PRÉSENTATION

SECURE AUTHENTICATION

Puissante authentification multifacteur pour
un accès sécurisé aux réseaux et aux données

Progress. Protected.

Authentification multi-facteur : qu'est-ce que c'est ?

L'authentification multifacteur (MFA), également appelée authentification à deux facteurs (2FA), requiert deux éléments d'information distincts pour vérifier l'identité d'un utilisateur. La MFA est beaucoup plus robuste que l'utilisation d'une authentification traditionnelle par mot de passe ou code PIN statique. En complétant l'authentification traditionnelle par un second facteur dynamique, elle réduit efficacement le risque d'atteinte à la sécurité des données causées par des mots de passe faibles ou fuités.

ESET Secure Authentication offre aux entreprises de toute taille un moyen simple de mettre en œuvre la MFA dans les systèmes couramment utilisés tels que les VPN, le protocole d'accès à distance RDP, Outlook Web Access, la connexion au système d'exploitation et bien d'autres.

Digital Security
Progress. Protected.

Assurez la sécurité des données et des actifs de votre entreprise

L'authentification multifacteur compense les risques d'attaques par « credential stuffing » (bourrage d'identifiants), qui utilisent des informations compromises sur les salariés. Ce risque est exacerbé par ceux qui :

- Utilisent le même mot de passe pour plusieurs sites et applications
- Communiquent leurs mots de passe à d'autres personnes
- Ne font que des modifications mineures lors de la mise à jour des mots de passe

MAUVAISES PRATIQUES LIÉES AUX MOTS DE PASSE

Les données sont l'une des ressources les plus précieuses de votre entreprise, que les collaborateurs peuvent compromettre de bien des façons. notamment par de mauvaises pratiques liées aux mots de passe. Non seulement ils utilisent le même mot de passe sur plusieurs sites web et applications, mais ils communiquent parfois librement leurs mots de passe à leur entourage. Comme si cela ne suffisait pas, lorsque des politiques de mot de passe sont appliquées, ils utilisent généralement des variantes de leur ancien mot de passe ou écrivent leurs mots de passe sur des post-it.

Une solution d'authentification multifacteur protège contre ces mauvaises pratiques en mettant en œuvre un élément d'authentification supplémentaire, par exemple en le générant à la volée sur le téléphone du collaborateur, en plus du mot de passe habituel.

La mise en place de cette solution permet d'empêcher les pirates d'accéder à vos systèmes en devinant des mots de passe faibles ou en exploitant les identifiants compromis des collaborateurs.

FUITES DE DONNÉES

Dans le paysage actuel de la cybersécurité, un nombre croissant de fuites de données se produisent chaque jour. L'une des façons les plus courantes pour les pirates d'accéder aux données de votre entreprise consiste à utiliser des mots de passe faibles ou volés, recueillis via des attaques de botnets, d'hameçonnage ou d'attaques ciblées. En plus de protéger les connexions normales des utilisateurs aux services critiques, les entreprises peuvent mettre en œuvre la MFA pour empêcher les accès administrateur non autorisés via escalade de privilèges.

