OVERVIEW

SECURE AUTHENTICATION

Potężne uwierzytelnianie wieloskładnikowe
dla bezpiecznego dostępu do sieci i danych

Progress. Protected.

Na czym polega **uwierzytelnianie wieloskładnikowe?**

Uwierzytelnianie wieloskładnikowe (MFA), w tym również uwierzytelnianie dwuskładnikowe (2FA), wymaga dwóch niezależnych informacji w celu zweryfikowania tożsamości użytkownika. MFA jest znacznie silniejsze niż użycie tradycyjnego, statycznego hasła lub uwierzytelniania, używając kodu PIN. Uzupełniając tradycyjne uwierzytelnianie o dynamiczny drugi czynnik, skutecznie zmniejsza ryzyko naruszenia bezpieczeństwa danych spowodowanego słabymi lub przejętymi hasłami.

ESET Secure Authentication zapewnia firmom każdej wielkości łatwy sposób na wdrożenie MFA w powszechnie wykorzystywanych systemach i narzędziach takich jak VPN, RDP, Outlook Web Access, logowanie do systemu operacyjnego i nie tylko.

Zapobiegaj naruszeniom danych i chroń zasoby swojej firmy

Uwierzytelnianie wieloskładnikowe może pomóc zrównoważyć ryzyko ataku „credential stuffing" – ataku wykorzystującego skompromitowane informacje o pracownikach. Ryzyko to jest powodowane przez osoby, które:

- Używają tego samego hasła w różnych aplikacjach i witrynach
- Udostępniają hasła osobom postronnym
- Podczas aktualizacji hasła dokonują jedynie drobnych zmian

SŁABA HIGIENA HASEŁ

Dane są jednym z najważniejszych aktywów Twojej firmy. Pracownicy mogą jednak narażać je na wiele sposobów. Jednym z największych zagrożeń jest zła higiena haseł. Pracownicy nie tylko używają identycznych haseł w różnych portalach i aplikacjach, ale czasami swobodnie dzielą się swoimi hasłami z przyjaciółmi, rodziną i współpracownikami. Poza tym, gdy firmy egzekwują polityki haseł, ich pracownicy używają często wyłącznie wariantów poprzednio wykorzystywanego hasła lub zapisują swoje poświadczenia na karteczkach samoprzylepnych.

Rozwiązanie umożliwiające wieloskładnikowe uwierzytelnianie chroni firmę przed nieprawidłową higieną haseł poprzez wdrożenie, oprócz standardowego hasła, dodatkowego elementu uwierzytelniającego – np. kodu jednorazowego generowanego na telefonie służbowym pracownika.

Wdrożenie rozwiązania tego rodzaju minimalizuje ryzyko uzyskania przez atakujących dostępu do Twoich systemów poprzez przejęcie słabych haseł lub wykorzystanie naruszonych danych uwierzytelniających pracownika.

NARUSZENIA DANYCH

W dzisiejszym cyfrowym świecie codziennie dochodzi do coraz większej liczby naruszeń bezpieczeństwa danych. Jednym z najczęstszych sposobów, w jaki hakerzy mogą uzyskać dostęp do danych Twojej firmy, są słabe lub przejęte hasła zebrane za pomocą automatycznych botów, ataków phishing lub ukierunkowanych. Oprócz samej ochrony logowań zwykłych użytkowników do krytycznych usług, firmy mogą wdrożyć MFA przy wszystkich eskalacjach uprawnień, aby zapobiec nieautoryzowanemu dostępowi administracyjnemu.

Dodając rozwiązanie uwierzytelniania wieloskładnikowego, Twoja firma znacznie utrudni hakerom uzyskanie dostępu do systemów i ostatecznie złamanie ich zabezpieczeń. Branże, w których najczęściej dochodzi do naruszeń danych, to tradycyjnie te, które przetwarzają cenne dane, takie jak finanse, handel detaliczny, opieka zdrowotna i sektor usług publicznych. Nie oznacza to jednak, że inne branże są bezpieczne. Po prostu hakerzy zazwyczaj przeliczają wymagany wysiłek na jego opłacalność.

