Livre blanc

# Anatomie des attaques basées sur l'identité

Comment vous protéger contre les menaces ciblant vos utilisateurs

# Sommaire

# Le rôle de l'identité dans la sécurité

À l'origine, le rôle de l'identité dans la stratégie de sécurité des entreprises se limitait à la vérification des utilisateurs valides au moment de l'authentification et à l'octroi d'un niveau d'accès approprié. Toutefois, face à la multiplication des attaques ciblant les utilisateurs et leurs identifiants, les systèmes de gestion des identités et des accès (IAM, Identity and Access Management) ont renforcé leurs fonctionnalités de sécurité pour les protéger contre ces menaces. L'identité revêt également une importance capitale pour les responsables de la sécurité qui ont entamé un parcours Zero Trust dans le but de renforcer leurs défenses.

Aujourd'hui, l'identité est devenue une composante essentielle de la stratégie de cybersécurité des entreprises. Dans un contexte de télétravail, de terminaux non gérés et d'environnements cloud et SaaS, l'identité est le seul élément commun qui relie les personnes aux terminaux, aux applications et aux ressources dont elles ont besoin pour faire leur travail. Les fournisseurs d'identité tirent parti de ces connexions.

Seule technologie universellement intégrée à l'infrastructure IT, l'identité est l'instrument idéal pour instaurer une approche plus collaborative de la sécurité IT. Grâce aux contrôles de sécurité d'Okta Workforce Identity Cloud et à ceux d'autres systèmes, vous pouvez évaluer les risques, contrer les menaces et renforcer votre niveau de cybersécurité. Cette approche de la sécurité axée sur l'identité offre d'importants avantages :

- Elle unifie et renforce les politiques, la visibilité et le contrôle en matière d'identité grâce à une plateforme alliant IAM, gouvernance et administration des identités (IGA, Identity Governance and Administration) et gestion des accès à privilèges (PAM, Privileged Access Management).
- Elle contribue à la détection des risques qui peuvent peser sur l'entreprise, soit de manière indépendante, soit en association avec vos produits de sécurité existants.
- Elle évalue continuellement les risques avant, pendant et après l'authentification des utilisateurs.
- Elle apporte une réponse adaptative aux menaces sur la base d'informations en temps réel.

Ce rapport s'intéresse aux menaces croissantes ci-dessous qui touchent aujourd'hui les entreprises, ainsi qu'à la façon dont Okta peut jouer un rôle dans la protection, la détection et la réponse aux menaces, avant, pendant et après l'authentification.

- Phishing
- Compromission des terminaux des utilisateurs finaux
- Menaces internes
- Menaces post-authentification
- Attaques par force brute

**Statistiques sur l'identité et la sécurité**

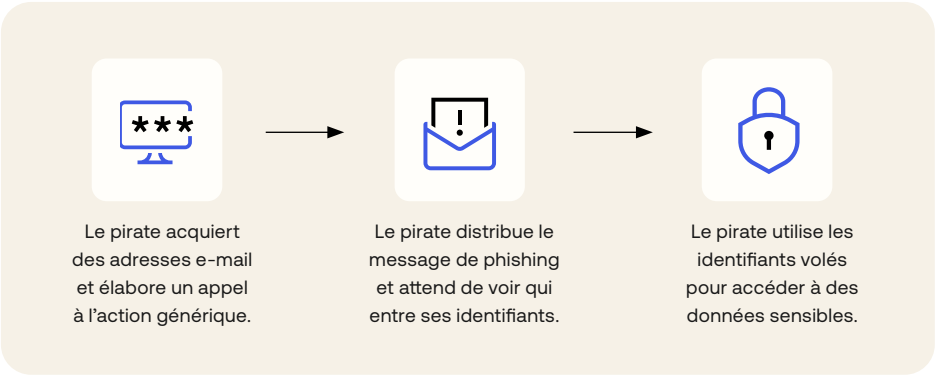
- En **2022**, **45 %** des brèches de données exploitaient des identifiants volés, contre **42 %** l'année précédente[1].
- **74 %** des brèches impliquent une interaction humaine, qu'il s'agisse d'une erreur, de l'usage abusif des privilèges, de l'utilisation d'identifiants volés ou de social engineering[1].
- **86 %** des brèches observées dans les applications web impliquent des identifiants volés[1].

