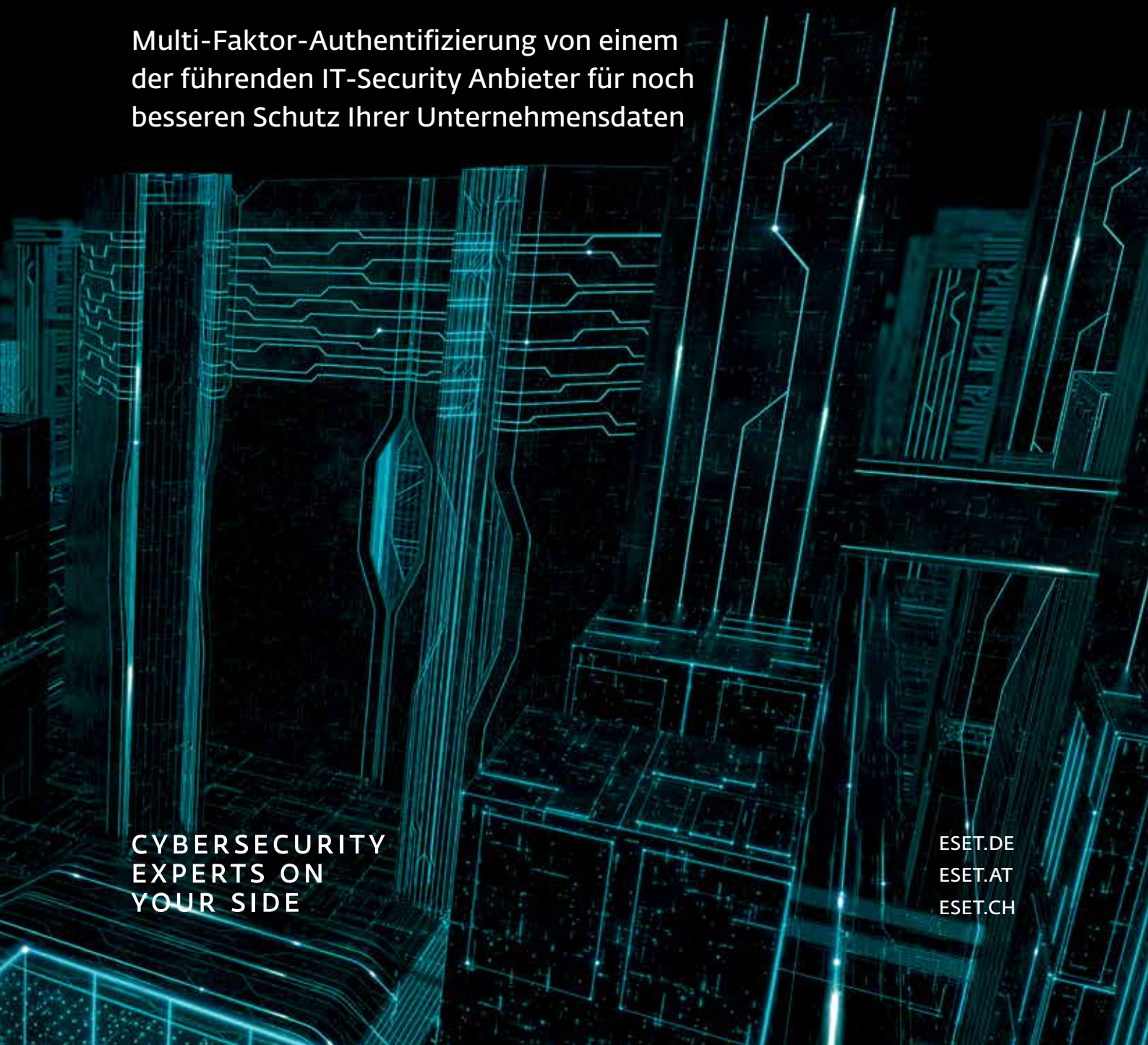
PRODUKTÜBERSICHT

SECURE AUTHENTICATION

Multi-Faktor-Authentifizierung von einem der führenden IT-Security Anbieter für noch besseren Schutz Ihrer Unternehmensdaten



