jamf

Gestion des identités et sécurité

Guide avancé

Chaque travailleur a sa propre identité

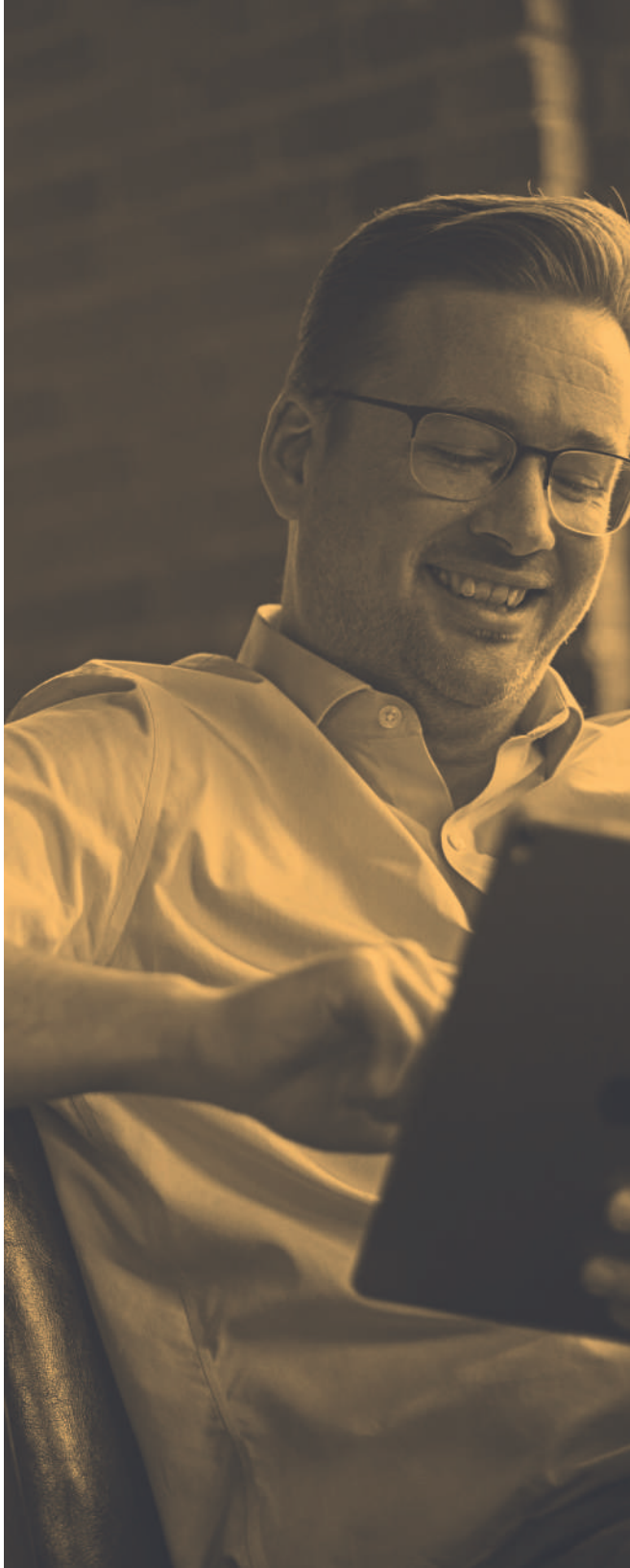
La gestion des identités est devenue crutiale au cours de la dernière décennie, alors que les organisations cherchent à s'adapter aux télétravail. La migration des configurations locales vers le cloud a amené d'innombrables organisations à se rapprocher de la gestion moderne des identités, un sujet sur lequel nous nous sommes plongés dans notre guide « La gestion des identités pour les débutants ». Cependant, la gestion des identités va bien au-delà de l'authentification et de l'autorisation, car les organisations cherchent à tirer parti des identités des utilisateurs pour atteindre leurs objectifs de Zero Trust (confiance zéro).

Un précepte majeur du Zero Trust est que vous ne devez pas faire confiance aux nombreux composants qui constituent la connexion entre vos utilisateurs et vos services. L'un des composants les plus importants à ce titre est le réseau.

Nous allons couvrir quelques-uns des aspects que vous devez envisager lorsque vous commencez votre planification en matière d'identité et de sécurité. Si vous n'avez pas encore lu notre introduction « Le modèle de sécurité Zero Trust : adopter une stratégie de sécurité plus moderne », vous pouvez commencer par là. Cet e-book se penche de plus près sur les concepts abordés dans les deux documents mentionnés ci-dessus, pour un niveau plus avancé.

