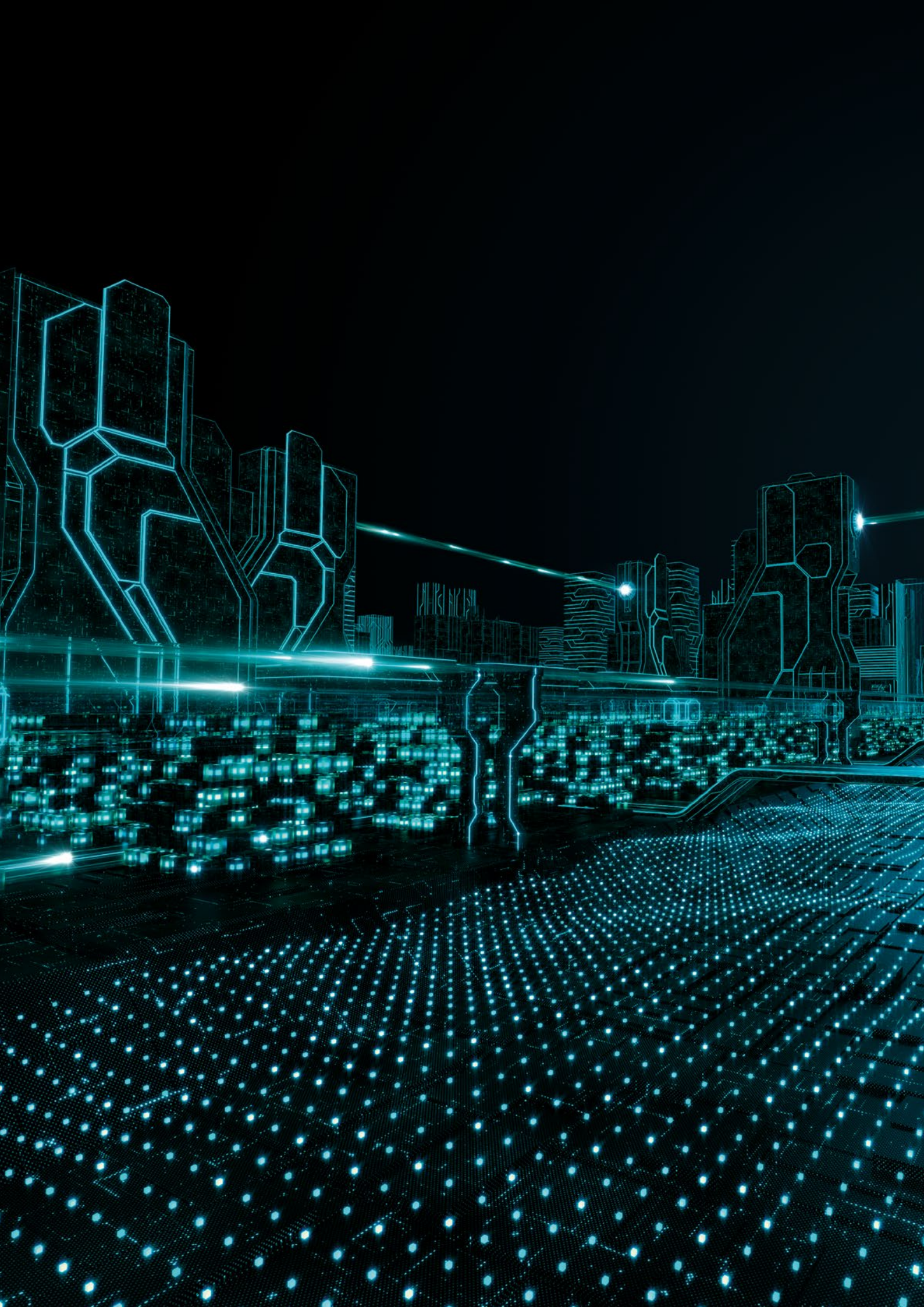
SECURE AUTHENTICATION

Rozwiązanie do dwuskładnikowego uwierzytelniania z wykorzystaniem telefonu komórkowego. Pomaga zagwarantować danym należyty poziom ochrony, zgodny z obowiązującymi przepisami prawa.

