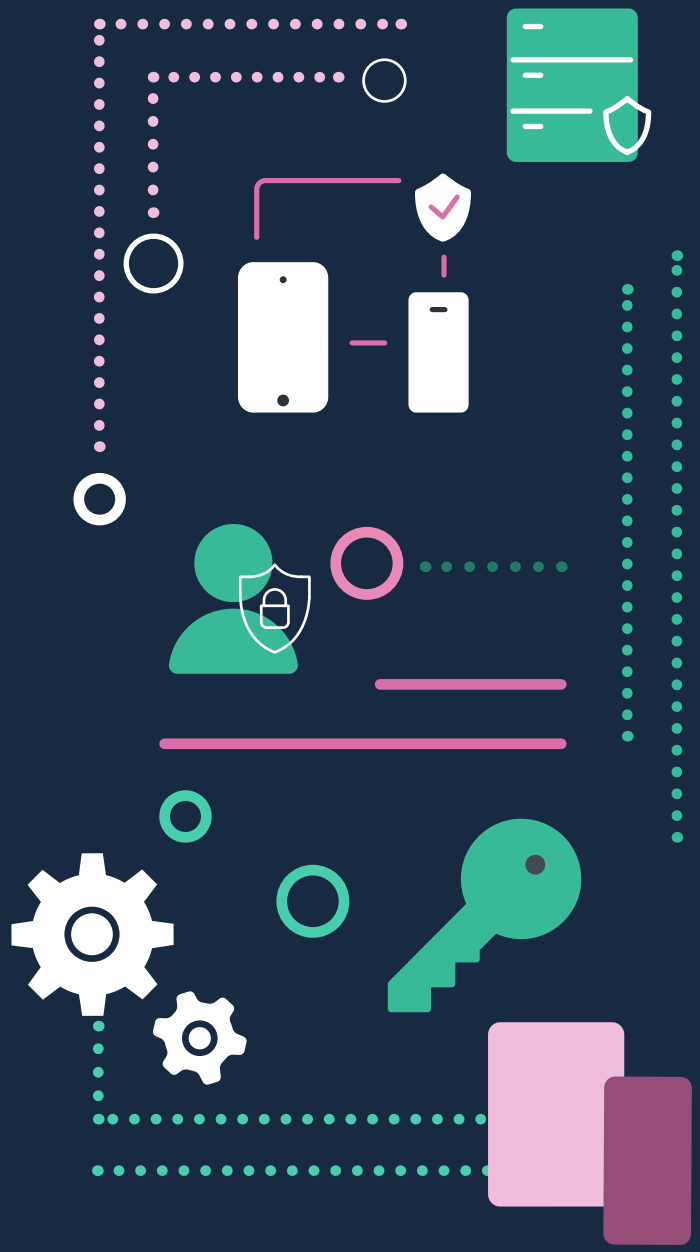


jamf

Gestion des identités et sécurité

guide avancé

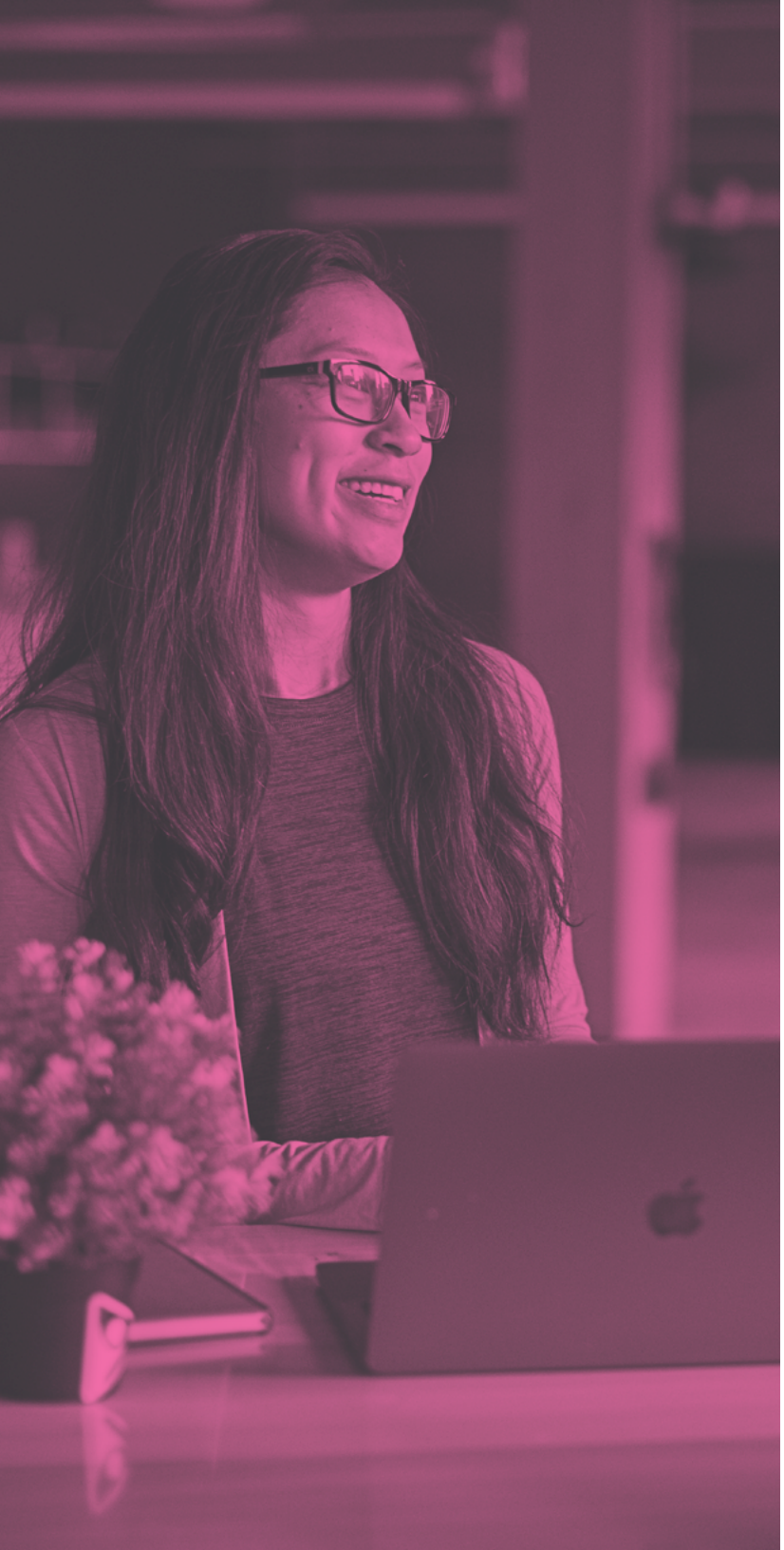
CHAQUE EMPLOYÉ A SA PROPRE IDENTITÉ

L'importance de la gestion des identités est devenue évidente au cours de la dernière décennie, en particulier dans les organisations qui doivent répondre aux besoins d'une main d'œuvre mobile. La migration vers le cloud a permis à d'innombrables organisations de faire un pas de plus vers une gestion moderne des identités. Nous avons d'ailleurs abordé ce sujet dans Introduction à la gestion des identités. Mais la gestion des identités va bien au-delà de l'authentification et de l'autorisation : aujourd'hui, les organisations cherchent à s'appuyer sur l'identité des utilisateurs pour atteindre leurs objectifs de sécurité zero-trust.

L'un des grands principes du zero-trust consiste à refuser votre confiance à la plupart des composants qui assurent la liaison entre vos utilisateurs et vos services. À commencer par le réseau, composant essentiel auquel vous ne pouvez et ne devez jamais faire confiance. Pour vous aider dans cette démarche, nous allons passer en revues les technologies et les aspects à prendre en compte pour planifier la gestion de vos identités et votre sécurité. Si vous n'avez pas encore lu notre introduction Le modèle de sécurité Zero Trust, c'est un excellent point de départ. Cet e-book va approfondir les concepts abordés dans les deux documents mentionnés plus haut pour les porter à un niveau plus avancé.

DANS CE GUIDE, NOUS ALLONS VOIR :

- Comment fonctionne l'authentification moderne
- Les techniques de sécurisation du trafic réseau
- Comment ajouter des workflows d'accès conditionnel
- Comment Jamf combine toutes ces fonctions



L'AUTHENTIFICATION MODERNE POUR LES IMPATIENTS

Dans notre précédent e-book, Introduction à la gestion des identités, nous avons abordé les différences entre l'autorisation et l'authentification. Voyons maintenant comment cela se passe concrètement avec les services modernes d'authentification unique (SSO).