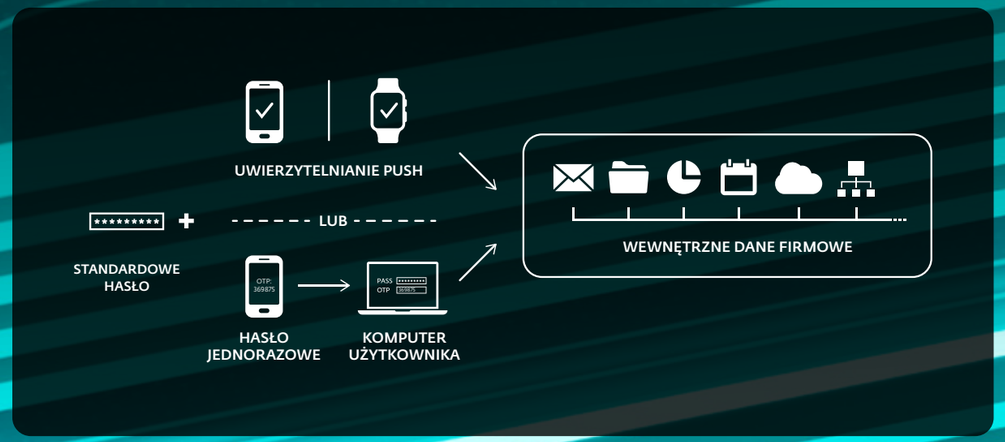
SPEŁNIANIE NORM I PRZEPISÓW

W pierwszej kolejności firma powinna rozważyć czy konieczne jest zapewnienie zgodności z przepisami czy też nie. Następnie muszą zweryfikować, jakie środki i zalecenia powinny wdrożyć, aby spełnić określone wymagania. Jeśli chodzi o uwierzytelnianie wieloskładnikowe, kilka przepisów, takich jak PCI-DSS i GLBA, wymaga jego wdrożenia, a wiele przepisów, w tym RODO i HIPAA, podkreśla potrzebę silniejszego uwierzytelniania.

Uwierzytelnianie wieloskładnikowe nie jest już tylko opcją dla większości firm obsługujących karty kredytowe lub transakcje finansowe, ale raczej wymaganym rozwiązaniem. Wszystkie przedsiębiorstwa powinny sprawdzić, które przepisy i regulacje ich dotyczą, i upewnić się, że spełniają ich wymagania.

Digital Security
Progress. Protected.

Uwierzytelnianie jednym dotknięciem, bez konieczności wprowadzania hasła jednorazowego.



Poczuj różnicę z ESET

UWIERZYTELNIANIE PUSH

Umożliwia uwierzytelnianie jednym kliknięciem, bez konieczności wprowadzania hasła jednorazowego. Współpracuje ze smartfonami iOS i Android.

CHROŃ APLIKACJE W CHMURZE

Dodaj MFA, aby wzmocnić dostęp do usług takich jak Google Apps, Dropbox i wielu innych. ESET obsługuje integrację za pośrednictwem protokołu SAML-2 używanego przez głównych dostawców usług uwierzytelniania.

KONFIGURACJA W 10 MINUT

Ciężko pracowaliśmy, abyś Ty mógł odetchnąć. Postanowiliśmy stworzyć rozwiązanie, które nawet mała firma nieposiadająca dedykowanego zespołu IT byłaby w stanie wdrożyć i skonfigurować. Niezależnie od tego, czy Twoja firma ma dziesiątki, czy tysiące użytkowników, rozwiązanie ESET Secure Authentication, dzięki możliwości konfiguracji uwierzytelniania dla wielu użytkowników jednocześnie, skraca czas wdrożenia do minimum.

WIELE SPOSOBÓW UWIERZYTELNIANIA

Nie ma potrzeby stosowania specjalnych tokenów ani urządzeń dla pracowników. ESET Secure Authentication działa płynnie na smartfonach, posiada zabezpieczenie kodem PIN dla większego bezpieczeństwa i umożliwia integrację z mechanizmem danych biometrycznych urządzenia (Touch ID, Face ID, odcisk palca) w celu zwiększenia bezpieczeństwa i poprawy komfortu użytkowania. W razie potrzeby obsługujemy również tokeny sprzętowe i klucze FIDO.

NIE POTRZEBA DEDYKOWANEGO SPRZĘTU

Wymagania dotyczące zasobów dla narzędzia ESET Secure Authentication są minimalne – możesz korzystać z wersji hostowanej w chmurze, dzięki czemu nie będziesz potrzebował dedykowanego serwera. Jednocześnie rozwiązanie oferuje możliwość wdrożenia lokalnie.