CYBERSECURITY EXPERTS ON YOUR SIDE

ESET.DE
ESET.AT
ESET.CH

Was ist eigentlich eine **Multi-Faktor-Authentifizierung?**

Bei der Multi-Faktor-Authentifizierung (MFA), oft auch als Zwei-Faktor-Authentifizierung (2FA) bekannt, handelt es sich um eine Authentifizierungsmethode, bei der sich Benutzer mit mehr als einem Element ausweisen müssen. 2FA ist so wesentlich sicherer als althergebrachte, statische Passwortabfragen. Durch Kombination eines statischen Passworts mit einem zweiten, dynamischen Faktor wird die Gefahr von Datenverlusten bedeutend verringert.

Mit ESET Secure Authentication implementieren Unternehmen jeder Größe einfach und unkompliziert eine MFA für gemeinsam genutzte Systeme (Windows- & Server Logins, Microsoft Cloud-Dienste wie Office 365 oder OWA, VPNs und RADIUS-basierte Dienste).

Drei **gute Gründe**

Oft wird dasselbe Passwort für mehrere Anwendungen und Webseiten verwendet, notiert oder an Dritte weitergegeben.

UNZUREICHENDE PASSWORT-PFLEGE

Häufig gelten Mitarbeiter als „größte Schwachstelle" der IT-Sicherheit eines Unternehmens. Vor allem schlecht gepflegte Passwörter stellen eine große Gefahr fürs Business dar. Oft wird dasselbe Passwort für mehrere Anwendungen und Webseiten verwendet, notiert oder an Dritte weitergegeben. Klassische Gegenmaßnahmen wie die Pflicht, Passwörter regelmäßig zu ändern, bringen dabei oft wenig und führen noch mehr in Versuchung, ähnliche Passwörter zu verwenden oder Post-its mit den wichtigsten Kennwörtern an den Rechner zu kleben.

Eine Multi-Faktor-Authentifizierung schützt Unternehmen vor diesen Risiken, indem die reguläre Anmeldung um einen zusätzlichen Faktor erweitert wird – z.B. durch die Eingabe eines Einmal-Passworts, das auf dem Smartphone des Mitarbeiters generiert wird. Damit schützen Sie sich vor Angreifern, die versuchen, durch einfaches Erraten schwacher Passwörter Zugang zu Ihren Systemen zu erlangen.