Il existe de nombreuses méthodes pour valider un utilisateur. Mais aujourd'hui, les plus courantes sont SAML (Security Assertion Markup Language) et OAuth combiné à OIDC (OpenID Connect). Ces deux systèmes poursuivent des objectifs très similaires : 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 son identité. Si vous connaissez Kerberos pour avoir travaillé avec Active Directory, vous comprenez de quoi il s'agit.

L'AUTHENTIFICATION MODERNE POUR LES IMPATIENTS

EN TANT QU'ADMINISTRATEUR, VOICI LES POINTS ESSENTIELS QUI VOUS CONCERNENT :

- L'authentification SAML génère des assertions. Ces blocs XML signés vous identifient et permettent à d'autres services d'avoir confiance dans votre authentification.
- Dans le cas de SAML, tous les services doivent disposer de certificats individuels pour communiquer avec le fournisseur d'authentification SAML. Cela complique l'utilisation des applications natives ou exécutées sur les appareils des utilisateurs.
- OIDC s'appuie sur OAuth pour générer des JWT (jetons web JSON) signés au format JSON et non XML, similaires par leur fonction aux assertions SAML.
- OIDC présente un avantage supplémentaire : le jeton d'identification, qui est toujours un JWT. C'est une sorte d'enregistrement d'utilisateur portable, et sa validité est, là aussi, attestée par une signature.

Lors de l'authentification auprès d'un service via SAML ou OIDC/ OAuth, le service ne reçoit jamais le mot de passe de l'utilisateur, qui n'est géré que par votre IdP. Il reçoit à la place une assertion SAML ou un jeton OAuth, signé par l'IdP pour obtenir la confiance du service. Les détails de mise en œuvre varient d'un système à l'autre, mais SAML et OIDC/OAuth fournissent tous deux des moyens très sûrs, modernes et extensibles d'authentifier un utilisateur auprès des 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="a4a9efd7a384732928bf1bdbg2afab3"
                     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 :