BEZPROBLEMOWA INTEGRACJA

Rozwiązanie oferuje dwa tryby integracji – z Active Directory dla organizacji wykorzystujących domenę Windows lub tryb autonomiczny, odpowiedni dla tych, które jej nie posiadają. Tak czy inaczej, wdrożenie i konfiguracja są łatwe i szybkie, a wszystkim można zarządzać za pomocą hostowanej w chmurze konsoli.

WSPARCIE DLA WIELU DZIERŻAW

Hostowana w chmurze wersja ESET Secure Authentication została zaprojektowana tak, aby zarządzać wieloma dzierżawami, dzięki czemu dostawcy usług zarządzania mogą administrować wieloma firmami swoich klientów, oferując elastyczność definiowania ustawień dla poszczególnych grup użytkowników.

OBSŁUGA VDIS I VPN

Możliwość integracji z rozwiązaniami VMware Horizon View, Citrix XenApp, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet, FortiGate, Juniper, Palo Alto i SonicWall. Wspierane są wszystkie rodzaje niestandardowej integracji z usługami VPN używających protokołu RADIUS.

ZAWIERA API I SDK

Dla organizacji, które chcą jeszcze więcej, udostępniliśmy pełne API i SDK, za pomocą których klienci mogą rozszerzyć MFA na aplikacje i platformy, z których korzystają – nawet bez dedykowanej wtyczki.

eset® Digital Security
Progress. Protected.

Przykłady użycia

Ochrona wielu lokacji

PROBLEM

Dostawca usług MSP musi obsługiwać kilka oddziałów lub różne firmy posiadające inne polityki bezpieczeństwa i konfiguracje środowiska.

ROZWIĄZANIE

- ✓ Utwórz każdą firmę jako lokację w ESET PROTECT Hub i przypisz jej określoną liczbę licencji na rozwiązanie ESET Secure Authentication. Po ponownym zalogowaniu do konsoli zobaczysz w menu dedykowaną sekcję dla utworzonej firmy.
- ✓ Obsługa wielu dzierżaw hostowana w chmurze, która nie wymaga wykorzystywania lokalnego sprzętu, pozwala na obsługę uwierzytelniania wieloskładnikowego dla różnych firm lub oddziałów.

Zapobiegaj naruszeniom

PROBLEM

Firmy pojawiają się w wiadomościach każdego dnia, aby ostrzec swoich klientów o wystąpieniu naruszenia bezpieczeństwa danych.

ROZWIĄZANIE

- ✓ Chroń wrażliwą komunikację, taką jak RDP, dodając do niej uwierzytelnianie wieloskładnikowe.
- ✓ Dodaj uwierzytelnianie wieloskładnikowe do wszystkich używanych sieci VPN.
- ✓ Wymagaj uwierzytelniania wieloskładnikowego, aby zalogować się do urządzeń zawierających wrażliwe dane.

Wzmocnij ochronę hasłem

PROBLEM

Użytkownicy mają tendencję do stosowania tych samych haseł w wielu aplikacjach i usługach internetowych, narażając w ten sposób firmy na ryzyko.

ROZWIĄZANIE

- ✓ Ogranicz dostęp do zasobów firmy, wykorzystując MFA.
- ✓ MFA zmniejsza obawy i niebezpieczeństwa związane z udostępnionymi lub skradzionymi hasłami, wymagając dodatkowego elementu uwierzytelniania, takiego jak zatwierdzenie wiadomości push.

Weryfikuj proces logowania

PROBLEM

Firmy korzystają ze wspólnych komputerów we wspólnych obszarach roboczych i wymagają weryfikacji wszystkich stron logujących się w ciągu dnia roboczego.

ROZWIĄZANIE

- ✓ Wdrożyć uwierzytelnianie wieloskładnikowe dla logowania na komputerze stacjonarnym na wszystkich urządzeniach we współdzielonych obszarach roboczych.