DATENSCHUTZ-VERLETZUNGEN

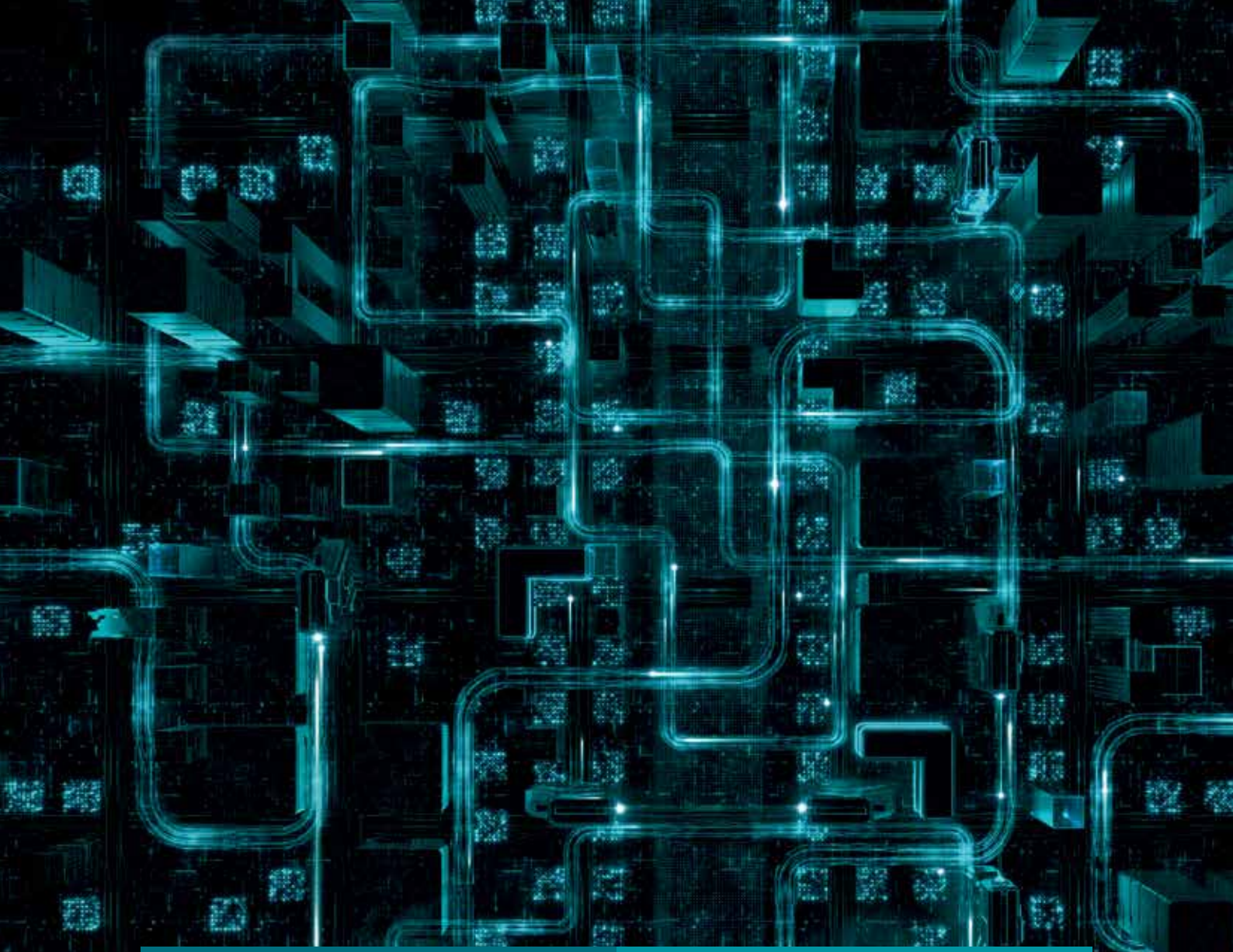
Beinahe täglich wird von Datenschutzverstößen in Unternehmen berichtet. Oft gelangen Angreifer über schwache oder gestohlene Zugangsdaten in das Unternehmensnetzwerk, die sie durch automatisierte Bots, Phishing oder zielgerichtete Angriffe ergattern. Über die Absicherung der normalen Logins hinaus kann die MFA auch privilegierte Zugänge vor unautorisierten Zugriffen schützen.

Mit einer Multi-Faktor-Authentifizierung ist es für Angreifer wesentlich schwerer, Zugriff auf Ihre Systeme und Daten zu erlangen. In der Regel sind Unternehmen von Datenschutzvorfällen betroffen, die mit sensiblen Informationen arbeiten. Dazu gehören insbesondere die Finanzbranche, der Einzelhandel, das Gesundheitswesen und der öffentliche Sektor. Das heißt jedoch keineswegs, dass andere Branchen sicher sind. Wie jeder andere „Unternehmer" wägen professionelle Hacker Kosten und Nutzen eines Angriffs sorgfältig ab. Entsprechend sollte man es Ihnen so schwer wie möglich machen.