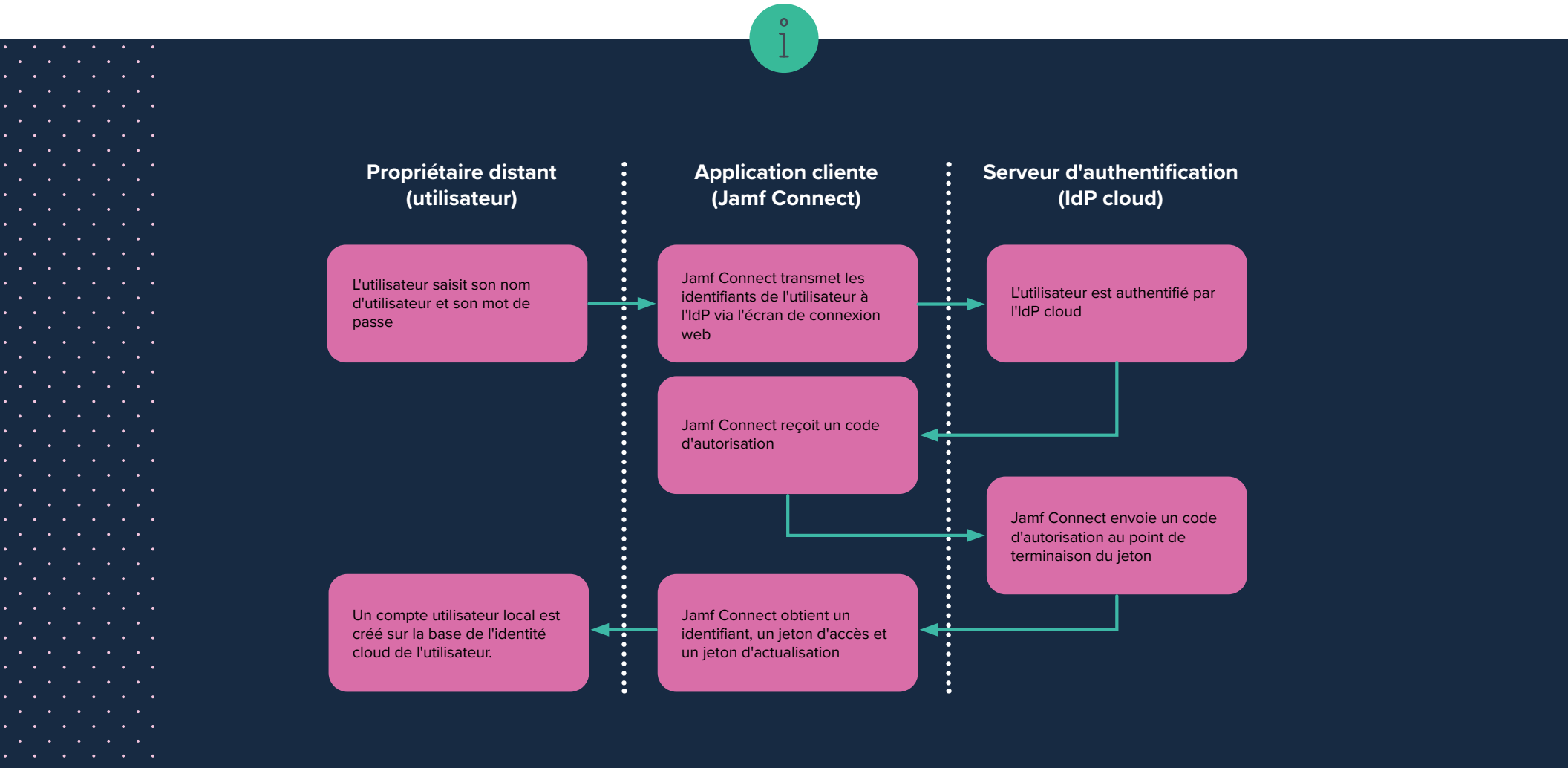
```
"app_displayname": "My Sample OIDC App Name",
  "appid": "2520beb2-535e-4e42-bf70-1d4cd5429551",
  "appidacr": "0",
  "family_name": "Lastname",
  "given_name": "Firstname",
  "idtyp": "user",
  "ipaddr": "52.205.5.180",
  "name": "Firstname Lastname",
  "oid": "0fa4b783-1c00-4765-b40d-c2b72de03079",
  "onprem_sid": "S-1-5-21-1861720204-2608728089-2580082577-1523",
  "platf": "5",
  "puid": "100320004CDFC4DB",
  "rh": "0.AQ4A2rA-GiB-Uuy8iVxxpwOALK-ICVeU0JOy3AdTNVClVFOAQ8.",
```

*Remarque : il s'agit d'une représentation partielle du jeton, et non d'un échantillon complet.

SAML ET OIDC/OAUTH AVEC JAMF

Jamf Pro utilise SAML, tandis que Jamf Connect et Jamf Protect utilisent OIDC/OAuth. Jamf Connect ne peut pas utiliser SAML parce qu'il faudrait transmettre des certificats et des clés privées aux appareils des utilisateurs sans savoir s'ils sont fiables. Au final, Jamf prend aisément en charge l'authentification multifacteur à partir de votre IdP cloud, sans avoir à gérer les utilisateurs sur chaque service.

Nous allons voir, à travers un exemple, comment Jamf Connect utilise un code d'autorisation OIDC pour authentifier le nom d'utilisateur et son mot de passe cloud en échange d'un autre code d'autorisation, envoyé par Jamf Connect au point de terminaison de jeton de votre IdP.



L'AUTHENTIFICATION MODERNE ET LA FÉDÉRATION DES IDP

On ne peut pas parler d'authentification moderne sans aborder le sujet de la fédération des IdP. Par exemple, vous utilisez peut-être Azure AD avec Microsoft Office 365. Mais en réalité, l'identité est fédérée avec Okta, car c'est votre IdP qui détient la « vérité » sur le mot de passe d'un utilisateur. La fédération peut être très complexe et impliquer de multiples couches de redirection. Pour résumer, le principe de base est qu'un IdP peut transmettre une authentification à un autre IdP.

La plupart du temps, les services capables de s'intégrer à un IdP via SAML ou OIDC n'ont pas besoin de savoir si vous êtes fédéré avec un autre fournisseur. Ces détails sont, pour l'essentiel, abstraits de la connectivité initiale.

