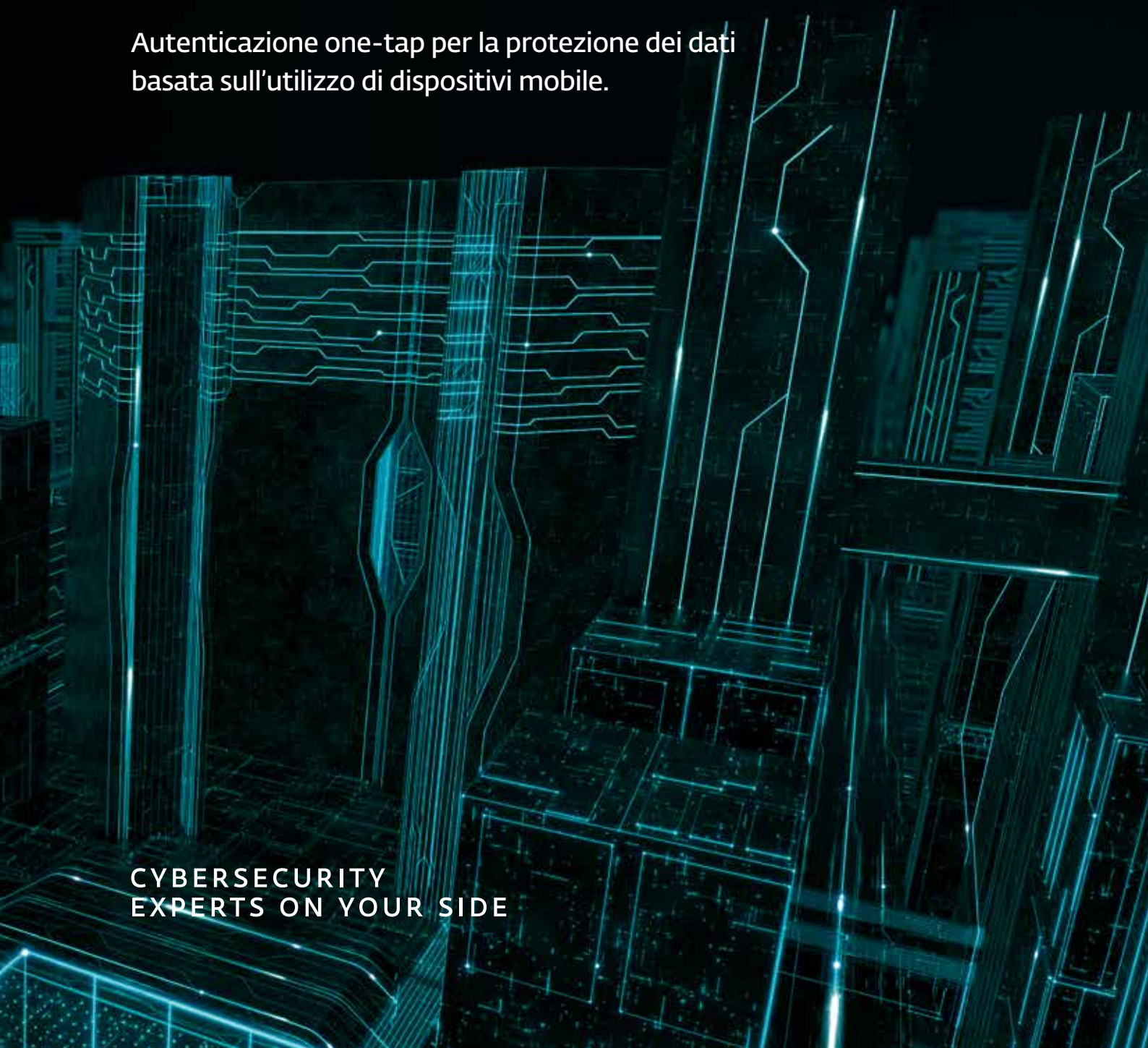
SOLUTION OVERVIEW

SECURE AUTHENTICATION

Autenticazione one-tap per la protezione dei dati basata sull'utilizzo di dispositivi mobile.