COMPLIANCE

Unternehmen müssen zunächst prüfen, ob sie Datenschutzvorgaben unterliegen oder nicht. Anschließend sollten sie ermitteln, welche Maßnahmen die Vorgaben empfehlen bzw. vorschreiben. Eine starke Authentifizierung ist mittlerweile integraler Bestandteil gesetzlicher und anderer Vorgaben, darunter der EU-DSGVO.

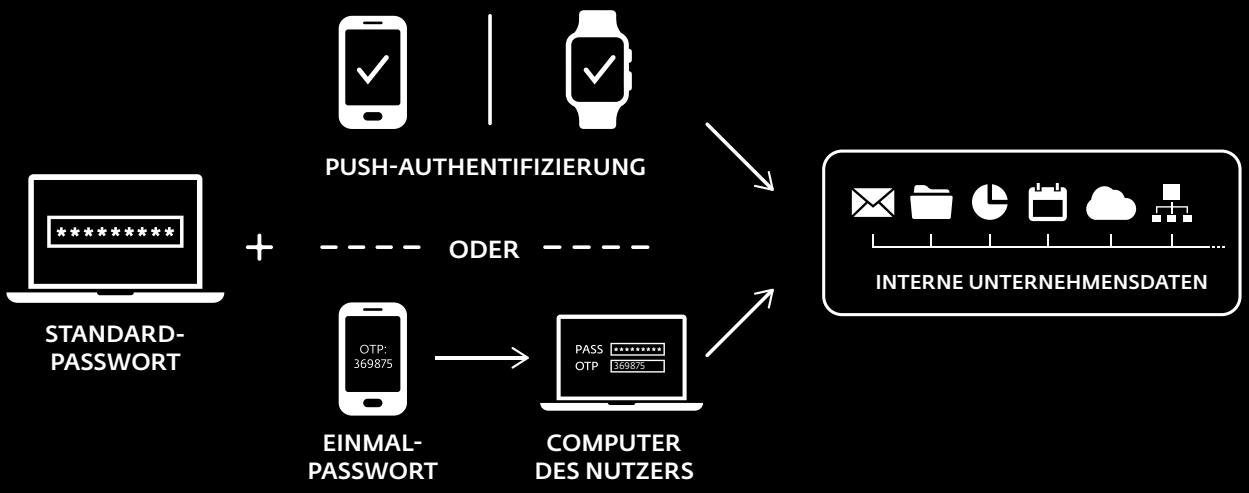
Vor allem Unternehmen, die mit Kreditkarteninformationen oder Gesundheitsdaten arbeiten, sind verpflichtet, den Schutz dieser Daten zu gewährleisten und entsprechende Maßnahmen vorzunehmen. Aber auch alle anderen Firmen sollten sorgfältig prüfen, ob bzw. an welche Datenschutzvorgaben sie gebunden sind.



Bei Nutzung einer Zwei-Faktor-Authentifizierung können Hacker Zugangsdaten nicht einfach erraten und entweder selbst verwenden oder zum Verkauf anbieten.

Nicht umsonst enthalten viele gesetzliche Vorgaben die Pflicht zu Multi-Faktor-Authentifizierung. Die meisten Datenlecks werden durch gestohlene oder schwache Passwörter verursacht.

Authentifizierung via Push-Benachrichtigung



ESET bietet einfach mehr

WÄHLEN SIE IHRE INTEGRATIONS-METHODE

ESET Secure Authentication bietet zwei verschiedene Integrationsmöglichkeiten. Innerhalb eines Windows-Netzwerks lässt sich die Lösung ins Active Directory integrieren, für Unternehmen ohne Windows-Domain steht der StandAlone-Modus bereit.

KEINE ZUSÄTZLICHE HARDWARE NÖTIG

ESET Secure Authentication erfordert keine zusätzliche Hardware. Nach der Installation der Anwendung auf Ihrem Server können Sie umgehend mit der Bereitstellung starten.