**[1]** 2023 Verizon Data Breach Investigations Report

# Phishing

Les tentatives de phishing constituent le premier cyberdélit signalé aux États-Unis et entraînent les pertes financières les plus importantes pour les victimes[2]. Les cybercriminels ont recours à l'IA et à l'automatisation pour lancer des attaques de phishing à grande échelle, ce qui les rend de plus en plus difficiles à détecter et à intercepter. La plupart des attaques de phishing commencent par des e-mails qui incitent les utilisateurs à saisir leurs identifiants sur un faux site. Ces e-mails et ces sites peuvent sembler convaincants par la qualité du branding et du langage employés, et utilisent des adresses e-mail source très proches de l'adresse cible. Une fois qu'un cybercriminel a accès aux identifiants d'un utilisateur, il s'en sert pour se connecter et s'introduire dans l'environnement visé afin de préparer une attaque de plus grande envergure, par exemple :

- Installation d'un ransomware sur les systèmes d'entreprise à des fins d'extorsion
- Compromission d'e-mails professionnels (BEC) afin de rediriger des fonds vers un compte bancaire contrôlé par le cybercriminel, par exemple en modifiant les numéros de compte utilisés pour les versements de salaires ou les factures
- Minage d'applications pour obtenir des données sensibles à vendre sur le Dark Web




Les entreprises investissent dans des filtres antispam, des logiciels de sécurité e-mail, des antivirus, des filtres web et des programmes de sensibilisation des utilisateurs qui les protègent contre les quelque 156 millions d'e-mails de phishing envoyés chaque jour dans le monde entier. Toutefois, les attaques gagnent en sophistication et parviennent plus fréquemment à contourner les défenses traditionnelles. Jusqu'ici, le MFA représentait la référence en matière de prévention du vol d'identifiants, y compris par le biais du phishing, mais de récentes attaques très médiatisées ont montré qu'il ne suffit plus à prévenir toutes les brèches de données. Le MFA peut être vulnérable aux attaques Adversary-in-the-Middle (AitM), aux attaques par échange de carte SIM, aux attaques Pass-the-Cookie, à la fatigue MFA et aux attaques par bombardement de demandes MFA (dans lesquelles les cybercriminels envoient des notifications push MFA répétées). Le MFA n'a de sens que s'il est résilient face au contournement et au piratage.

**[2]** Federal Bureau of Investigation Internet Crime Report 2022

## Stratégies d'atténuation des risques

1. **Outils et formation des utilisateurs.** Étant donné que les attaques de phishing ciblent les utilisateurs, il est essentiel de leur fournir des outils à des fins de prévention.

    a. Organisez des campagnes de simulation de phishing avec Okta Workflows en envoyant de fausses invites MFA pour apprendre aux utilisateurs à ne pas se laisser piéger par des demandes MFA à répétition.

    b. Faites en sorte que les utilisateurs puissent être facilement informés des modifications apportées au méthodes d'authentification de leurs comptes avec Okta HealthInsight. Cette fonctionnalité permet également aux utilisateurs de signaler les événements d'authentification suspects en toute simplicité.

2. **Principe du moindre privilège.** Okta Identity Governance (OIG) offre des contrôles d'accès qui limitent l'accès des utilisateurs aux seules ressources dont ils ont besoin pour leur rôle ou un projet pendant une durée limitée ; une telle stratégie réduit le risque de déplacement latéral en cas d'attaque de phishing ou d'autre tentative de social engineering fructueuse. De même, OIG automatise et gère les processus liés aux arrivées, transferts et départs de collaborateurs sur toutes les ressources cloud et on-premise, et certifie l'accès de manière récurrente. Cette automatisation réduit le risque que des cybercriminels utilisent des comptes inactifs pour lancer des attaques de phishing ou obtenir un accès.