CYBERSECURITY
EXPERTS ON YOUR SIDE

Che cosa è un **prodotto di autenticazione multi-fattore?**

L'Autenticazione multi-fattore (MFA), nota anche come Autenticazione a due fattori (2FA), è un metodo che richiede due informazioni indipendenti per verificare l'identità di un utente. Consente quindi una autenticazione molto più forte della tradizionale password statica o dell'autenticazione tramite PIN. Integrando l'autenticazione tradizionale con un secondo fattore dinamico, riduce efficacemente il rischio di violazioni dei dati causate da password deboli o rubate.

ESET Secure Authentication fornisce un modo semplice, per le aziende di tutte le dimensioni, di implementare l'autenticazione multi-fattore sui sistemi comunemente utilizzati come VPN, Desktop remoto, Office 365, Outlook Web Access, l'accesso al sistema operativo e altro ancora.

Perché scegliere **l'Autenticazione a più fattori?**

Non solo i dipendenti utilizzano la stessa password su più siti Web e applicazioni, ma a volte le condividono liberamente con amici, familiari e colleghi di lavoro.

PASSWORD DEBOLI

Il proverbio dice, "i dipendenti sono il tuo anello più debole", in quanto possono mettere a rischio l'attività in diversi modi. Uno dei rischi maggiori è l'utilizzo di password deboli. Non solo i dipendenti utilizzano la stessa password su più siti Web e applicazioni, ma a volte le condividono liberamente con amici, familiari e colleghi di lavoro. Come se non bastasse, quando le aziende impongono criteri più stretti per la scelta delle password, di solito il dipendente utilizza varianti della propria password precedente o scrive la nuova su di un post-it.

Una soluzione di autenticazione a più fattori protegge l'azienda implementando, oltre alla normale password, una password aggiuntiva, ad es. generandola sul telefono del dipendente. In questo modo si impedisce ai malintenzionati di accedere ai propri sistemi semplicemente indovinando una password debole.