CYBERSECURITY
EXPERTS ON YOUR SIDE



Czym jest **uwierzytelnianie wieloskładnikowe?**

Uwierzytelnianie wieloskładnikowe (Multi-Factor Authentication – MFA), nazywane także uwierzytelnianiem dwuskładnikowym (Two-Factor Authentication – 2FA) to metoda uwierzytelniania wymagająca podania dwóch niezależnych informacji w celu weryfikacji tożsamości użytkownika. Uwierzytelnianie dwuskładnikowe zapewnia o wiele silniejszą ochronę niż tradycyjne hasło statyczne lub kod PIN. Dodanie do tradycyjnego sposobu autoryzacji drugiego, dynamicznego składnika skutecznie ogranicza ryzyko naruszenia zabezpieczeń powodowanych przez używanie słabych haseł lub ich wyciek.

ESET Secure Authentication to proste w obsłudze rozwiązanie pozwalające wdrożyć w firmie, niezależnie od jej wielkości, uwierzytelnianie wieloskładnikowe na etapie logowania do m.in. sieci VPN, pulpitów zdalnych, Office 365, Outlook Web Access czy systemu operacyjnego.

Dlaczego warto korzystać **z uwierzytelniania wieloskładnikowego?**

Pracownicy nie tylko często używają tego samego hasła na różnych stronach internetowych i aplikacjach, ale też czasem udostępniają je znajomym, rodzinie lub współpracownikom.

ZŁE NAWYKI DOTYCZĄCE HASEŁ

Mówi się, że „pracownicy są najsłabszym ogniwem firmy", ponieważ to zwykle oni narażają przedsiębiorstwo na różnego rodzaju niebezpieczeństwa. Jednym z największych zagrożeń są złe nawyki dotyczące haseł. Pracownicy nie tylko często używają tego samego hasła na różnych stronach internetowych i aplikacjach, ale też zdarza się, że udostępniają je znajomym, rodzinie i współpracownikom. Jakby tego było mało, gdy firma próbuje wdrożyć konkretne zasady dotyczące haseł, pracownicy wymyślają nowe warianty dotychczasowych haseł lub zapisują je na samoprzylepnych karteczkach.

Uwierzytelnianie wieloskładnikowe chroni firmę przed skutkami takich sytuacji poprzez wprowadzenie dodatkowego hasła, np. generowanego za pomocą telefonu pracownika. Takie rozwiązanie uniemożliwia niepowołanym osobom uzyskanie dostępu do Twojej sieci lub danych.