Nous couvrirons :

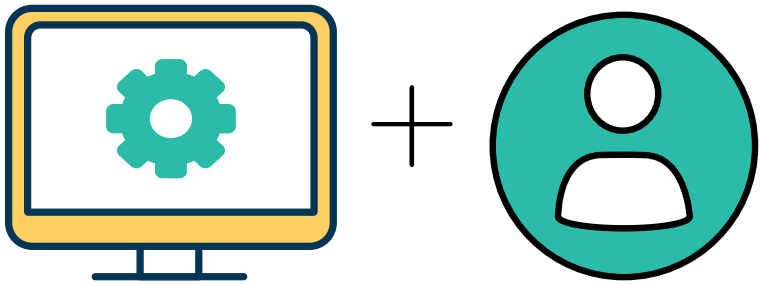
- Le fonctionnement de l'authentification moderne
- Les techniques de sécurisation du trafic réseau
- L'ajout de workflows d'accès conditionnel
- La façon dont Jamf rassemble tous ces éléments

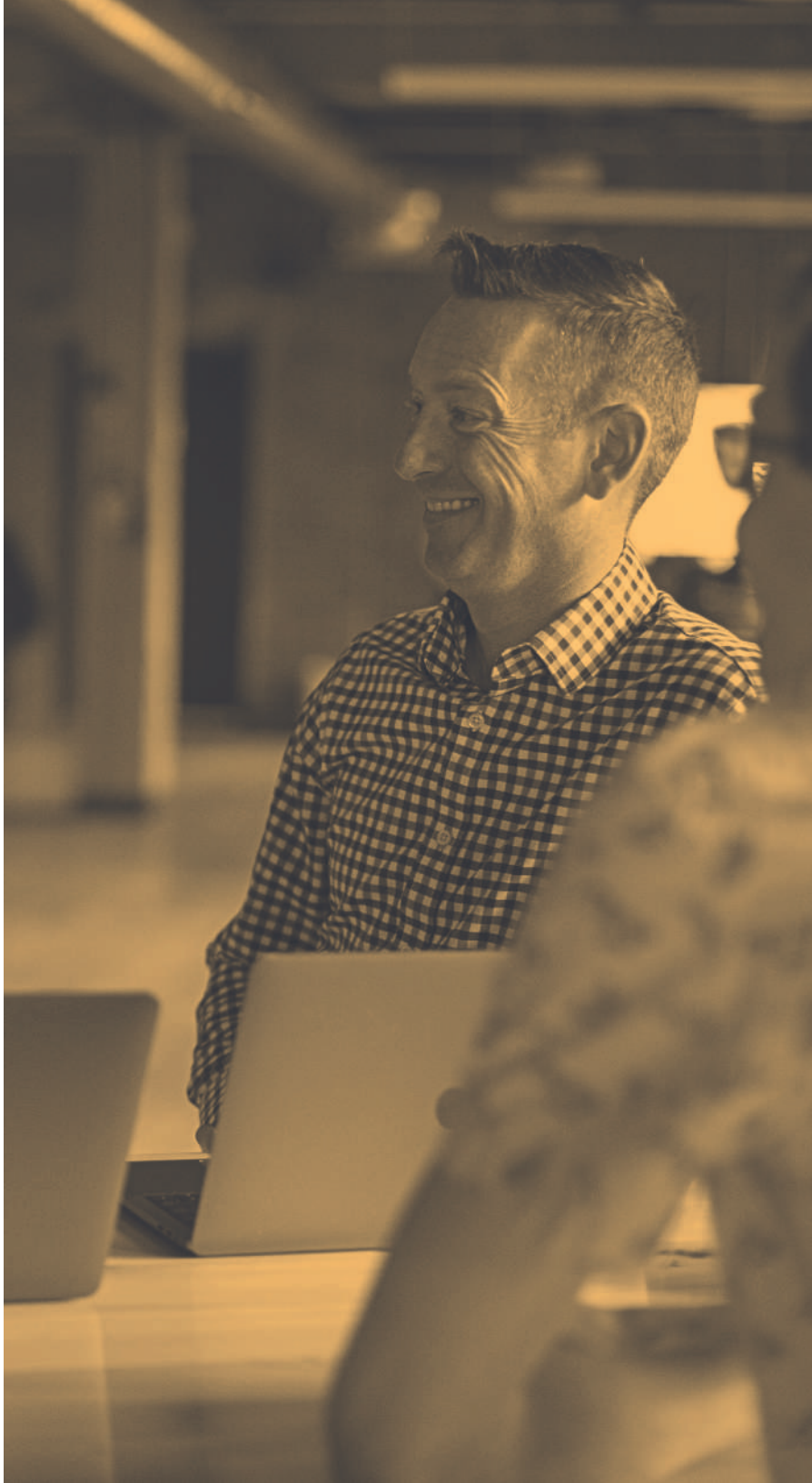


L'AUTHENTIFICATION MODERNE POUR LES IMPATIENTS

Dans notre précédent e-book « La gestion des identités pour les débutants », nous avons expliqué les différences entre autorisation et authentification. Découvrons maintenant comment les choses fonctionnent en pratique avec les services modernes qui permettent d'utiliser l'authentification unique (SSO).