AUTHENTIFICATION MULTIFACTEUR

Puisque nous avons parlé des méthodes d'authentification, nous devons également mentionner l'authentification multifacteur (AMF) et l'authentification sans mot de passe.

Le vol d'identifiants de connexion est un problème de sécurité majeur pour les organisations aujourd'hui. En effet, 80 % des violations concernent des mots de passe volés ou faibles. Pourtant, selon le Forum économique mondial, moins de 10 % des dépenses sont consacrées à la lutte contre la compromission des identifiants. Pour lutter contre ce phénomène, de nombreuses organisations s'appuient sur leur fournisseur d'identité pour introduire l'AMF et la sécurité sans mot de passe.

Les IdP prennent en charge une grande variété de solutions d'AMF mais aussi quelques solutions sans mot de passe. Les méthodes traditionnelles d'AMF reposent sur des mots de passe à usage unique (OTP) : en plus de son mot de passe, l'utilisateur doit saisir un code numérique à durée de vie très courte. Ce code peut être généré sur un petit porte-clés avec un écran LCD, ou par une application sur un appareil personnel.

Pour faciliter la tâche des utilisateurs, de nombreux fournisseurs d'identité proposent désormais leur propre application pour smartphone. Après avoir saisi son mot de passe, l'utilisateur reçoit une notification push sur l'appareil, à laquelle il doit généralement répondre par une forme d'authentification biométrique, comme Face ID ou Touch ID, afin de confirmer son identité.

Autre type d'AMF de plus en plus populaire, le FIDO (Fast Identity Online) est 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. Le FIDO, comme d'autres formes d'AMF, peut aussi servir à l'authentification sans mot de passe. L'utilisateur ne saisit aucun mot de passe : l'AMF est utilisée pour l'ensemble du processus.

Les produits Jamf sont compatibles avec une grande variété d'AMF. Dans la mesure où la plupart des authentifications IdP sont gérées dans une vue web, toute la configuration de l'AMF est gérée par l'IdP lui-même.

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

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

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

AU-DELÀ DES VPN

Avant l'avènement du zero-trust, si vous vouliez protéger le trafic entre les appareils de vos utilisateurs et vos services, vous aviez très probablement recours à un VPN (réseau privé virtuel). Si le VPN reste un outil très utile pour le service informatique, il présente néanmoins quelques inconvénients :

- La plupart des VPN nécessitent un logiciel client pour fonctionner
- Il n'est pas toujours compatible avec l'authentification cloud.
- Il nécessite généralement l'installation d'un équipement dédié dans votre réseau et ne protège pas toujours les services basés sur le cloud.
- Les utilisateurs ont souvent une mauvaise expérience sur mobile.