NARUSZENIA ZABEZPIECZEŃ DANYCH

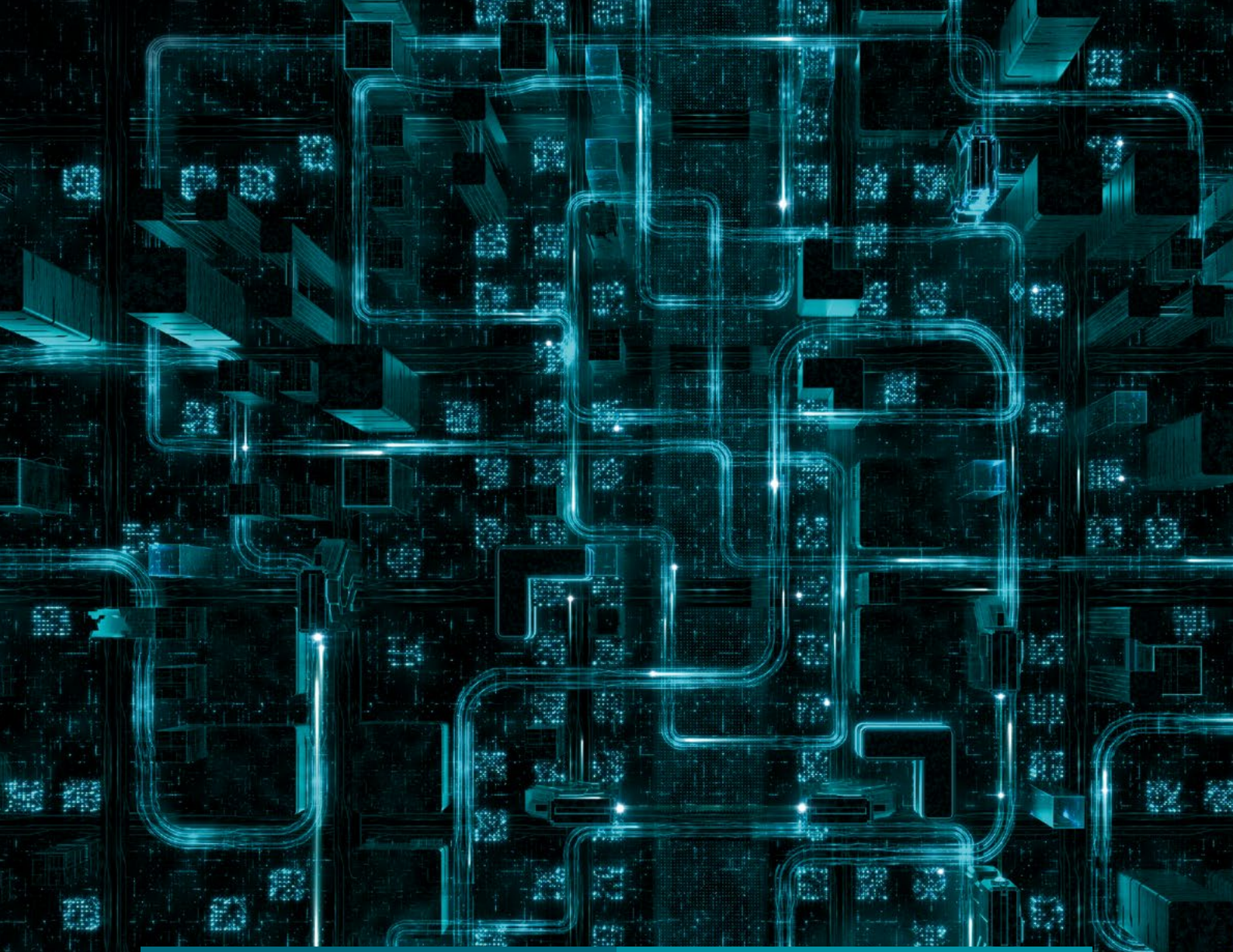
W dzisiejszych czasach rośnie liczba przypadków naruszenia bezpieczeństwa danych. Hakerzy uzyskują dostęp do ważnych dla firmy informacji zwykle poprzez kradzież lub przełamanie słabych haseł zabezpieczających. Firmy mogą jednak zapobiegać nieuprawnionemu dostępowi do danych czy to przez osoby niepowołane, czy też przez pracowników nieposiadających odpowiednich uprawnień, stosując uwierzytelnianie wieloskładnikowe.

Wdrożenie takiego rozwiązania znacząco utrudnia możliwość uzyskanie dostępu do sieci firmowej i danych w niej zgromadzonych. Warto dodać, że szczególnie podatne na ataki są obecnie firmy działające w branżach wymagających przetwarzania cennych danych, takie jak przedsiębiorstwa branży finansowej, handlowej, instytucje ochrony zdrowia oraz sektora publicznego.

ZGODNOŚĆ Z PRZEPISAMI

W przypadku zgodności z przepisami firmy powinny przede wszystkim wiedzieć, które przepisy są dla nich obowiązujące. Następnie muszą zapoznać się z wymogami i zaleceniami oraz wdrożyć je. Stosowanie uwierzytelniania wieloskładnikowego jest obecnie wymagane przez kilka norm, m.in. PCI-DSS czy GLBA, a większość przepisów, takich jak RODO i HIPAA, zwraca uwagę na potrzebę stosowania silniejszych rozwiązań w zakresie uwierzytelniania użytkownika.