Bien qu'il existe de nombreuses méthodes pour valider un utilisateur, les plus courantes aujourd'hui sont SAML (Security Assertion Markup Language) et OAuth combiné avec OIDC (OpenID Connect). Les deux systèmes accomplissent des objectifs très similaires, à savoir authentifier un utilisateur auprès d'une source de vérité, généralement appelée fournisseur d'identité (IdP), puis générer un code qui peut être partagé avec d'autres services pour prouver qui vous êtes. Si vous avez utilisé Kerberos avec Active Directory, vous constaterez qu'il existe de nombreuses similitudes ici.





L'AUTHENTIFICATION MODERNE POUR LES IMPATIENTS

Voici les points essentiels pour les administrateurs :

- L'authentification SAML génère des assertions, des blocs signés de XML qui vous identifient et permettent à d'autres services d'avoir la certitude que vous avez été authentifié.
- SAML exige que tous les services aient des certificats individuels à utiliser lors de la communication avec le fournisseur d'authentification SAML, ce qui complique l'utilisation d'applications natives ou s'exécutant sur les appareils des utilisateurs.
- OIDC fonctionne avec OAuth pour générer des jetons Web JSON (JWT) signés qui sont du JSON, et non du XML, mais qui sont fonctionnellement similaires aux assertions SAML.
- OIDC a l'avantage supplémentaire d'offrir un jeton d'identification qui est un enregistrement portable de l'utilisateur, signé pour prouver qu'il est valide.

Lors de l'authentification auprès d'un service via SAML ou OIDC/OAuth, le service n'obtient jamais réellement le mot de passe de l'utilisateur, car cette partie est uniquement gérée par votre fournisseur d'identité. Le service obtient seulement une assertion SAML ou un jeton OAuth qui est signé par le fournisseur d'identité, afin que le service puisse lui faire confiance. Bien qu'il existe de subtiles différences d'implémentation entre les deux, SAML et OIDC/OAuth fournissent des moyens très sûrs, modernes et extensibles d'authentifier un utilisateur auprès de services.

L'AUTHENTIFICATION MODERNE POUR LES IMPATIENTS

Voici un exemple d'assertion SAML :

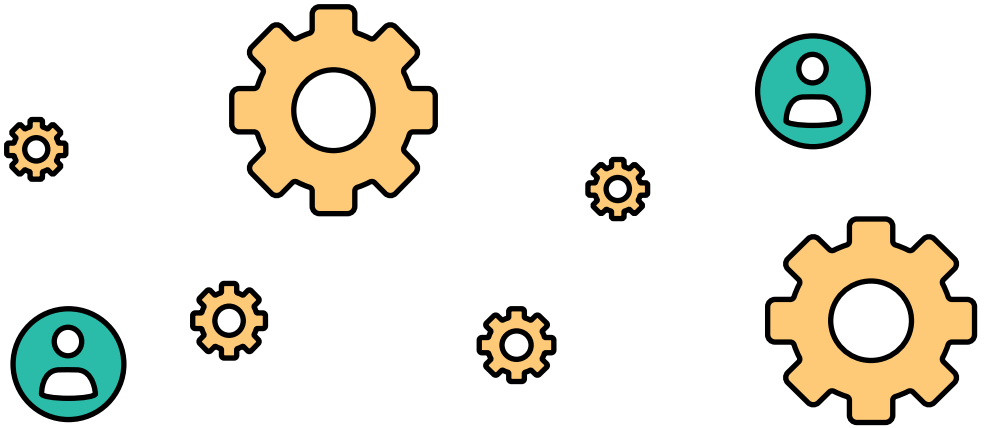
```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                     AssertionConsumerServiceURL="https://[servername].jamfcloud.com/saml/SSO"
                     Destination="https://login.microsoftonline.com/[tenant]/saml2"
                     ForceAuthn="false"
                     ID="a4a0efd7a304732928bf1bdbg2afab3"
                     IsPassive="false"
                     IssueInstant="2021-04-02T16:30:58.826Z"
                     ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                     Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://[servername].jamfcloud.com/saml/metadata</saml2:Issuer>
</saml2p:AuthnRequest>
```