3. **Authentification renforcée**. La détection des comportements d'Okta Adaptive MFA analyse les comportements récurrents des utilisateurs et crée des profils en fonction des activités antérieures. Vous pouvez configurer des règles de politique qui répondent automatiquement aux changements de comportement des utilisateurs, par exemple en exigeant un facteur supplémentaire si un utilisateur tente de se connecter à partir d'un autre pays ou d'une autre adresse IP.

4. **Authentification résistante au phishing.** L'authentification résistante au phishing est conçue pour empêcher les cybercriminels de contourner le MFA en éliminant les secrets partagés tels que les questions de sécurité. Elle empêche également les utilisateurs de se faire duper par des domaines frauduleux. Okta prend en charge :

    a. Les principales méthodes d'authentification résistantes au phishing, y compris les authentificateurs FIDO2 WebAuthn et les cartes à puce PIV/CAC

    b. Okta FastPass, un authentificateur Zero Trust sans mot de passe, résistant au phishing, adapté aux terminaux gérés et non gérés

5. **Détection des menaces.** Les équipes sécurité peuvent tirer parti des intégrations Okta avec les principaux fournisseurs e-mail et configurer des politiques d'authentification adaptative basées sur le risque. Par exemple, les politiques Okta pourraient renforcer l'authentification ou verrouiller des comptes utilisateurs en réponse aux menaces détectées au niveau de la messagerie. Okta Identity Threat Protection avec Okta AI utilise les signaux de sécurité de diverses solutions de sécurité, y compris les outils de protection e-mail. Si ces technologies détectent des e-mails de phishing entrants ou des liens malveillants, Okta en est averti et peut relever le niveau de risque de l'utilisateur et déclencher des réponses directes appropriées.
6. **Réponse aux menaces.** Au-delà de la détection, Okta Identity Threat Protection orchestre des réponses sur mesure en fonction de la configuration des politiques et des niveaux de risque des utilisateurs évalués. Par exemple, un niveau de risque moyen peut inciter Okta Identity Threat Protection à envoyer des notifications au SIEM ou à l'équipe de réponse aux incidents, tandis qu'un risque élevé peut déclencher la réauthentification des utilisateurs, fermer une session utilisateur ou même déconnecter des utilisateurs d'applications prises en charge pour lesquelles la fonctionnalité est activée.

# Compromission des terminaux des utilisateurs finaux

Le télétravail et le BYOD ont ouvert la voie à de nouvelles menaces ciblant les téléphones, les ordinateurs portables et autres terminaux des utilisateurs. Face à l'adoption croissante de méthodes résistantes au phishing, les cybercriminels peuvent également avoir recours à la compromission de terminaux pour infiltrer votre entreprise.

Les cyberattaques commencent souvent par la compromission du terminal d'un utilisateur final, par exemple en incitant ce dernier à installer un malware. Ce malware peut alors capturer des identifiants et, comme dans le cas du phishing, permettre au cybercriminel de se déplacer latéralement dans l'environnement d'entreprise pour propager des ransomwares, exfiltrer des données sensibles ou lancer une attaque BEC. L'identité peut jouer un rôle dans la prévention et la détection de certaines attaques de terminaux en ajoutant une sécurité supplémentaire aux appareils et en les vérifiant pendant et après l'authentification.

## Stratégies d'atténuation des risques

1. **Device Trust.** Device Trust permet de s'assurer que seuls les utilisateurs possédant des terminaux gérés de confiance peuvent accéder à votre environnement. Okta renforce les politiques Device Trust en s'assurant que chaque terminal géré dispose d'une posture de sécurité adaptée avant qu'un utilisateur ne soit autorisé à se connecter. L'application Okta Verify s'intègre avec les outils MDM (Mobile Device Management) et EDR (Endpoint Detection and Response), et capture les signaux des terminaux au moment de la connexion. En fonction de ces signaux et des politiques que vous définissez, Okta prend une décision d'accès.