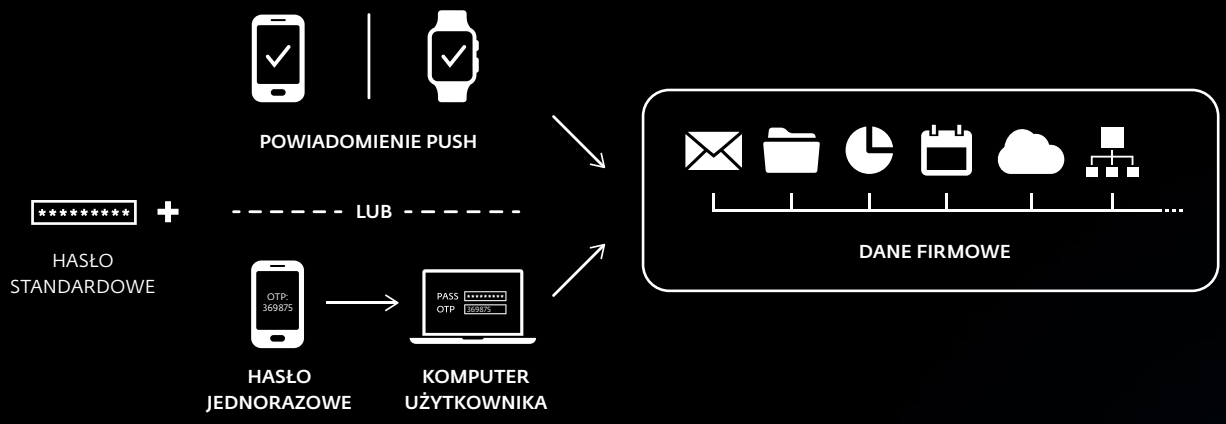
Dla większości firm obsługujących karty kredytowe i transakcje finansowe uwierzytelnianie wieloskładnikowe to już nie kwestia wyboru, a konieczności. Każde przedsiębiorstwo powinno przeanalizować, czy aktualne przepisy nie wymagają od niego stosowania konkretnych zabezpieczeń.



Kradzież lub przełamywanie słabych haseł to jedne z najczęściej stosowanych przez hakerów metod.

Stosowanie wieloskładniowego uwierzytelniania uniemożliwia niepowołanym osobom uzyskanie dostępu do Twojej sieci lub danych.

Szybkie uwierzytelnianie, bez konieczności ponownego wpisywania hasła jednorazowego.



Skuteczność ESET

WYBIERZ SPOSÓB INTEGRACJI

Oprogramowanie ESET Secure Authentication zostało zaprojektowane jako samodzielne rozwiązanie obsługiwane za pomocą webowej konsoli zarządzającej. Rozwiązanie pozwala na integrację z usługą Active Directory, co ułatwia i przyspiesza instalację i konfigurację ESET Secure Authentication w firmie oraz zapobiega konieczności dodatkowego szkolenia pracowników w zakresie korzystania z uwierzytelniania dwuskładnikowego.

BRAK KONIECZNOŚCI POSIADANIA SPECJALNEGO SPRZĘTU

Ponieważ ESET Secure Authentication nie wymaga użycia dodatkowego sprzętu, jego wdrożenie nie generuje dodatkowych kosztów. Wystarczy zainstalować na serwerze aplikację o rozmiarze 10MB i zacząć korzystać z rozwiązania.

KOMPATYBILNOŚĆ Z DOSTĘPNYMI NA RYNKU SMARTFONAMI

Pracownicy nie muszą posiadać specjalnych tokenów i urządzeń. Rozwiązanie ESET Secure Authentication jest kompatybilne z niemal wszystkimi dostępnymi na rynku smartfonami.

KONFIGURACJA W 10 MINUT

Twórcy rozwiązania ESET Secure Authentication spędzili wiele godzin, dopracowując je tak, aby jego konfiguracja była możliwie najłatwiejsza. Naszym celem było opracowanie aplikacji, której instalacja i konfiguracja będzie możliwa nawet w małej firmie bez działu IT. Konfiguracja rozwiązania ESET Secure Authentication jest tak samo szybka w przedsiębiorstwie zatrudniającym pięć oraz 100 000 pracowników.

PEŁNE SDK I API W ZESTAWIE

Z myślą o przedsiębiorstwach pragnących rozszerzyć funkcjonalność rozwiązania ESET Secure Authentication udostępniamy pełny zestaw narzędzi dla programistów i interfejs programowania aplikacji.

POWIADOMIENIA PUSH

Umożliwia szybkie uwierzytelnianie, bez konieczności ponownego wpisywania hasła jednorazowego. Rozwiązanie jest kompatybilne z telefonami z systemem i OS, Android i Windows 10 Mobile.

"Jednorazowa instalacja, łatwość konfiguracji, integracja z usługą Active Directory i, co bardzo istotne, możliwość udostępnienia aplikacji pracownikom eliminująca konieczność ciągłego wysyłania wiadomość SMS. Ponadto bardzo ucieszyła nas bezproblemowa współpraca z oprogramowaniem OpenVPN, dzięki której nie musieliśmy zmieniać dotychczasowej konfiguracji w związku z wdrożeniem nowego rozwiązania."