Funkcjonalności i zabezpieczane platformy

FUNKCJONALNOŚCI	SZCZEGÓŁY	
WIELE DZIERŻAW Dostępne tylko dla MSP i wersji hostowanej w chmurze.	Wiele lokacji/firm	✓
ZABEZPIECZENIE LOKALNEGO LOGOWANIA	Logowanie do systemu Windows	✓
ZABEZPIECZENIE ZDALNEGO LOGOWANIA	Serwer Radius do ochrony VPN	✓
	Usługa RDP	✓
OCHRONA APLIKACJI INTERNETOWYCH	Serwer Microsoft Exchange	✓
	Serwer Microsoft SharePoint	✓
	Remote Desktop Web Access	✓
	Microsoft Dynamics CRM	✓
	Remote Web Access	✓
OCHRONA ACTIVE DIRECTORY FEDERATION SERVICES (AD FS)		✓
IDENTITY PROVIDER CONNECTOR (SAML)		✓
PROXY		✓
API		✓
BIAŁA LISTA ADRESÓW IP	Globalna biała lista adresów IP	✓
	Biała lista adresów IP wg funkcjonalności	✓
UWIERZYTELNIANIE	OTP przez wiadomości SMS	✓
	OTP w aplikacji mobilnej	✓
	Powiadomienia push w aplikacji mobilnej	✓
	Tokeny sprzętowe	✓
	Klucze FIDO	✓
POWIADOMIENIA	Problem	✓
	Logowanie do konsoli internetowej	✓
	Użytkownik zablokowany	✓
	Użytkownik odblokowany	✓
	Licencje	✓
OGRANICZANIE	Ograniczanie oparte na czasie	✓
DZIENNIKI AUDYTU I RAPORTY	Raport	✓
	Filtr	✓
	Eksport	✓

Digital Security
Progress. Protected.

To jest ESET

Proaktywna ochrona. Minimalizacja ryzyka dzięki profilaktyce.

Zapobiegaj znanym i nieznanym cyberzagrożeniom dzięki wykorzystaniu sztucznej inteligencji. Łączymy moc sztucznej inteligencji i wiedzę ekspertów, aby ochrona była prosta w obsłudze i skuteczna.

Doświadcz najlepszej w swojej klasie ochrony dzięki innowacyjnej analizie zagrożeń, wykonywanej przez naszą rozległą sieć badawczo-rozwojową prowadzoną przez docenianych w branży specjalistów.

ESET PROTECT, wykorzystująca usługi chmurowe platforma do cyberbezpieczeństwa i XDR, łączy w sobie zapobieganie i proaktywne wykrywanie zagrożeń nowej generacji z szeroką gamą usług zabezpieczających, w tym zarządzanie wykrywaniem i reagowaniem na incydenty.

Nasze wysoce konfigurowalne rozwiązania obejmują lokalne wsparcie i mają minimalny wpływ na wydajność, identyfikują i neutralizują znane i pojawiające się zagrożenia, zanim będą mogły zostać wykonane i wspierają ciągłość działania oraz obniżają koszty wdrożenia i zarządzania.

ESET chroni swoją firmę, dzięki czemu możesz uwolnić pełny potencjał technologii.

ESET W LICZBACH

1 mld+
użytkowników na świecie

400k+
klientów biznesowych

195
krajów i terytoriów

13
centrów badawczo-rozwojowych

NASI KLIENCI

MITSUBISHI MOTORS
Drive your Ambition

zabezpieczamy ponad 9 000 stacji roboczych od 2017 roku

Allianz Suisse

zabezpieczamy ponad 4 000 skrzynek pocztowych od 2016 roku

Canon
Canon Marketing Japan Group

chronimy ponad 32 000 stacji roboczych od 2016 roku

T

partner ISP od 2008 roku baza ponad 2 milionów klientów

ESET UZNANY PRZEZ

AV comparatives APPROVED Business Security DEC 2023

ESET niezmiennie osiąga **najwyższe wyniki w niezależnych testach** przeprowadzonych przez AV-Comperatives i osiąga najlepsze wskaźniki wykrywalności przy braku lub minimalnej ilości fałszywych alarmów.

G2 Leader SPRING 2024

ESET konsekwentnie osiąga czołowe miejsca w globalnej platformie recenzji użytkowników G2, a nasze rozwiązania **cieszą się uznaniem klientów na całym świecie.**

kuppingercole ANALYSTS

Firma ESET jest **uznawana za lidera rynku** i ogólnego lidera w dziedzinie MDR według raportu KuppingerCole LeadershipCompass 2023.