UNTERSTÜTZUNG ALLER GÄNGIGEN SMARTPHONES

Ihre Mitarbeiter können bereits eingesetzte Smartphones weiter nutzen. ESET Secure Authentication ist für die Verwendung auf allen iOS und Android Smartphones geeignet. Für noch mehr Schutz und Bedienkomfort kann die App mit den Geräte-eigenen biometrischen Verfahren (Touch ID, Face ID, Android Fingerprint) genutzt werden.

IN 10 MINUTEN EINSATZBEREIT

Bei der Entwicklung von ESET Secure Authentication haben wir darauf geachtet, die Installation so einfach wie möglich zu gestalten. Unabhängig von Ihrer Firmengröße beansprucht die Installation von ESET Secure Authentication dank der Möglichkeit, mehrere Nutzer gleichzeitig einzurichten, nur wenig Zeit.

EINSCHLIESSLICH SDK UND API

Zur individuellen Anpassung der Funktionalitäten stellen wir sowohl ein SDK als auch eine API bereit. So können Unternehmen ESET Secure Authentication nach ihrem Bedarf erweitern und die Nutzung auf eigene Anwendungen oder Webservices ausweiten.

PUSH-AUTHENTIFIZIERUNG

Bequeme Authentifizierung ohne Eingabe eines Einmal-Passworts über die Bestätigung einer Push-Benachrichtigung. Funktioniert auf iOS und Android Smartphones.

„Einfachste Installation, Setup und Integration ins Active Directory. Einer der größten Vorteile war für uns, dass unsere Mitarbeiter sich per App authentifizieren können und nicht andauernd SMS bekommen. Außerdem ließ es sich völlig unkompliziert in unser bestehendes VPN-Setup integrieren.“

— Tom Wright, IT Service Officer, Gardners Books

Use Cases

Datenlecks vermeiden

Immer wieder wird von Datenschutz-Vorfällen berichtet, bei denen Unternehmen Kunden nicht über Datenlecks informiert haben.

LÖSUNG

- ✓ Schützen Sie sensible Kommunikation wie z.B. das Remote Desktop Protokoll mithilfe der Multi-Faktor-Authentifizierung.
- ✓ Richten Sie für alle im Unternehmen verwendeten VPNs eine 2FA ein.
- ✓ Verwenden Sie 2FA, um den Zugriff auf Geräte mit sensiblen Daten einzuschränken.
- ✓ Schützen Sie sensible Unternehmensdaten mit ESET Endpoint Encryption.

ESET-PRODUKTE

- ✓ ESET Secure Authentication
- ✓ ESET Endpoint Encryption

Verstärkung für Passwörter

Nicht selten nutzen Mitarbeiter dieselben Passwörter für verschiedene Anwendungen und Webseiten. Für Unternehmen ein hohes Sicherheitsrisiko.

LÖSUNG

- ✓ Schützen Sie Unternehmensressourcen durch Multi-Faktor-Authentifizierung.
- ✓ Durch die Verwendung einer Multi-Faktor-Authentifizierung sind unsichere oder gestohlene Passwörter kein Problem mehr.

ESET PRODUKTE

- ✓ ESET Secure Authentication

Sichere Benutzerlogins

Oftmals werden in Unternehmen Rechner und Arbeitsplätze genutzt, an denen sich täglich viele unterschiedliche Nutzer anmelden.

LÖSUNG

- ✓ Mit einer Zwei-Faktor-Authentifizierung sind geteilte Rechner umfassend geschützt.

ESET-PRODUKTE

- ✓ ESET Secure Authentication

Technische Features und unterstützte Plattformen

PUSH-AUTHENTIFIZIERUNG

Authentifizierung über die Bestätigung einer Push-Benachrichtigung. Funktioniert mit iOS und Android Smartphones.

WEITERE AUTHENTIFIZIERUNGS-MÖGLICHKEITEN

ESET Secure Authentication unterstützt Push-Benachrichtigungen, die Bereitstellung von Einmal-Passwörtern über die mobile Client-App, SMS oder bestehende Hardware-Token sowie FIDO-basierte Sticks und individuelle Methoden.