DATA BREACH

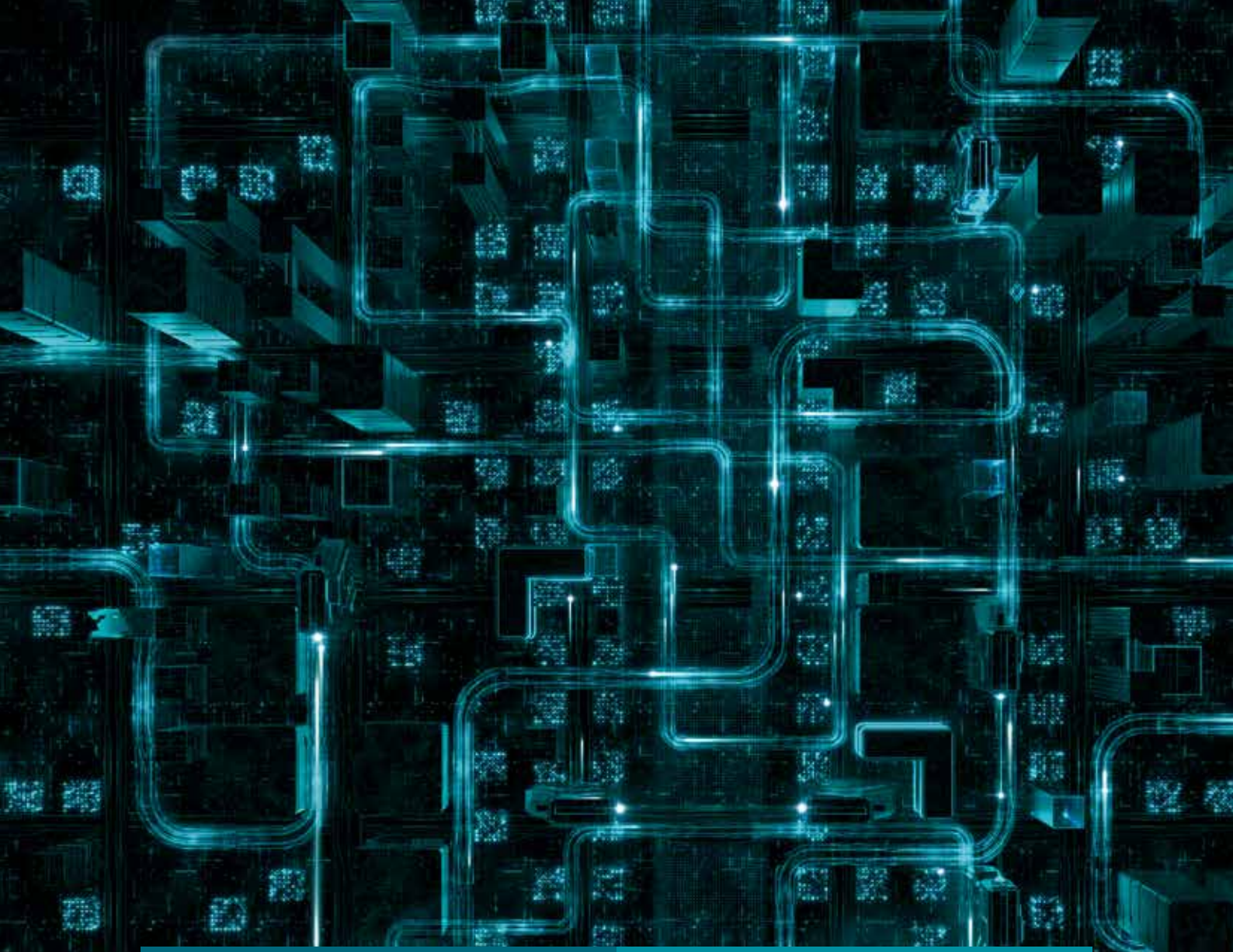
L'attuale panorama della cybersecurity presenta ogni giorno un numero crescente di violazioni dei dati. Uno dei modi più comuni con cui gli hacker accedono ai dati della vostra azienda è attraverso password deboli o rubate. Inoltre, per proteggere il normale accesso degli utenti ai servizi critici, le aziende possono implementare l'autenticazione a più fattori con livelli di privilegio crescenti per impedire gli accessi non autorizzati.

Aggiungendo una soluzione multi-fattore, le aziende rendono molto più difficile agli hacker l'accesso ai propri sistemi e, in ultima analisi, la loro compromissione. I settori principalmente colpiti dalle violazioni sono tradizionalmente quelli che trattano dati sensibili. Tuttavia ciò non significa che gli altri settori siano al sicuro, semplicemente gli hacker in genere si concentrano sui settori che ritengono più interessanti.

COMPLIANCE

Quando si tratta di compliance, la maggior parte delle aziende deve innanzitutto capire se la propria organizzazione rientra tra quelle interessate da una data conformità. Successivamente, deve esaminare i requisiti che la conformità raccomanda e imporre di implementarli. Oggigiorno sono molti i regolamenti e le leggi, come GDPR, PCI-DSS, HIPAA, SOX e GLBA, che richiedono che l'autenticazione a più fattori venga implementata.