Tom Wright, IT Service Officer, Gardners Books

Przykładowe zastosowania

Zapobieganie kradzieży danych

Każdego dnia jakaś firma informuje swoich klientów o zaistniałym naruszeniu bezpieczeństwa danych.

ROZWIĄZANIE

- ✓ Ochrona podatnych na ataki kanałów łączności, np. połączeń pulpitu zdalnego, poprzez dodanie uwierzytelniania wieloskładnikowego.
- ✓ Korzystanie z uwierzytelniania wieloskładnikowego dla wszystkich połączeń VPN.
- ✓ Wymóg stosowania uwierzytelniania wieloskładnikowego podczas logowania na urządzenia zawierające wrażliwe dane.
- ✓ Ochrona wrażliwych danych za pomocą rozwiązania ESET Endpoint Encryption.

PRODUKTY ESET

- ✓ ESET Secure Authentication
- ✓ ESET Endpoint Encryption

Weryfikacja procesu logowania użytkownika

Z komputerów dostępnych w biurze każdego dnia korzystają naprzemiennie różni pracownicy firmy. Dostęp do komputera i swoich danych pracownik uzyskuje po zalogowaniu na danej maszynie.

ROZWIĄZANIE

- ✓ Wdrożenie uwierzytelniania wieloskładnikowego na wszystkich urządzeniach w biurze.

PRODUKTY ESET

- ✓ ESET Secure Authentication

Silniejsza ochrona za pomocą hasła

Użytkownicy korzystają z tych samych haseł w różnych aplikacjach i stronach internetowych, co może narazić firmę na niebezpieczeństwo.

ROZWIĄZANIE

- ✓ Możliwość ograniczenia dostępu do zasobów firmy poprzez wykorzystanie uwierzytelniania wieloskładnikowego.
- ✓ Ograniczenie ryzyka związanego z udostępnieniem lub kradzieżą hasła poprzez wprowadzenie dodatkowego składnika uwierzytelniania, np. powiadomienia push.

PRODUKTY ESET

- ✓ ESET Secure Authentication

Właściwości techniczne i chronione platformy

UWIERZYTELNIANIE PUSH

Proste rozwiązanie kompatybilne z wszystkimi telefonami z systemem iOS i Android.

INNE METODY UWIERZYTELNIANIA

ESET Secure Authentication może dostarczać hasło jednorazowe za pośrednictwem aplikacji mobilnej, powiadomień push, tokenów sprzętowych, wiadomości SMS, a także kluczy FIDO i innych niestandardowych rozwiązań.

ZDALNE ZARZĄDZANIE

Rozwiązaniem można zarządzać za pośrednictwem konsoli webowej. Istnieje możliwość integracji z usługą Active Directory w celu ułatwienia zarządzania oraz opcja samodzielnej pracy dla organizacji niekorzystających z domeny systemu Windows

OBSŁUGA ZABEZPIECZEŃ

ESET Secure Authentication natywnie wspiera wirtualne sieci prywatne (VPN), protokół pulpitu zdalnego (RDP), Outlook Web Access (OWA), VMware Horizon View oraz usługi oparte na protokole RADIUS.

DODATKOWA OCHRONA SYSTEMU OPERACYJNEGO

Funkcja uwierzytelniania wieloskładnikowego umożliwia dodatkową weryfikację użytkowników podczas logowania się do systemu operacyjnego oraz chroni przed eskalacją uprawnień.

Rozwiązanie współpracuje z systemami Windows, macOS i Linux.

OBSŁUGA ROZWIĄZAŃ W CHMURZE

Możliwość dodania wieloskładnikowego uwierzytelniania usług Google Apps, Office 365, Dropbox i wielu innych. ESET oferuje integrację za pośrednictwem protokołu SAML-2 wykorzystywaną przez wielu dostawców tożsamości.

OBSŁUGA TOKENÓW SPRZĘTOWYCH

Choć korzystanie z tokenów sprzętowych nie jest wymagane, rozwiązanie obsługuje wszystkie zgodne z OATH tokeny HOTP działające w oparciu na zdarzeniach, a także klucze sprzętowe FIDO2 i FIDO U2F.

WSPIERANE ROZWIĄZANIA VDI I VPN

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, Stormshield.

.