À titre de comparaison, voici un exemple de jeton OAuth :

```
"app_displayname": "My Sample OIDC App Name",
  "appid": "2520beb2-535e-4e42-bf70-104cd5429551",
  "appidacr": "0",
  "family_name": "Lastname",
  "given_name": "Firstname",
  "idtyp": "user",
  "ipaddr": "52.205.5.180",
  "name": "Firstname Lastname",
  "oid": "0fa4b783-1c80-4765-b40d-c2b72de03079",
  "onprem_sid": "S-1-5-21-1861720204-2688728089-2580082577-1523",
  "platf": "5",
  "puid": "10032000ACDFC4D8",
  "rh": "0.AQ4A2rA_-GIB-UuvBjVxxpwQALK-ICVeU0JOv3AdTNVClVEOA08.",
  "scp": "User.Read profile openid email",
```

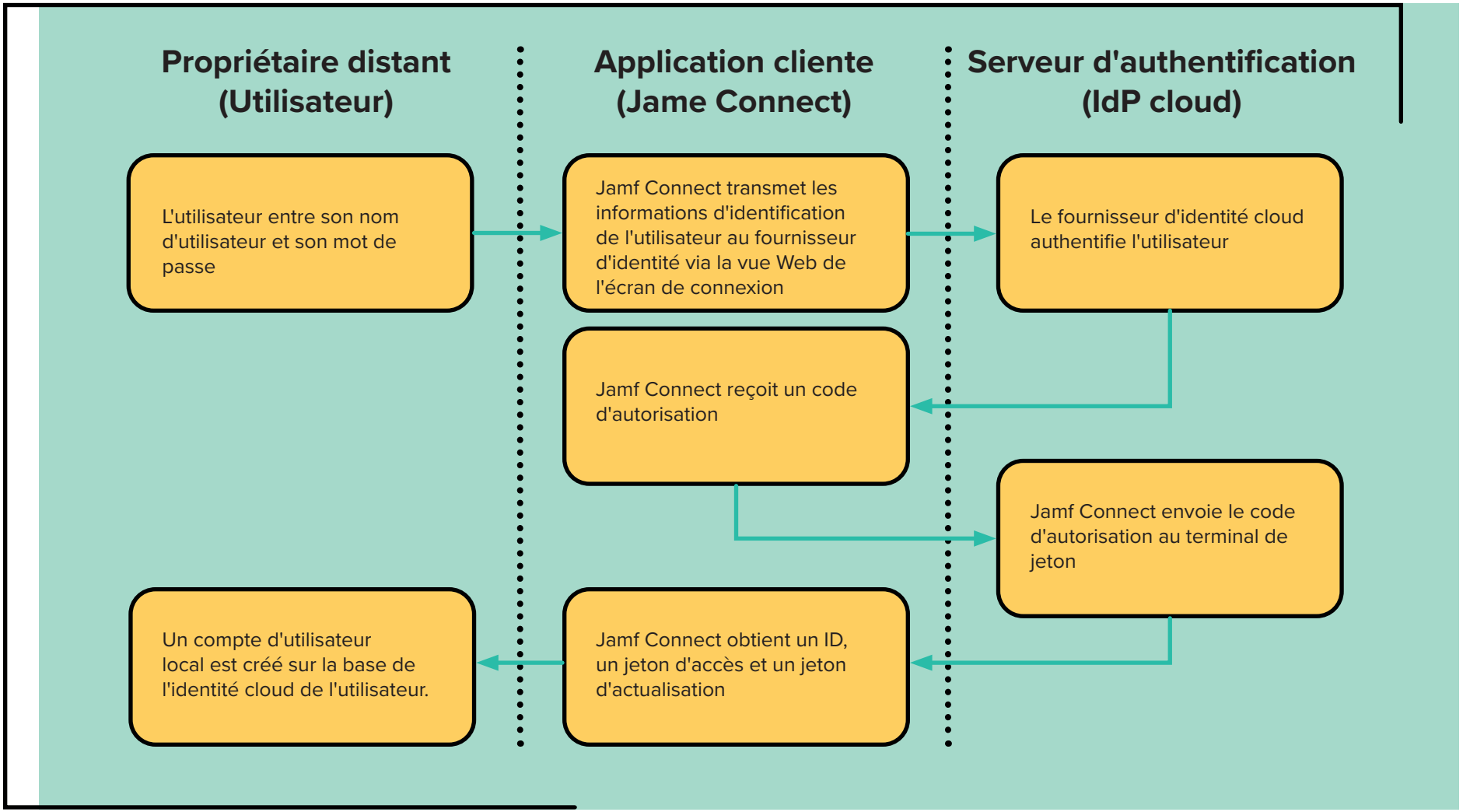
SAML et OIDC/ OAuth avec Jamf

Jamf Pro utilise SAML, tandis que Jamf Connect et Jamf Protect utilisent OIDC/ OAuth. SAML n'est pas applicable à Jamf Connect en raison de la nécessité d'avoir des certificats et de transmettre les certificats et clés privées vers des machines utilisateur auxquelles vous ne savez pas si vous pouvez faire confiance. Ainsi, Jamf prend facilement en charge l'authentification multifacteur à partir de votre fournisseur d'identité cloud, sans avoir à microgérer les utilisateurs sur chaque service.



SAML et OIDC/OAuth avec Jamf

Voici un exemple montrant comment Jamf Connect utilise l'attribution de code d'autorisation OIDC pour authentifier le nom d'utilisateur et le mot de passe cloud de l'utilisateur en échange d'un code d'autorisation, que Jamf Connect envoie au terminal de jeton de votre fournisseur d'identité.

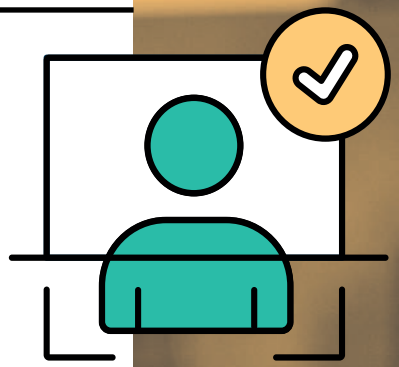


Authentification moderne et fédération des IdP

Impossible de parler d'authentification moderne sans parler de la fédération des fournisseurs d'identité. Grâce à elle, vous pouvez utiliser Azure AD avec Microsoft Office 365, alors que l'identité est réellement fédérée avec Okta : c'est votre fournisseur d'identité qui sert de source de vérité pour le mot de passe d'un utilisateur. Bien que la fédération peut devenir très compliquée et impliquer plusieurs couches de redirection, le concept de base est qu'un fournisseur d'identité peut déléguer l'authentification à un autre.