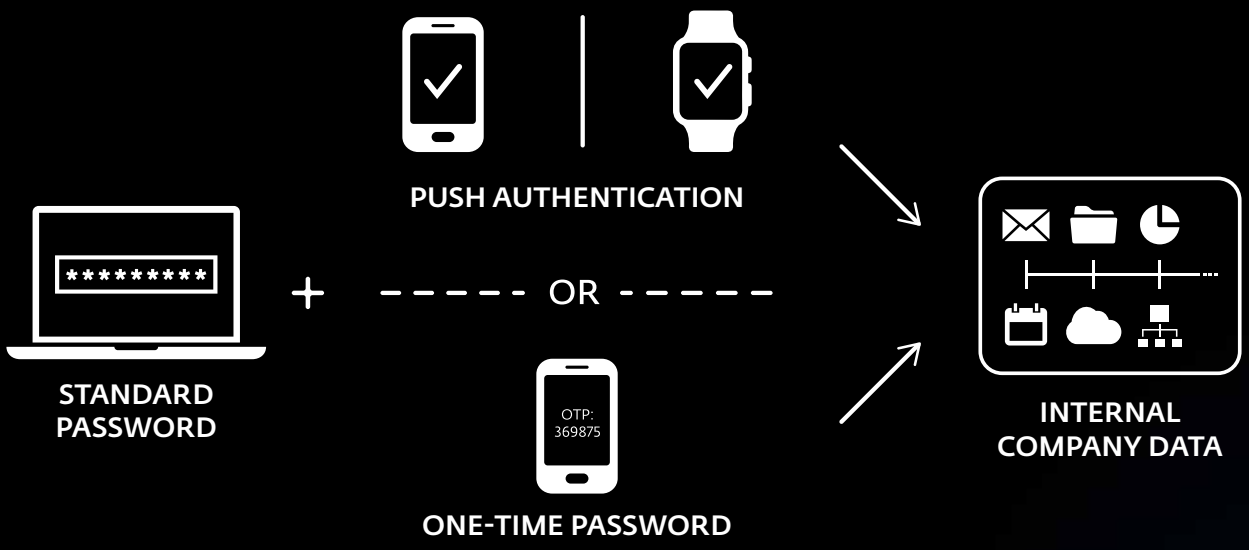
L'autenticazione a più fattori quindi non è più una soluzione opzionale ma, per la maggior parte delle aziende che gestisce carte di credito o informazioni sulla salute, è piuttosto una soluzione obbligatoria. Tutte le aziende dovrebbero effettuare una valutazione per capire se devono rispettare determinate conformità.



Uno dei modi più comuni con cui gli hacker possono accedere ai dati della tua azienda è attraverso password deboli o rubate.

L'utilizzo di questa soluzione impedisce agli aggressori di accedere ai tuoi sistemi semplicemente indovinando una password debole.

Autentica con un singolo tocco, senza bisogno di ridigitare la password monouso.



I punti di forza di ESET

SCEGLI IL METODO DI INTEGRAZIONE

ESET Secure Authentication è stata progettata per funzionare come soluzione indipendente, gestita tramite una console Web. In un ambiente di Dominio Windows, può integrarsi con Active Directory. Questo consente una installazione e configurazione semplice e veloce ed elimina la necessità di corsi di formazione per implementare l'autenticazione a due fattori nella propria organizzazione.

NON RICHIEDE HARDWARE DEDICATO

Tutti i costi di ESET Secure Authentication sono integrati poiché non richiede hardware dedicato. Basta installare l'applicazione da 10 MB su qualsiasi server e avviare il provisioning.

FUNZIONA CON TUTTI I TIPI DI SMARTPHONE

Non sono necessari token o dispositivi speciali per i dipendenti. ESET Secure Authentication funziona con tutti i tipi di smartphone.

SI INSTALLA IN 10 MINUTI

Molte ore di sviluppo sono state dedicate alla creazione di ESET Secure Authentication per garantire che l'installazione fosse il più semplice possibile. L'obiettivo era creare un'applicazione che una piccola azienda senza personale IT potesse installare e configurare. Indipendentemente dal fatto che un'azienda abbia 5 o 100.000 utenti, ESET Secure Authentication, grazie alla sua capacità di gestire più utenti contemporaneamente, riduce al minimo i tempi di installazione.

FULL SDK E API INCLUSI

Per le aziende più esigenti, includiamo un SDK completo e API che le imprese possono utilizzare per estendere la funzionalità in base alle proprie esigenze.