2. **Device Assurance.** Pour les terminaux gérés ou non gérés sans support MDM ou EDR, Okta Verify peut effectuer des contrôles d'intégrité sur les terminaux et prendre une décision d'accès en fonction de vos politiques. Par exemple, vous pouvez exiger le chiffrement des disques et l'installation des versions les plus récentes des systèmes d'exploitation, ainsi qu'interdire les terminaux débridés. Après l'authentification, FastPass peut continuer à vérifier les terminaux en arrière-plan chaque fois qu'un utilisateur ouvre une nouvelle application. Selon les informations renvoyées par le terminal, FastPass peut demander une réauthentification ou rejeter la demande d'accès à l'application.

3. **Protection de l'accès aux terminaux.** Okta Device Access étend les mêmes expériences MFA sécurisées à la façon dont les utilisateurs se connectent à leurs ordinateurs de bureau, offrant ainsi un niveau de protection supplémentaire à leurs terminaux. Okta Device Access peut vérifier l'identité d'un utilisateur et lui octroyer un accès même sans connexion Internet.

4. **Filtres d'applications de confiance.** Les administrateurs peuvent créer une liste d'autorisation d'applications pour s'assurer que les applications malveillantes ou non vérifiées sur les terminaux des utilisateurs ne peuvent pas exploiter FastPass pour obtenir un accès non autorisé.
5. **Détection et réponse aux menaces.** Identity Threat Protection s'intègre avec les principales solutions EDR pour l'analyse et la réponse aux malwares sur les terminaux. Les réponses automatisées incluent des actions telles qu'une demande de réauthentification ou la déconnexion des utilisateurs sur les terminaux compromis en fonction de l'évaluation des risques en temps réel effectuée par Identity Threat Protection.

## Menaces internes

Les menaces internes sont en hausse et peuvent être malveillantes, comme dans le cas d'une tentative délibérée de voler des informations ou de nuire à l'entreprise. Cependant, 55 % des incidents d'origine interne sont dus à la négligence d'un collaborateur, par exemple s'il ne sécurise pas ses terminaux, n'installe pas les mises à jour de sécurité ou ne respecte pas les politiques de sécurité de l'entreprise. Les autres menaces internes incluent les erreurs légitimes et les utilisateurs piégés par un nouveau type d'attaque. L'année dernière, le confinement d'un incident d'origine interne a nécessité 86 jours en moyenne, le coût moyen par entreprise des risques internes s'élevant à 16,2 millions de dollars[3].

L'identité joue un rôle dans le programme de gestion des risques internes des entreprises. Par exemple, 56 %[3] des sociétés ont déployé des solutions PAM pour réduire le risque que des utilisateurs internes accèdent à des identifiants et à des comptes à privilèges par erreur ou à des fins malveillantes. De même, les systèmes IGA peuvent réduire l'impact des menaces internes sur une entreprise.

**[3]** Cost of Insider Risks Global Report, 2023

## Stratégies d'atténuation des risques

1. **Protection de l'accès aux terminaux.** Imaginez qu'un utilisateur interne égare un ordinateur portable ou le laisse dans un lieu non sécurisé. Device Access offre une couche de sécurité supplémentaire visant à empêcher les utilisateurs non vérifiés d'accéder aux données stockées sur le terminal, même si ce dernier n'est pas connecté à Internet.

2. **Principe du moindre privilège.** Okta Identity Governance aide les entreprises à créer des processus qui limitent l'accès des utilisateurs internes aux applications et ressources dont ils ont besoin pour leur rôle ou un projet, réduisant ainsi d'accès inapproprié à des informations sensibles. Les administrateurs peuvent configurer les accès pour qu'ils expirent après un certain temps ou exécuter des campagnes Access Certifications afin de vérifier que les accès sont appropriés.