REMOTE MANAGEMENT

Zentrale Verwaltung über die ESET Secure Authentication Web-Konsole. Die Lösung lässt sich problemlos in Ihr bestehendes Active Directory integrieren und funktioniert zudem unabhängig in Unternehmen ohne Windows-Domain.

ABGESICHERTE ZUGÄNGE

ESET Secure Authentication unterstützt VPNs, RDP und Outlook Web Access (OWA) ebenso wie VMWare Horizon View und RADIUS-basierte Services.

ZUSÄTZLICHER LOGIN-SCHUTZ

Desktop-Logins und privilegierte Zugänge können ebenfalls durch die MFA-Lösung geschützt werden. Unterstützt sowohl Windows als auch macOS und Linux.

CLOUD SUPPORT

Nutzen Sie die MFA zur Absicherung Ihrer Zugänge zu Diensten wie Google Apps, Office 365 und Dropbox. ESET unterstützt die Integration über das SAML-2 Protokoll, das viele Identity Provider einsetzen.

UNTERSTÜTZUNG VON TOKEN

Während die Nutzung von Hardware-Token nicht erforderlich ist, unterstützt die Lösung alle ereignisbasierten OATH-konformen HOTP/TOTP-Token sowie FIDO2 und FIDO U2F Hardware-Schlüssel.

UNTERSTÜTZTE VPNS

VMware Horizon View, Citrix XenApp, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall.

Über ESET

ESET wurde in Gartners Magic Quadrant for Endpoint Protection Platforms* 2019 zum „Challenger" gekürt.

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

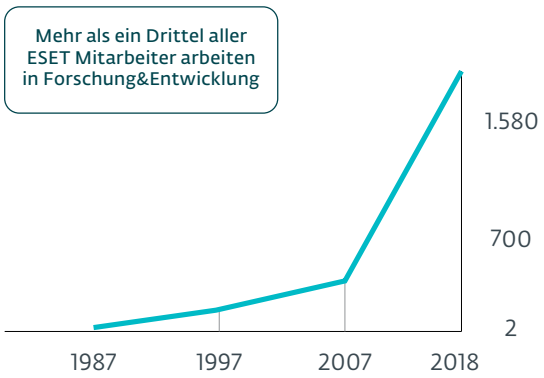
110+ Mio.
Nutzer weltweit

400k+
Business-kunden

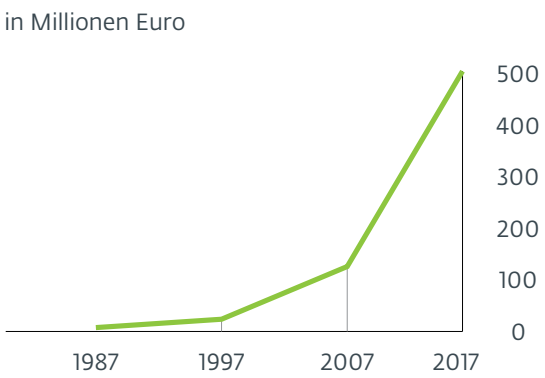
200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

ESET MITARBEITER



ESET ERLÖSE



*Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, 20. August 2019. 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