En général, les services qui peuvent s'intégrer à un fournisseur d'identité via SAML ou OIDC n'ont pas besoin de savoir si vous êtes fédéré avec un autre fournisseur. La plupart de ces détails sont extraits de la connexion initiale.

AUTHENTIFICATION MULTIFACTEUR



Penchons-nous à présent sur l'authentification multifacteur (MFA) et l'authentification sans mot de passe.

Les identifiants de connexion volés sont l'un des principaux problèmes de sécurité des entreprises. En fait, 80 % de toutes les violations de données impliquent des mots de passe volés ou faibles, mais moins de 10 % des ressources sont consacrées à l'élimination des informations d'identification compromises, d'après le Forum économique mondial. Pour lutter contre cela, de nombreuses organisations utilisent leur fournisseur d'identité pour introduire l'authentification multifacteur et la sécurité sans mot de passe.

Les fournisseurs d'identité peuvent prendre en charge une grande variété de solutions MFA et, dans une moindre mesure, sans mot de passe. Les types MFA traditionnels étaient basés sur des mots de passe à usage unique (OTP) qui obligeaient l'utilisateur à entrer un nombre différent à chaque authentification, en plus de son mot de passe. Le numéro était généré soit sur un petit porte-clés avec un écran LCD soit dans une application sur l'appareil de l'utilisateur.

Pour faciliter les choses, de nombreux fournisseurs d'identité ont maintenant leur propre application pour appareils mobiles où, après avoir entré un mot de passe, l'utilisateur reçoit une notification push et doit y répondre, généralement avec une forme d'authentification biométrique (reconnaissance faciale ou d'empreinte digitale) pour confirmer son identité.

Authentification multifacteur

Un autre type de MFA qui gagne rapidement du terrain est FIDO (Fast Identity Online), une méthode d'authentification axée sur la confidentialité et la sécurité. Elle est intégrée à la plupart des navigateurs Web modernes et peut également prendre la forme d'une clé de sécurité externe. FIDO et d'autres formes de MFA peuvent également être utilisés pour l'authentification sans mot de passe : l'utilisateur n'a pas à saisir de mot de passe car l'authentification multifacteur est utilisée pour l'ensemble du processus.