3. **Accès aux comptes à privilèges.** Réduisez le risque que des utilisateurs internes bénéficient d'un accès inapproprié à des ressources sensibles. Okta Privileged Access protège les ressources stratégiques en éliminant les accès permanents, en sécurisant les comptes partagés et en établissant une responsabilité individuelle d'utilisation. Okta unifie les fonctionnalités PAM essentielles avec l'IAM et la gouvernance des identités au sein d'une même plateforme, ce qui accroît la visibilité et simplifie l'application de politiques pour les comptes et ressources à privilèges. Cette unification élimine la nécessité de recourir à des outils IAM, IGA et PAM cloisonnés et renforce la sécurité. Les comportements ou les signaux qui augmentent les niveaux de risque des utilisateurs dans l'IAM sont automatiquement transmis à Privileged Access afin que des mesures soient prises, ce qui réduit le risque que des utilisateurs internes malveillants ou négligents exploitent des identifiants à privilèges.

4. **Détection des menaces.** Il arrive que des utilisateurs légitimes fassent un usage abusif des ressources de l'entreprise. Identity Threat Protection avec Okta AI fonctionne avec d'autres outils de sécurité tels que des solutions EDR, CASB ou SIEM. Ces outils identifient les comportements suspects, par exemple si un utilisateur télécharge un grand nombre de fichiers à partir d'un annuaire, et avertissent Okta du risque élevé que représente l'utilisateur.

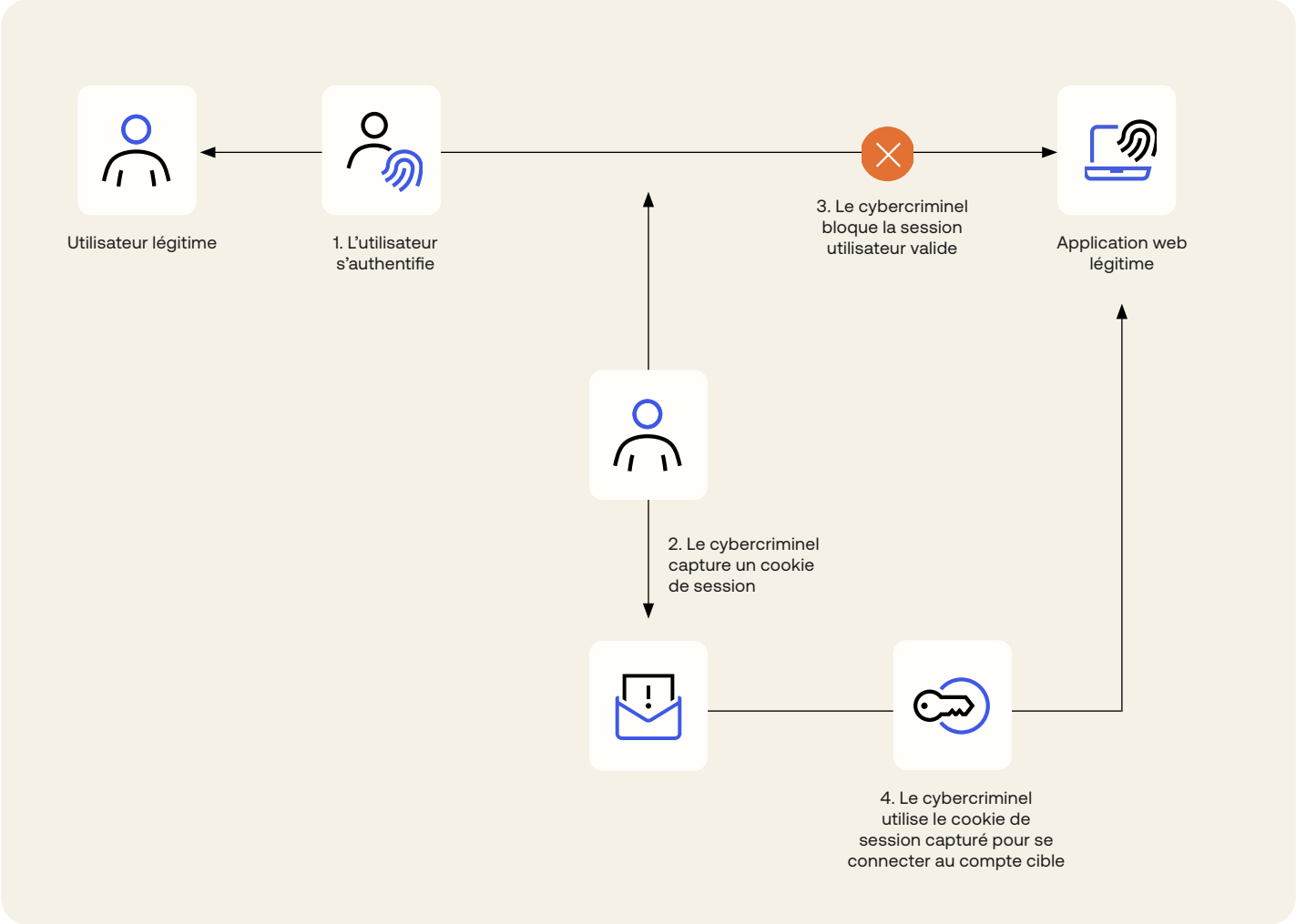
5. **Réponse aux menaces.** Comme pour les autres attaques, Okta peut répondre aux profils de risque élevé des utilisateurs de manière automatique et appropriée en exigeant une réauthentification, en limitant l'accès ou en déconnectant les utilisateurs des applications prises en charge.