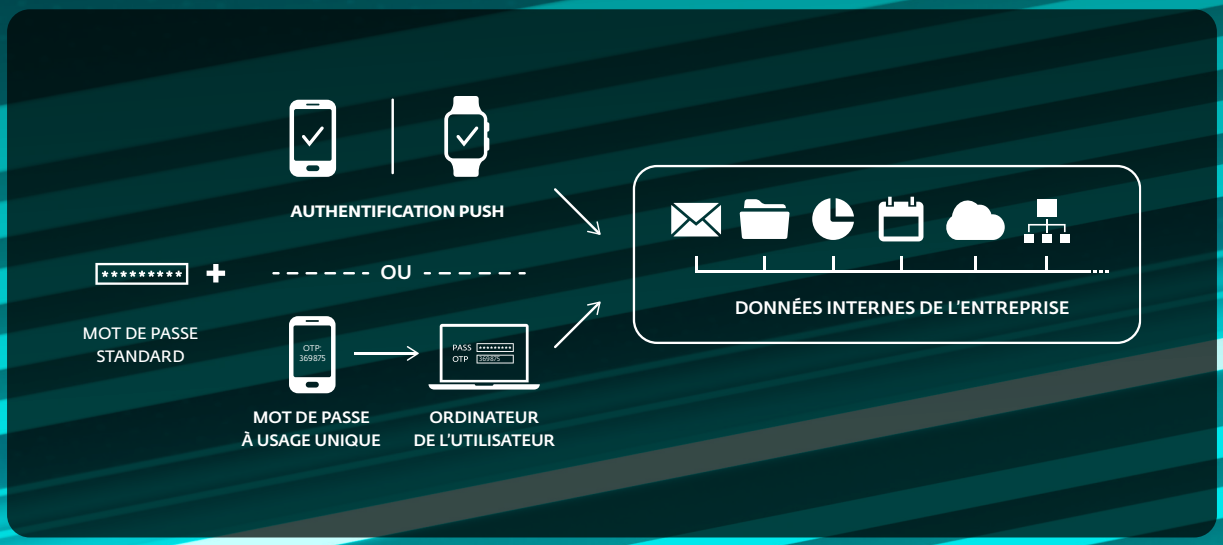
En ajoutant une solution multifacteur, il sera beaucoup plus difficile pour les pirates d'accéder à vos systèmes et de les compromettre. Les principaux secteurs d'activité concernés par les fuites de données sont traditionnellement ceux qui traitent des données précieuses, tels que les secteurs de la finance, du commerce de détail, de la santé, et le secteur public. Cela ne signifie pas pour autant que les autres secteurs sont à l'abri, mais simplement que les pirates s'intéressent généralement de près au ratio gain/effort.

CONFORMITÉ

En matière de conformité, la plupart des entreprises doivent d'abord déterminer si elles sont tenues d'atteindre un objectif de conformité ou non. Elles doivent ensuite examiner les mesures et les recommandations que leur entreprise doit mettre en œuvre pour être conforme. En ce qui concerne l'authentification multifacteur, plusieurs réglementations telles que PCI-DSS et GLBA exigent sa mise en œuvre, et de nombreuses lois, dont le RGPD et l'HIPAA, soulignent la nécessité d'une authentification plus forte.

L'authentification multifacteur n'est plus seulement une option pour la plupart des entreprises qui traitent des cartes de crédit ou des transactions financières, mais une solution obligatoire. Toutes les entreprises doivent examiner les lois et les règlements qui leur sont applicables, et veiller à qu'elles en respectent les exigences.

Permettez l'authentification d'un simple appui sur l'écran, sans requérir la saisie d'un mot de passe à usage unique.



Les avantages ESET

AUTHENTIFICATION PUSH

Elle vous permet l'authentification par un simple appui sur l'écran, sans avoir à saisir de mot de passe à usage unique. Fonctionne avec les smartphones iOS et Android.

PROTÉGEZ VOS APPLICATIONS DANS LE CLOUD

Ajoutez la MFA pour renforcer l'accès à des services tels que les applications Google, Dropbox et bien d'autres. ESET prend en charge l'intégration via le protocole d'authentification SAML-2 utilisé par les principaux fournisseurs d'identité.

INSTALLATION EN 10 MINUTES

Nous avons travaillé dur pour que vous n'ayez pas à le faire. Nous nous sommes donnés pour objectif de créer une solution que même une petite entreprise sans personnel informatique peut mettre en œuvre et configurer. Que votre entreprise compte des dizaines ou des milliers d'utilisateurs, ESET Secure Authentication réduit au minimum le temps d'installation grâce à sa capacité à provisionner plusieurs utilisateurs en même temps.