Les produits Jamf prennent en charge une grande variété d'options MFA. Étant donné que la plupart des authentifications de fournisseur d'identité sont gérées dans une vue Web, toutes les étapes de configuration et d'installation des solutions MFA sont traitées par le fournisseur d'identité lui-même.

Par exemple, Jamf Connect peut utiliser l'API d'authentification Okta pour configurer des tâches Jamf Connect pour les utilisateurs :

- Authentification cloud sur un compte local
- Synchronisation des mots de passe
- Connexion des utilisateurs à Okta

Lisez la documentation pour les développeurs d'Okta pour en savoir plus sur cette API.

AU-DELÀ DES VPN

Avant le Zero Trust, si vous vouliez protéger le trafic entre les appareils de vos utilisateurs et les services que vous fournissiez, vous utilisiez très probablement un VPN (réseau privé virtuel). Bien que les VPN restent un outil très utile pour les services informatiques, ils présentent certains inconvénients. La plupart des VPN nécessitent un logiciel client pour fonctionner, peuvent ne pas prendre en charge l'authentification cloud, nécessitent généralement du matériel dédié dans votre réseau et, surtout, au vu des tendances actuelles, ne protègent pas facilement les services dans le cloud.

La plupart des utilisateurs ayant une bande passante de plus en plus rapide chez eux, la prise en charge d'un VPN capable de gérer le trafic qu'ils génèrent peut rapidement devenir très coûteuse.

Accès réseau Zero Trust

ZTNA (Zero-Trust Network Access) est une nouvelle option de connexion sécurisée des clients aux services. Avec ZTNA, aucun VPN n'est requis. En fait, dans la plupart des cas, aucun logiciel client n'est nécessaire. Les utilisateurs se connectent via un navigateur Web à un service ZTNA qui peut nécessiter une authentification moderne, et qui sert ensuite de proxy ou sécurise d'une autre manière la connexion de l'utilisateur.

Les solutions ZTNA ont été conçues à l'origine pour protéger les services locaux anciens quand l'ajout d'une authentification moderne aurait été prohibitif. Aujourd'hui, beaucoup s'en servent également pour protéger les services cloud. Vous trouverez des solutions ZTNA qui sont elles-mêmes basées sur le cloud ou conçues pour résider dans votre propre centre de données si vous voulez plus de contrôle. À mesure que les solutions ZTNA deviennent plus robustes, vous pouvez sécuriser plus que le seul trafic Web. Cela vous offre l'opportunité de réellement abandonner le VPN pour sécuriser l'accès à votre réseau.

ACCÈS CONDITIONNEL

Une architecture Zero Trust robuste comprendra souvent des éléments d'accès conditionnel ou de confiance d'appareil. Dans ces situations, l'état de l'appareil lui-même est pris en compte dans la décision de faire confiance ou non à la connexion. Les appareils gérés aident les entreprises à mieux comprendre les risques liés aux appareils et à décider quels utilisateurs de confiance, sur des appareils de confiance et utilisant des applications de confiance peuvent accéder aux données et aux ressources.

L'accès conditionnel implique généralement une collaboration entre votre fournisseur d'identité et un agent local ou votre solution de gestion des appareils pour déterminer quelle version du système d'exploitation l'appareil utilise, quelles politiques de sécurité sont en place ou un certain nombre d'autres attributs qui aident à déterminer la posture de sécurité de l'appareil. Le fournisseur d'identité peut alors autoriser la connexion ou, dans certains cas, exiger une authentification supplémentaire, par exemple avec l'authentification multifacteur (MFA), avant de valider complètement l'utilisateur.

L'accès conditionnel, comme son nom l'indique, est conditionné en fonction de l'application qu'un utilisateur tente d'utiliser. Pour les services à faible sécurité, comme l'accès à un système de tickets de support informatique, vous n'avez peut-être pas besoin de MFA. Cependant, l'accès à un référentiel de code source peut nécessiter non seulement que l'utilisateur s'authentifie, mais aussi qu'il utilise un appareil appartenant à et géré par l'entreprise.

Accès conditionnel

Il existe un certain nombre de fournisseurs qui permettent de gérer l'identité et l'accès aux services, comme Centrify, Duo Security, Microsoft, Ping Identity, Okta et Salesforce. Beaucoup de ces outils fonctionnent avec les infrastructures d'authentification existantes, comme votre fournisseur d'identité cloud, et étendent ces identités aux services cloud à l'aide des protocoles décrits ci-dessus : OIDC et SAML.