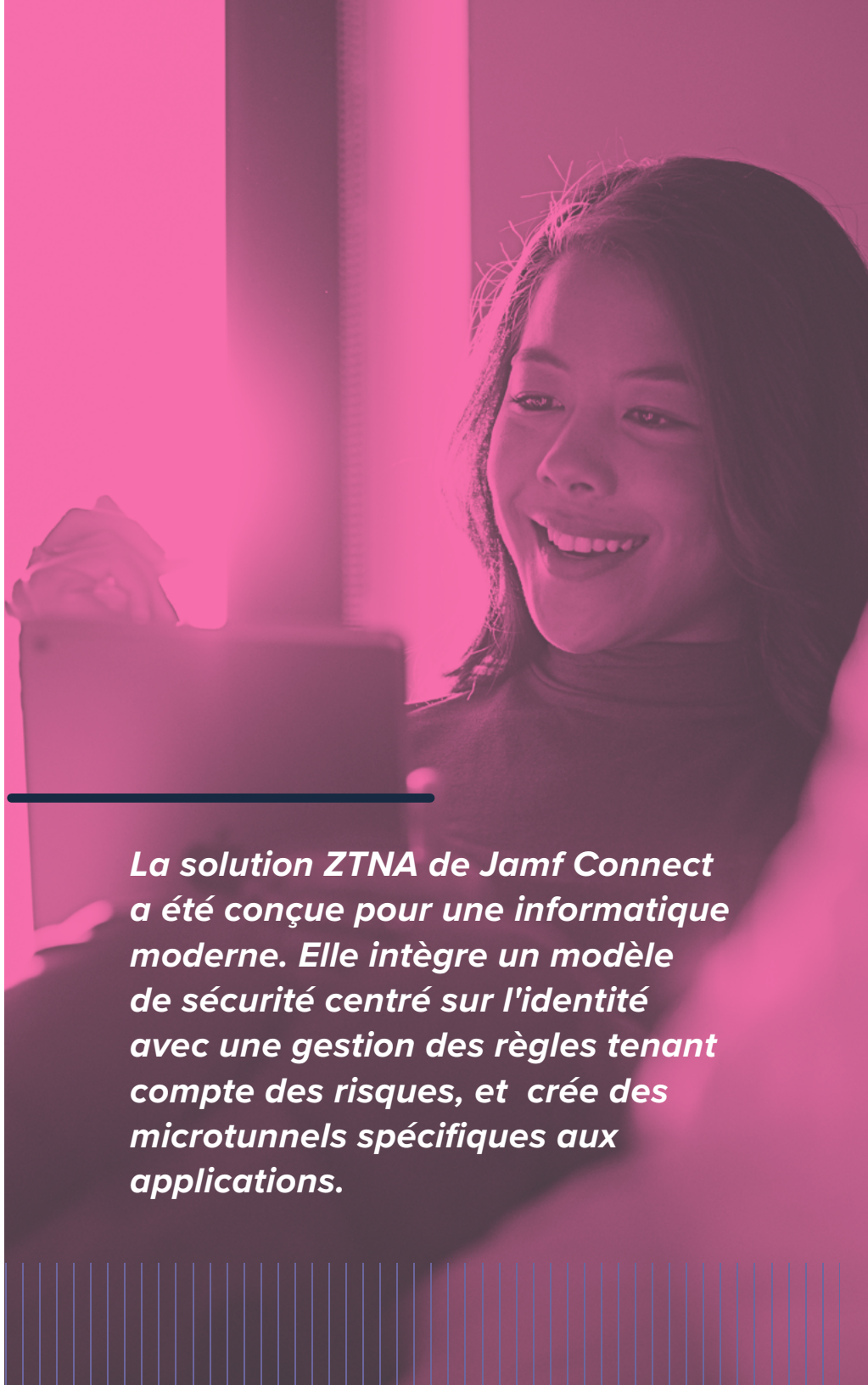
La plupart des utilisateurs ont désormais une connexion à haut débit à leur domicile, et un VPN capable de gérer ce volume de trafic peut rapidement devenir très coûteux.

ACCÈS RÉSEAU ZERO-TRUST

Plus récent, l'accès réseau Zero-Trust (ZTNA) sécurise la connexion entre les clients et les services. Avec le ZTNA, aucun VPN n'est nécessaire – ni même, dans la plupart des cas, aucun logiciel client. L'utilisateur se connecte par le biais d'un navigateur web à un service ZTNA qui peut exiger une authentification moderne. Le service établit ensuite la connexion via un proxy ou autre moyen de sécurisation.

À l'origine, les solutions ZTNA ont été conçues pour protéger les services traditionnels sur site – l'ajout d'une authentification moderne aurait été prohibitif. Mais aujourd'hui, nombre d'entre elles protègent également les services basés dans le cloud au besoin. Vous trouverez des solutions ZTNA elles-mêmes basées sur le cloud, et d'autres conçues pour résider dans votre propre centre de données pour davantage de contrôle. Les solutions ZTNA deviennent plus robustes, et vous pouvez maintenant sécuriser davantage que le seul trafic web. Vous pouvez donc vous passer du VPN pour sécuriser l'accès à votre réseau.

Découvrez le ZTNA avec Jamf.



La solution ZTNA de Jamf Connect a été conçue pour une informatique moderne. Elle intègre un modèle de sécurité centré sur l'identité avec une gestion des règles tenant compte des risques, et crée des microtunnels spécifiques aux applications.

ACCÈS CONDITIONNEL

Une architecture zero-trust robuste comprend souvent des éléments d'accès conditionnel ou de confiance dans les appareils. Dans ce cas, l'état de l'appareil lui-même entre en ligne de compte dans l'évaluation de la fiabilité de la connexion. La gestion des appareils aide les organisations à mieux comprendre les risques liés aux appareils. Grâce à cela, elle peut décider quelles personnes de confiance, utilisant des appareils et des applications fiables, doivent avoir accès aux données et aux ressources.

