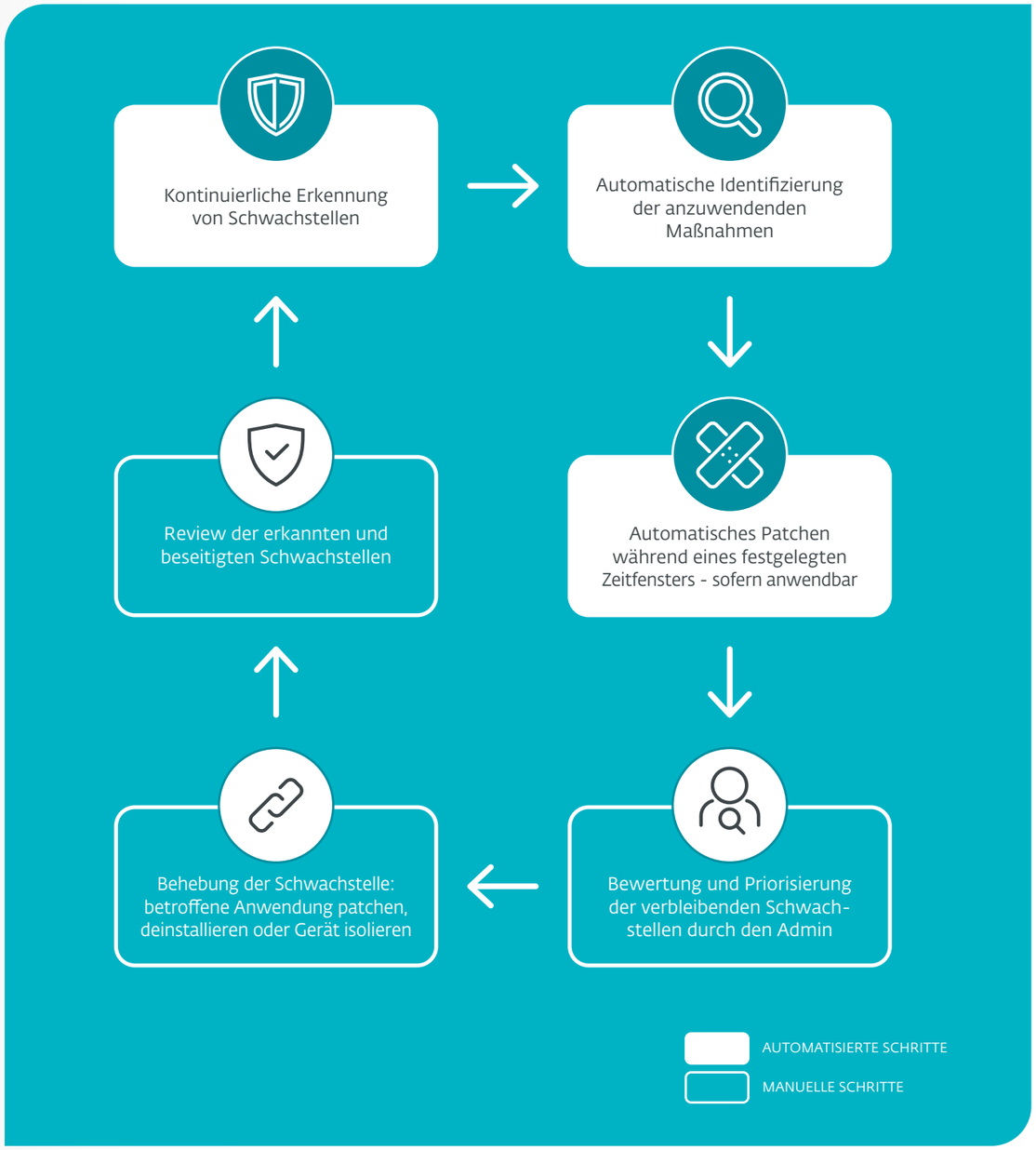
Für einen umfassenden Überblick über die aktuelle Sicherheitslage im Unternehmensnetzwerk unterstützt ESET PROTECT unsere Endpoint Detection and Response (EDR) Lösung ESET Inspect. ESET Inspect ist plattformübergreifend für Windows, Linux und macOS einsetzbar, bietet erweiterte Funktionalitäten zur Erkennung und Eliminierung von Bedrohungen und lässt sich nahtlos in Ihr SOC integrieren.

Zentrales Schwachstellen- und Patch-Management

ESET Vulnerability & Patch Management* unterstützt Organisationen dabei, Sicherheitslücken in ihren Systemen zuverlässig zu erkennen und zu beheben. Die Lösung identifiziert Schwachstellen in Betriebssystemen sowie gängigen Anwendungen und ermöglicht Admins, sowohl automatisch als auch manuell Patches auf allen Endgeräten zu installieren. Die Patch Policy lassen sich individuell anpassen und mithilfe zahlreicher Filteroptionen können Schwachstellen entsprechend ihres Schweregrads priorisiert werden. Dank des umgehenden Reportings haben Organisationen Sicherheitsrisiken direkt im Blick und können entsprechende Gegenmaßnahmen einleiten. IT-Admins erhalten so eine bessere Kontrolle über Ihre IT-Landschaft und sparen dank automatisierter Workflows wertvolle Zeit. ESET Vulnerability & Patch Management ist in ESET PROTECT Cloud verfügbar.

*Systemvoraussetzungen für ESET Vulnerability & Patch Management: ESET PROTECT Cloud und ESET Endpoint Security for Windows 10.1 oder neuer

ESET VULNERABILITY & PATCH MANAGEMENT – **SO FUNKTIONIERT'S**



Digital Security
Progress. Protected.

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 mithilfe von Cloud Sandboxing frei von Zero Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank 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

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal www.teletrust.de/itsmie

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

ISO 9001 SGS

ISO/IEC 27001 SGS

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2013 zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400k+
Geschützte Unternehmen

195
Länder & Regionen

13
Forschungs- und Entwicklungszentren weltweit

welivesecurity by ESET

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

ESET.DE | ESET.AT | ESET.CH

Digital Security
Progress. Protected.

ESET.DE | ESET.AT | ESET.CH

Stand: 06/2023