Prenons un exemple de la façon dont Jamf fonctionne avec Microsoft pour obtenir un accès conditionnel. Jamf Pro peut appliquer des stratégies sur les appareils afin d'accéder à Microsoft Office 365 en tirant parti de l'accès conditionnel Enterprise Mobility + Security (EMS). Les ordinateurs Mac gérés par Jamf ont désormais accès aux applications Microsoft, à condition qu'ils respectent les politiques de conformité des appareils Microsoft Endpoint Manager. Une fois que les données du Mac sont dans le cloud, Endpoint Manager et EMS peuvent s'intégrer pleinement à Jamf pour donner accès aux capacités de gestion sur l'appareil. Si un Mac non géré demande l'accès à la messagerie électronique ou à d'autres services cloud, le service informatique peut activer un processus d'inscription lancé par l'utilisateur à partir de Jamf Pro et s'assurer que les appareils non sécurisés ou non gérés sont inscrits dans la gestion avant de se voir accorder l'accès.

ACCÈS CONDITIONNEL

Une fois les informations d'identification de l'utilisateur vérifiées par Microsoft et celles de l'appareil par Jamf, une analyse du risque de l'utilisateur, de l'appareil (est-il conforme à la stratégie de l'organisation ?) et de l'application (quelle application est utilisée ?) est exécutée pour déterminer s'il convient d'accorder ou de bloquer l'accès à partir des ressources cloud. Tout cela se déroule en temps réel.

Les organisations bénéficient désormais d'une extension de l'authentification multifacteur grâce à une conformité vérifiée :

1. Nom d'utilisateur et mot de passe
2. Code et jeton
3. Conformité des appareils

Cela permet aux organisations de fournir de manière contextuelle et dynamique le bon accès en fonction de l'utilisateur, de l'appareil et du cadre de ce cas d'utilisation. De cette façon, elles peuvent efficacement offrir le périmètre flexible que les travailleurs multi-appareils et multi-sites exigent aujourd'hui.

SÉCURITÉ DES TERMINAUX

Les mesures de sécurité mises en œuvre par la gestion des identités affectent à la fois les utilisateurs finaux et les équipes informatiques tout au long du cycle de vie des employés, qu'ils travaillent sur place ou à distance. Les applications SaaS et la connexion des employés aux ressources de l'entreprise offrent la possibilité d'atténuer les risques pour vos terminaux, vos utilisateurs et les données de votre entreprise.

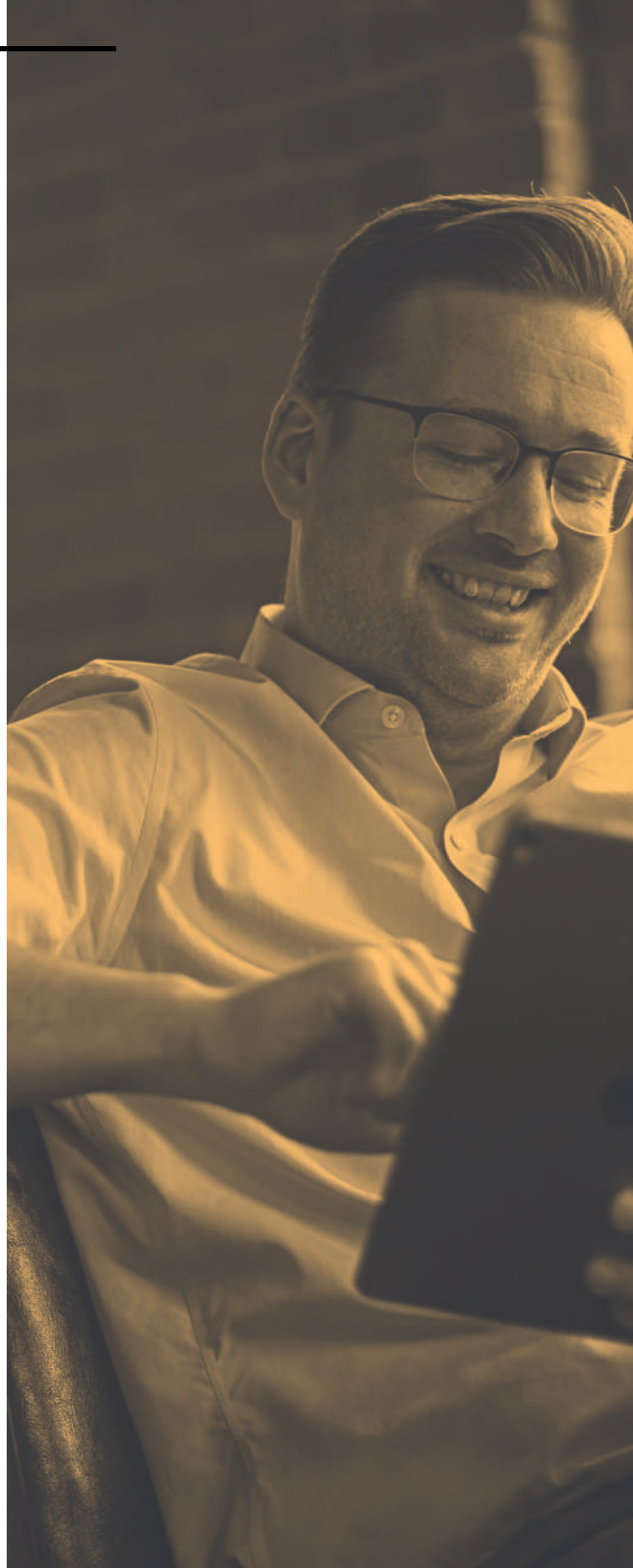
La sécurité des terminaux est la pratique consistant à atténuer les risques d'exploitation par des acteurs malveillants pour les appareils ou terminaux des utilisateurs finaux. Il devient de plus en plus important de s'assurer que les appareils et les données sont utilisés à des fins légitimes par des utilisateurs autorisés, en particulier quand les données sont distribuées dans diverses applications SaaS. Pour atteindre cet objectif, de nombreux rouages doivent s'activer ensemble. La gestion des identités en est un exemple, mais citons également l'antivirus (AV), la gestion de la configuration de la sécurité ou encore la détection des terminaux.