PLUSIEURS FAÇONS DE S'AUTHENTIFIER

Les collaborateurs n'ont pas besoin de jetons ou d'appareils spéciaux. ESET Secure Authentication fonctionne sans problème sur les smartphones, dispose de son propre code PIN pour plus de sécurité et peut s'intégrer aux fonctionnalités biométriques des appareils (Touch ID, Face ID, empreinte digitale Android) pour améliorer la sécurité et l'expérience utilisateur. Les clés de sécurité FIDO et les jetons matériels sont également pris en charge au besoin.

AUCUN MATÉRIEL DÉDIÉ N'EST NÉCESSAIRE

Les besoins d'ESET Secure Authentication en ressources sont minimes. Vous pouvez utiliser la version Cloud et n'avez donc pas besoin d'un serveur dédié. La solution peut cependant être déployée sur site.

INTÉGRATION TRANSPARENTE

Deux modes d'intégration sont possibles : l'intégration Active Directory pour les organisations utilisant un domaine Windows, ou le mode autonome qui convient à celles qui n'ont pas de domaine. Quoi qu'il en soit, l'installation et la configuration sont rapides et faciles, et tout est administré de manière transparente via une console dans le Cloud.

MULTI-TENANT

La version d'ESET Secure Authentication dans le Cloud est multi-tenant afin que les prestataires de services managés puissent administrer plusieurs sites ou entreprises, avec la possibilité de définir des paramètres spécifiques pour des groupes d'utilisateurs individuels.

VDI ET VPN PRIS EN CHARGE

VMware Horizon View, Citrix XenApp, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet, FortiGate, Juniper, Palo Alto et SonicWall sont pris en charge. N'importe quel VPN RADIUS peut être pris en charge via une intégration personnalisée.

API COMPLÈTE ET SDK INCLUS

Pour les clients qui souhaitent aller encore plus loin, nous avons inclus une API et un SDK complets afin d'étendre la MFA aux applications ou aux plateformes qu'ils utilisent, même sans plugin dédié.

Cas d'utilisation

Protéger plusieurs sites

PROBLÈME

Un MSP doit gérer plusieurs succursales ou entreprises avec une variété de politiques de sécurité et de configurations.

SOLUTION

- ✓ Créez chaque entreprise en tant que site dans le portail ESET PROTECT Hub et attribuez-leur une certaine part de la licence ESET Secure Authentication. Lorsque vous vous connecterez de nouveau à la console, vous verrez apparaître l'élément de menu Entreprises.
- ✓ Le multi-tenant dans la version Cloud, qui ne nécessite pas de matériel local, permet de gérer l'authentification multifacteur pour différentes entreprises ou succursales à partir d'une seule instance.

Prévention des fuites de données

PROBLÈME

Chaque jour, des entreprises avertissent leurs clients qu'une atteinte à la sécurité de leurs données s'est produite.

SOLUTION

- ✓ Protéger les communications vulnérables telles que le protocole d'accès à distance RDP en ajoutant l'authentification multifacteur.
- ✓ Ajouter l'authentification multifacteur à tous les VPN utilisés.
- ✓ Exiger l'authentification multifacteur pour se connecter aux appareils contenant des données sensibles.

Renforcer la protection par mot de passe

PROBLÈME

Les utilisateurs ont tendance à utiliser les mêmes mots de passe pour plusieurs applications et services web, ce qui met les entreprises en danger.

SOLUTION

- ✓ Restreindre l'accès aux ressources de l'entreprise grâce à l'utilisation de l'authentification multifacteur.
- ✓ Elle réduit l'inquiétude et le danger associés au partage ou au vol de mots de passe en exigeant un élément d'authentification supplémentaire, tel que qu'une approbation par message Push.

Vérifier le processus de connexion des utilisateurs

PROBLÈME

Les entreprises utilisent des ordinateurs partagés dans des espaces de travail communs et exigent la vérification de toutes les personnes qui se connectent au cours d'une journée de travail.