# Menaces post-authentification

La sécurisation de la première connexion ne suffit plus. Avec l'adoption croissante de méthodes d'authentification multifacteur et résistante au phishing, il va devenir plus difficile pour les cybercriminels de voler des identifiants au moment de la connexion. Cela va entraîner une hausse des attaques ciblant les utilisateurs et leurs terminaux après la réussite de l'authentification. Plusieurs brèches très médiatisées ont déjà démontré les opportunités d'attaques post-authentification.

## Détournement de session

Après qu'un utilisateur s'authentifie avec succès sur un serveur d'applications particulier, le serveur génère un token ou un cookie de session stocké dans le navigateur de l'utilisateur. Le détournement de session peut employer plusieurs méthodes pour voler un token de session : attaques par scripts intersites (XSS), installation de malwares, reniflage de session, etc. Une fois que le cybercriminel dispose d'un token de session valide, il peut faire tout ce qu'un utilisateur légitime est autorisé à faire dans cette application.



## Stratégies d'atténuation des risques

1. **Configurations d'atténuation des risques.** Okta permet de définir un certain nombre de configurations différentes afin de réduire le risque de vol de sessions :

    a. Vous pouvez faire en sorte que les sessions utilisateurs expirent après un laps de temps ou une durée d'inactivité spécifique, ce qui réduit la période pendant laquelle les cybercriminels peuvent voler des tokens de session ou utiliser des tokens volés.

    b. De même, Okta Identity Governance peut provisionner des droits d'accès granulaires aux applications pour les utilisateurs en fonction de leur rôle ou des projets sur lesquels ils travaillent ; cette stratégie réduit les risques associés aux cookies de session volés en limitant les actions autorisées dans une application spécifique.

    c. Vous pouvez définir une règle de politique d'authentification pour exiger des utilisateurs qu'ils se réauthentifient à chaque fois qu'ils essaient d'accéder à une nouvelle application. L'utilisation de l'authentification sans mot de passe via FastPass réduit les désagréments potentiels pour les utilisateurs.

2. **Sécurité VPN supplémentaire.** Les réseaux privés virtuels (VPN) sont un excellent moyen de déjouer le reniflage de session. Toutefois, les VPN ne nécessitent souvent qu'un nom d'utilisateur et un mot de passe, qui sont vulnérables aux attaques. Okta s'intègre avec de nombreux VPN et ajoute une couche de sécurité supplémentaire avec le MFA ou le MFA résistant au phishing, ce qui réduit le risque d'attaques par reniflage réussies lorsque des utilisateurs sont connectés à des réseaux Wi-Fi publics.

3. **Analyse des risques associés aux sessions.** Une fois que les utilisateurs sont authentifiés, Identity Threat Protection surveille les sessions utilisateurs en continu afin de détecter les comportements suspects ou inhabituels. L'analyse comportementale est optimisée par un système d'analytique. Identity Threat Protection reçoit également des signaux de sécurité d'Okta Verify et d'outils de sécurité tiers, offrant une vue en temps réel des risques associés aux sessions.