AUTENTICAZIONE PUSH

Autenticazione single-touch, senza bisogno di riscrivere la password monouso. Funziona su dispositivi iOS, Android e Windows 10 Mobile.

"Installazione su un unico server, facilità di configurazione, integrazione con Active Directory e, uno dei principali vantaggi, un'applicazione da fornire ai membri del nostro staff così da non dover scambiare SMS costanti. Inoltre, il fatto che funzioni perfettamente con la VPN aperta ci ha reso molto felici poiché non abbiamo dovuto modificare la nostra configurazione VPN per ospitare il software."

Tom Wright, IT Service Officer, Gardners Books

Casi pratici

Prevenzione data breach

Le aziende registrano ogni giorno una violazione dei dati e devono informarne i propri clienti.

SOLUZIONE

- ✓ Proteggere le comunicazioni vulnerabili, come il Desktop Remoto, aggiungendo l'autenticazione a due fattori.
- ✓ Aggiungere l'autenticazione a due fattori a tutte le VPN utilizzate.
- ✓ Richiedere l'autenticazione a due fattori per accedere ai dispositivi che contengono dati sensibili.
- ✓ Proteggere i dati sensibili con ESET Endpoint Encryption.

SOLUZIONI ESET CONSIGLIATE

- ✓ ESET Secure Authentication
- ✓ ESET Endpoint Encryption

Rafforzare la protezione delle password

Gli utenti utilizzano spesso le stesse password in più applicazioni e servizi Web mettendo a rischio la propria organizzazione.

SOLUZIONE

- ✓ Limitare l'accesso alle risorse aziendali sfruttando l'autenticazione a più fattori.
- ✓ L'installazione dell'autenticazione a più fattori riduce la preoccupazione associata alle password condivise o rubate richiedendo una OTP oltre a una password.

SOLUZIONI ESET CONSIGLIATE

- ✓ ESET Secure Authentication

Verifica del processo di login degli utenti

Le aziende utilizzano computer condivisi in aree di lavoro condivise. La verifica di tutti gli utenti che effettuano l'accesso durante la giornata lavorativa è fondamentale.

SOLUZIONE

- ✓ Implementare l'autenticazione a due fattori per gli accessi desktop su tutti i dispositivi in aree di lavoro condivise.

SOLUZIONI ESET CONSIGLIATE

- ✓ ESET Secure Authentication

Caratteristiche tecniche e piattaforme protette

AUTENTICAZIONE PUSH

Autenticazione single-touch tramite smartphone su dispositivi iOS, Android e Windows 10 Mobile.

COME AUTENTICARSI

ESET Secure Authentication supporta sia applicazioni mobile, notifiche push, token e SMS sia metodi personalizzati per la consegna di password monouso.

GESTIONE DA REMOTO

Avviene tramite la console Web ESET Secure Authentication o Microsoft Management Console (MMC). È possibile l'integrazione con Active Directory per una installazione e configurazione facile e veloce ma funziona anche autonomamente nei sistemi senza un dominio Windows.

MAGGIORE PROTEZIONE

Virtual Private Networks (VPN) aziendali, Protocollo Desktop Remoto (RDP), Outlook Web Access (OWA), VMware Horizon View e servizi basati su Radius sono tutti supportati nativamente da ESET Secure Authentication.

PROTEZIONE AGGIUNTIVA DEI SISTEMI OPERATIVI

ESET Secure Authentication fornisce protezione aggiuntiva per il login al desktop e per l'aumento dei privilegi di accesso attraverso l'autenticazione a più fattori. Supporta Windows, macOS e Linux.

SUPPORTO PER SERVIZI CLOUD

Oltre alle applicazioni on-premise, ESET Secure Authentication supporta anche servizi Web/Cloud come Google Apps e Microsoft ADFS 3.0 (incluso Office 365).

SUPPORTO PER HARD TOKEN

Anche se i token hardware non sono richiesti, tutti gli HOTP token basati su eventi che sono OATH-compliant sono supportati, come sono supportate le hardware key che utilizzano i protocolli FIDO2 e FIDO U2F.