Sécurité des terminaux

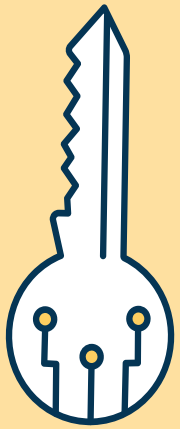
Les organisations ne peuvent pas attendre que des logiciels malveillants, publicitaires ou autrement indésirables apparaissent et espérer régler le problème avec des outils de sécurité qui nuisent plus à l'appareil qu'ils ne le protègent, tout en affectant la productivité. Elles doivent songer à implémenter un AV qui identifie et atténue efficacement les attaques spécifiques à Mac sans gaspiller de ressources précieuses à chercher des menaces propres à Windows. La sécurité englobe un grand nombre de sujets. La bonne nouvelle est que Jamf peut vous aider avec tout cela.

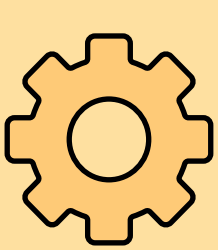
En plus des capacités de gestion des identités de Jamf Connect et des outils de sécurité intégrés de Jamf Pro, Jamf Protect est conçu pour s'intégrer de manière transparente dans le paysage de sécurité de votre organisation afin de bloquer les logiciels malveillants macOS, vous protéger contre les menaces spécifiques à Mac et surveiller la conformité des terminaux.

Pour les organisations qui ont des environnements plus complexes avec une variété d'outils de sécurité, examinons à nouveau la combinaison des capacités de Microsoft et de Jamf. Les administrateurs informatiques et les équipes de sécurité peuvent avoir une visibilité complète sur les activités de sécurité de leur flotte Mac à partir de la vitrine unique qu'ils connaissent déjà. Jamf Protect pousse nativement toutes les données de sécurité et alertes spécifiques à Mac directement dans Azure Sentinel avec une configuration minimale. Toutes les activités malveillantes ou suspectes sur Mac, ainsi que les notifications liées aux logiciels malveillants s'intègrent facilement aux flux de travail préexistants. Les efforts et le temps requis pour le personnel de sécurité et informatique sont donc minimaux. Grâce à la détection des attaques et aux informations de journal de Jamf Protect, Azure Sentinel peut étendre ses capacités pour identifier et corriger les attaques à grande échelle contre tous les appareils Mac, tout en maintenant une meilleure sécurité pour l'organisation dans son ensemble.



Il est clair que le modèle de sécurité traditionnel basé sur le périmètre doit être repensé. Les entreprises peuvent atteindre une sécurité moderne et même le Zero Trust tout en travaillant avec les partenaires qui leur fournissent déjà des identités. Les gens se déplacent, les données circulent et les organisations ont besoin de solutions modernes pour faire face à ces changements. Elles doivent penser à la sécurité basée sur les appareils, à la sécurité basée sur l'utilisateur, à l'authentification multifacteur, et tout ce qui se trouve au-delà. Elles doivent sécuriser leurs terminaux.





Jamf offre un moyen de lier tous ces éléments. La meilleure sécurité commence ici !

Lancez-vous