4. **Réévaluation du contexte.** Pour les entreprises comportant un ensemble hétérogène de terminaux, FastPass effectue des contrôles d'intégrité en mode silencieux sur les terminaux à chaque fois qu'un utilisateur authentifié ouvre une nouvelle application. Cette approche procure une assurance supplémentaire que le terminal et sa posture n'ont pas changé avant d'autoriser l'accès, ce qui réduit le risque de détournement de session.

5. **Comptes à privilèges.** Okta Privileged Access réduit la surface d'attaque des sessions en contrôlant l'accès aux comptes à privilèges du personnel autorisé qui en a légitimement besoin et en limitant la portée des autorisations pendant les sessions.

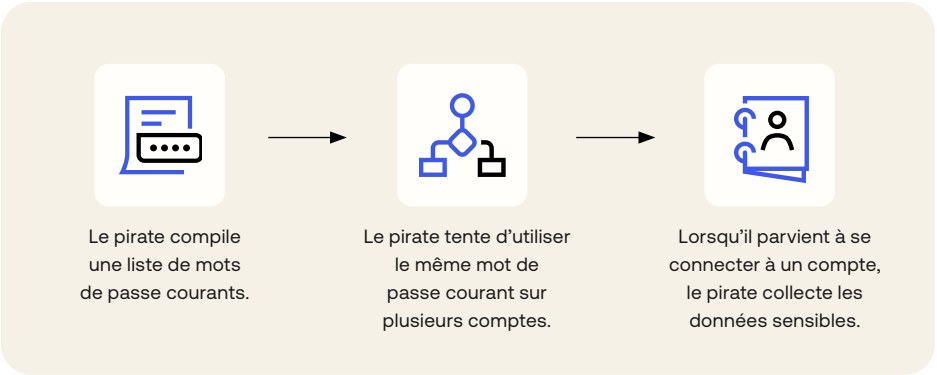
6. **Réponse aux menaces.** Okta peut apporter une réponse adaptative aux risques identifiés dans les sessions utilisateurs en exigeant une réauthentification ou en fermant la session. À l'inverse, Identity Threat Protection peut optimiser l'expérience utilisateur en prolongeant la durée des sessions pour les utilisateurs aux profils de risque faible.

# Attaques par force brute

Les attaques par force brute ne disparaîtront pas tant que les gens continueront d'utiliser des mots de passe faibles ou de réutiliser des mots de passe existants.

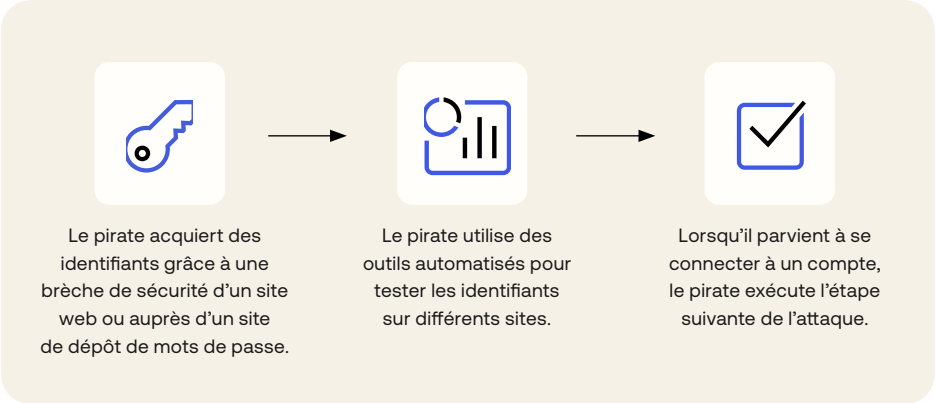
## Password spray

Le password spray est une attaque volumétrique qui ne cible pas des utilisateurs ou comptes spécifiques. Un cybercriminel utilise plusieurs mots de passe courants sur plusieurs comptes dans l'espoir qu'un utilisateur y ait recours comme identifiant de connexion. Souvent, les attaquants tentent de rester sous les seuils déclenchant le verrouillage des comptes en utilisant un nombre limité de mots de passe plausibles pour de nombreux comptes. Pour améliorer la probabilité de tomber sur le bon mot de passe, ils peuvent effectuer des recherches sur les entreprises ciblées afin de déterminer si un système exige des mots de passe d'une longueur particulière ou des caractères spéciaux.