O ESET

ESET jest globalnym dostawcą oprogramowania zabezpieczającego komputery firm oraz użytkowników indywidualnych, któremu zaufało ponad 5 milionów Polaków i ponad 110 milionów osób na świecie. Producent został uznany jedynym Challengerem w raporcie Gartner Magic Quadrant dwa lata z rzędu[1].

Od ponad 30 lat ESET w swoich centrach badawczo-rozwojowych, m.in. od ponad dekady w Krakowie, rozwija najlepsze w branży oprogramowanie i usługi bezpieczeństwa informatycznego, dostarczając firmom i użytkownikom indywidualnym kompleksowe rozwiązania do ochrony przed stale ewoluującymi zagrożeniami.

ESET jest firmą o wysokiej płynności finansowej, od początku pozostającą w rękach prywatnych przedsiębiorców. Dzięki temu ESET ma pełną swobodę działania i może zapewnić najlepszą ochronę wszystkim swoim klientom.

Produkty ESET dostępne są w ponad 200 krajach świata. W Polsce za dystrybucję rozwiązań ESET odpowiada firma DAGMA.

ESET W LICZBACH

110 mln+
użytkowników na całym świecie

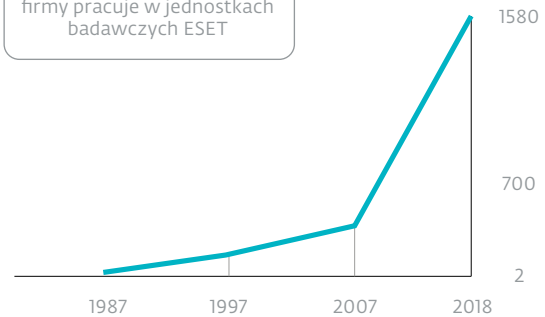
5 mln+
użytkowników w Polsce

400 tys.+
klientów biznesowych

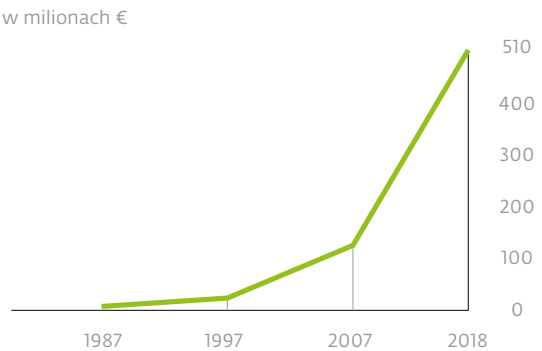
13
centrów badawczo-rozwojowych

PRACOWNICY ESET

Więcej niż 1/3 pracowników firmy pracuje w jednostkach badawczych ESET



PRZYCHODY ESET



[1] Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, 20 sierpnia 2019. Gartner nie promuje żadnego sprzedawcy, produktu ani usług przedstawionych w publikacjach badawczych. Publikacje badawcze Gartnera zawierają opinie organizacji badawczej Gartnera i nie powinny być interpretowane jako stwierdzenia faktów. Gartner zrzeka się wszelkich gwarancji wyrażonych lub domniemanych, w odniesieniu do tych badan, w tym wszelkich gwarancji przydatności handlowej lub jakości do określonego celu.

WYBRANI KLIENCI

MITSUBISHI MOTORS
Drive your Ambition

Od 2017 roku ESET chroni ponad 14000 stanowisk.

Canon
Canon Marketing Japan Group

Od 2016 roku ESET chroni ponad 9000 stanowisk.

Allianz Suisse

Od 2016 roku ESET chroni ponad 4000 kont pocztowych.

T-Mobile jest partnerem ISP od 2008 roku. W swojej bazie posiada 2 mln klientów.

WYBRANE NAGRODY

AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS 10/2019 av-test.org

CRN

AV comparatives APPROVED Business Security JUL 2019

PRODUKT ROKU 2019 WYBÓR CZYTELNIKÓW IT professional

"Biorąc pod uwagę cechy produktu, zarówno w zakresie ochrony przed złośliwym oprogramowaniem, możliwościami zarządzania, jak również w zakresie globalnego zasięgu klientów i wsparcia technicznego, ESET powinien być brany pod uwagę w zapytaniach ofertowych i przetargach dotyczących wdrożenia rozwiązań antywirusowych."

Tom Wright, IT Service Officer, Gardners Books

ENJOY SAFER TECHNOLOGY™