GOLD ENDPOINT PROTECTION PLATTFORMEN (EPP) SECURITY INSIDER AWARD 2019

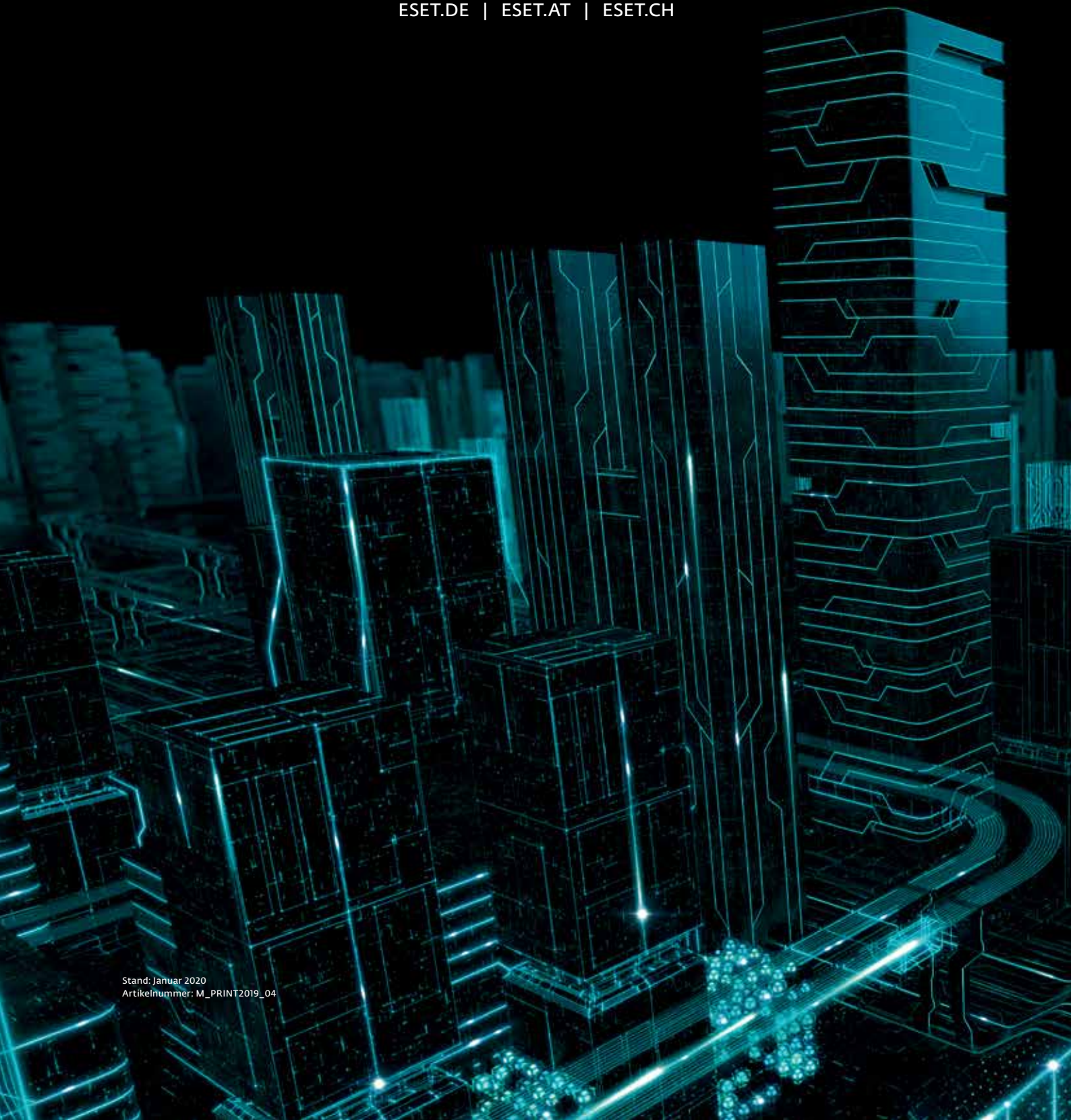
„Angesichts der guten Schutz- und Verwaltungs-Funktionen sowie der globalen Reichweite des Supports sollte ESET bei Ausschreibungen von großen Unternehmen für IT-Sicherheitslösungen immer in die engere Wahl genommen werden."

KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018

ENJOY SAFER TECHNOLOGY™

ESET.DE | ESET.AT | ESET.CH



Stand: Januar 2020
Artikelnummer: M_PRINT2019_04