## Credential stuffing

Lors d'une attaque par credential stuffing, le cybercriminel tente d'appliquer des identifiants valides (souvent collectés à partir d'un dépôt de données en ligne) à de nombreux sites différents, dans l'espoir qu'une paire d'identifiants fonctionne. Ce type d'attaque exploite la tendance des utilisateurs à réutiliser le même mot de passe sur plusieurs sites. L'acteur malveillant utilise des outils automatisés pour couvrir un grand nombre de systèmes en un court laps de temps. Cette attaque est souvent couronnée de succès, car les identifiants valides ne déclenchent pas de règles de verrouillage des comptes.



## Stratégies d'atténuation des risques

1. **Outils et formation des utilisateurs.** Pour les entreprises qui utilisent encore des mots de passe :
    a. Réduire la réutilisation des mots de passe peut entraver les chances de réussite des attaques par credential stuffing. Pour y parvenir, vous pouvez décharger les utilisateurs de la responsabilité de créer des mots de passe forts. Le plugin Okta pour navigateur peut suggérer des mots de passe uniques et les enregistrer automatiquement lorsque les utilisateurs créent de nouveaux comptes.
    b. Okta peut aider votre entreprise à bannir les mots de passe courants en appliquant des critères obligatoires lors de la création de compte, ce qui réduit le risque d'attaque par password spray.
2. **Détection des adresses IP malveillantes.** ThreatInsight agrège les données de l'ensemble des clients Okta et s'en sert pour détecter les adresses IP malveillantes qui tentent de lancer des attaques basées sur les identifiants. Okta empêche ces adresses IP d'atteindre l'étape d'authentification, ce qui réduit le risque de verrouillage des comptes d'utilisateurs légitimes.
3. **Méthodes d'authentification sécurisées.** Okta propose plusieurs options d'authentification pour déjouer les attaques par force brute :
    a. FastPass est un authentificateur Zero Trust qui élimine la nécessité d'utiliser des mots de passe, un vecteur d'attaque important. Il évalue également l'intégrité des terminaux et des navigateurs, et permet de s'assurer que seuls les utilisateurs de confiance et leurs terminaux peuvent accéder à votre environnement.
    b. Okta prend en charge un large éventail d'autres méthodes d'authentification résistantes au phishing.
    c. La solution Adaptive MFA s'assure que les cybercriminels ne peuvent pas mener à terme le flux d'authentification même s'ils sont en possession d'un identifiant compromis. Okta analyse les comportements des utilisateurs (emplacement, adresse IP et autres points de données du même type) pour établir un profil de référence et déterminer le niveau de risque de la tentative de connexion. Si le MFA n'est pas un contrôle que vous pouvez appliquer pour chaque utilisateur et chaque connexion, vous pouvez cependant l'associer à d'autres contrôles tels que les empreintes des terminaux. En outre, les administrateurs sécurité peuvent configurer un CAPTCHA dans le flux de connexion pour renforcer la sécurité de la demande d'authentification.

# Résumé

Okta Workforce Identity Cloud offre un large éventail de fonctionnalités qui protègent les utilisateurs, leurs terminaux et leurs sessions contre les menaces avant, pendant et après l'authentification. L'analyse comportementale, les contrôles des terminaux et les intégrations prêtes à l'emploi avec d'autres outils de sécurité permettent à Okta d'évaluer le risque en continu et d'aider votre entreprise à répondre automatiquement aux risques liés aux identités avant qu'ils ne vous portent préjudice.

Apprenez-en davantage sur Okta Workforce Identity Cloud.