SOLUTION

- ✓ Mettre en œuvre l'authentification multifacteur pour les ouvertures de session sur tous les appareils des espaces de travail partagés.

Fonctionnalités techniques et plateformes protégées

FONCTIONNALITÉ	DÉTAIL	
MULTI-TENANT Disponible uniquement pour les MSP dans la version Cloud.	Plusieurs sites/entreprises	✓
PROTECTION DE LA CONNEXION LOCALE	Connexion à Windows	✓
PROTECTION DE LA CONNEXION À DISTANCE	Serveur Radius pour la protection par VPN	✓
	Bureau à distance	✓
PROTECTION DES APPLICATIONS WEB	Microsoft Exchange Server	✓
	Microsoft SharePoint Server	✓
	Remote Desktop Web Access	✓
	Microsoft Dynamics CRM	✓
	Remote Web Access	✓
PROTECTION DES SERVICES DE FÉDÉRATION ACTIVE DIRECTORY (AD FS)		✓
CONNECTEUR POUR FOURNISSEUR D'IDENTITÉ (SAML)		✓
PROXY		✓
API		✓
LISTE BLANCHE D'ADRESSES IP	Liste blanche globale d'adresses IP	✓
	Liste blanche d'adresses IP par fonctionnalité	✓
PROVISIONNEMENT	OTP via SMS	✓
	OTP via application mobile	✓
	Notification Push via application mobile	✓
	Jeton matériel	✓
	FIDO	✓
NOTIFICATIONS	Problème	✓
	Connexion à la console web	✓
	Utilisateur verrouillé	✓
	Utilisateur déverrouillé	✓
	Licences	✓
LIMITATION	Restriction basée sur des horaires	✓
RAPPORTS ET JOURNAUX D'AUDIT	Rapport	✓
	Filtre	✓
	Export	✓

À propos d'ESET

QUAND LA TECHNOLOGIE ENGENDRE LE PROGRÈS, ESET® EST LÀ POUR LE PROTÉGER.

ESET apporte plus de 30 ans d'innovation technologique et les solutions de cybersécurité les plus avancées du marché. Notre protection moderne pour endpoints s'appuie sur les technologies de sécurité multicouches uniques ESET LiveSense®, combinées à l'utilisation continue du machine learning et du Cloud.Les meilleurs renseignements au monde sur les menaces ainsi que **des études avancées offrent aux produits ESET un équilibre parfait entre** prévention, détection et traitement. Nous nous attachons à protéger les progrès de nos clients en leur garantissant une protection maximale facile à utiliser et d'une vitesse inégalée.

ESET EN QUELQUES CHIFFRES

+ 1 Mrd
internautes protégés

+ 400 k
entreprises clientes

200
pays et territoires

12
centres de recherche

QUELQUES-UNS DE NOS CLIENTS

MITSUBISHI MOTORS
Drive your Ambition

Protégés par ESET depuis 2017 : 9 000 endpoints

Allianz Suisse

Protégé par ESET depuis 2016 : +4 000 boîtes mail

Canon
Canon Marketing Japan Group

Protégés par ESET depuis 2016 : 32 000 endpoints

Partenaire de sécurité FAI depuis 2008 : 2 millions d'utilisateurs

RECONNAISSANCES

AV comparatives APPROVED Business Security DEC 2023

ESET est constamment **parmi les éditeurs les plus performants des tests indépendants** d'AV-Comparatives, et atteint les meilleurs taux de détection avec peu voire aucuns faux positifs.

G2 Leader SPRING 2024

ESET obtient régulièrement les meilleures notes sur la plateforme mondiale d'évaluation des utilisateurs G2, et ses solutions sont **appréciées par les clients du monde entier**.

kuppingercole ANALYSTS

ESET est **reconnu comme un leader du marché** et un leader en général du MDR, selon le KuppingerCole Leadership Compass 2023.