VPN SUPPORTATE

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

Informazioni su ESET

ESET – uno dei principali produttori di software per la sicurezza digitale - è stato riconosciuto come unico Challenger nel Gartner Magic Quadrant 2018 per le piattaforme di protezione degli endpoint.*

Per oltre 30 anni, ESET® ha sviluppato software e servizi di sicurezza IT tra i migliori del settore, offrendo soluzioni di protezione immediate e complete contro le minacce di cybersecurity per aziende e consumatori di tutto il mondo. ESET è un'azienda privata senza debiti e senza prestiti, per questo motivo abbiamo la libertà di fare ciò che deve essere fatto per la massima protezione di tutti i nostri clienti.

ESET IN NUMERI

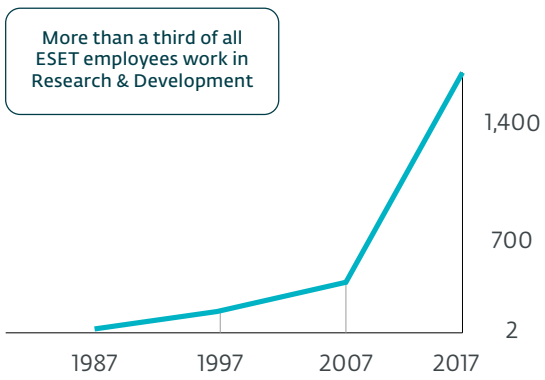
110m+
utenti nel mondo

400k+
clienti aziendali

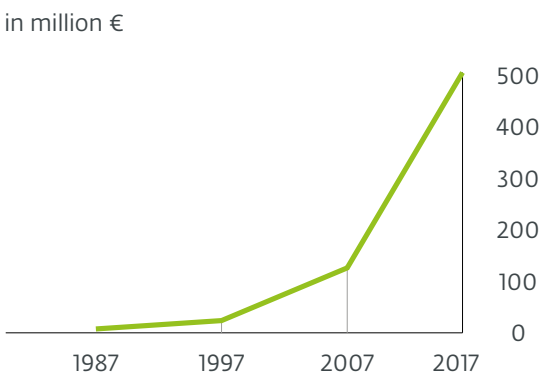
200+
paesi & territori

13
centri R&D globali

DIPENDENTI ESET



FATTURATO ESET



*Gartner non sostiene alcun fornitore, prodotto o servizio citato nelle sue pubblicazioni di ricerca. Le pubblicazioni di ricerca di Gartner sono costituite dalle opinioni dell'organizzazione di ricerca di Gartner e non devono essere interpretate come dati di fatto. Gartner non rilascia alcuna garanzia, espressa o implicita, in relazione a questa ricerca, comprese eventuali garanzie di commerciabilità o idoneità per uno scopo particolare.

ALCUNI DEI NOSTRI CLIENTI

HONDA

protetti da ESET dal 2011

licenze prolungate 3x, ampliate 2x

GREENPEACE

protetti da ESET dal 2008

licenze prolungate/ampliate 10x

Canon

protetti da ESET dal 2016

più di 14.000 endpoint

T . .

Partner di sicurezza ISP dal 2008

2 millioni di customer base

I PREMI PIÙ IMPORTANTI

SE Labs AAA ENTERPRISE ENDPOINT OCT-DEC 2016

THE CHANNEL CO. CRN ★★★★★ PARTNER PROGRAM GUIDE WINNER 2017

AV comparatives Approved Business Product 2017

SC MEDIA RECOMMENDED

"Date le buone funzionalità anti-malware e quelle legate alla gestione dei prodotti, senza dimenticare la portata globale di clienti e il supporto fornito, ESET dovrebbe essere nella lista da prendere in considerazione nelle RFP aziendali per le soluzioni anti-malware."

KuppingerCole Leadership Compass
Enterprise Endpoint Security: Anti-Malware Solutions, 2018

ENJOY SAFER TECHNOLOGY™