Généralement, l'accès conditionnel s'appuie à la fois sur votre IdP et sur un agent local ou votre solution de gestion des appareils. Il détermine ainsi la version de l'OS de l'appareil, les règles de sécurité éventuellement en place, et d'autres critères permettant de déterminer la posture de l'appareil. L'IdP peut alors autoriser la connectivité ou, dans certains cas, exiger une authentification supplémentaire – AMF, par exemple – avant d'authentifier complètement l'utilisateur.

L'accès conditionnel, comme son nom l'indique, dépend de l'application que l'utilisateur tente d'utiliser. Certains services peu risqués, comme les systèmes de tickets d'assistance, n'ont pas besoin d'AMF. En revanche, pour accéder à un dépôt de code source, on exigera du demandeur qu'il réussisse un défi AMF, mais aussi qu'il utilise un appareil sous le contrôle de l'entreprise.

Plusieurs fournisseurs facilitent la gestion des identités et des accès aux services, notamment Centrify, Duo Security, Microsoft, Ping Identity, Okta et Salesforce. Bon nombre de ces outils sont compatibles avec l'infrastructure d'authentification existante, comme votre fournisseur d'identité cloud. Ils étendent l'utilisation des identités aux services cloud grâce aux protocoles évoqués plus haut, OIDC et SAML.

Voyons, par exemple, comment Jamf fonctionne avec Microsoft pour fournir un accès conditionnel. Jamf Pro peut appliquer des règles aux appareils pour gérer l'accès à Microsoft Office 365 en tirant parti de l'accès conditionnel Enterprise Mobility + Security (EMS). Les ordinateurs Mac gérés par Jamf ont maintenant accès aux applications Microsoft, dès lors qu'ils respectent les règles de conformité établies par Microsoft Endpoint Manager. Une fois que les données du Mac sont dans le cloud, Endpoint Manager et EMS s'intègrent entièrement à Jamf pour fournir des capacités de gestion sur l'appareil. Si un Mac non géré demande l'accès à la messagerie ou à d'autres services cloud, le service informatique peut activer un processus d'inscription à l'initiative de l'utilisateur à partir de Jamf Pro. Ce faisant, il s'assure que les appareils non sécurisés ou non gérés sont inscrits dans la solution de gestion avant d'accéder à quoi que ce soit.

L'ACCÈS CONDITIONNEL JAMF PREND EN CHARGE NON SEULEMENT MICROSOFT, MAIS AUSSI LES PRINCIPAUX LEADERS DU SECTEUR COMME GOOGLE ET AWS.

Une fois l'utilisateur vérifié par Microsoft et l'appareil contrôlé par Jamf, le système procède à une analyse du risque lié à l'utilisateur, à l'appareil (conformité aux règles de l'organisation) et à l'application. Il détermine ensuite s'il faut accorder ou bloquer l'accès aux ressources cloud, le tout en temps réel

Les organisations bénéficient désormais d'une extension de l'authentification multifacteur par le biais de la vérification de conformité :

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

Aujourd'hui, les employés utilisent plusieurs appareils et travaillent depuis plusieurs endroits. Les organisations peuvent maintenant fournir dynamiquement un accès adapté au contexte, en fonction de l'utilisateur, de l'appareil et du cas d'utilisation, et créer ainsi un périmètre adaptatif et flexible.

SÉCURITÉ DES TERMINAUX

Les mesures de sécurité mises en œuvre dans le cadre de la gestion des identités concernent à la fois les utilisateurs finaux et le service informatique tout au long du cycle de vie des employés, sur place comme en télétravail. Les applications SaaS et la connexion des employés aux ressources de l'entreprise sont autant d'occasions de limiter les risques pour vos terminaux, vos utilisateurs et les données.

La sécurité des terminaux vise à atténuer les risques d'exploitation des appareils des utilisateurs finaux par des acteurs malveillants. Il devient absolument indispensable de veiller à ce que les appareils et les données soient utilisés à des fins légitimes par des utilisateurs autorisés, surtout quand ces données sont réparties dans diverses applications SaaS. Pour atteindre cet objectif, de nombreuses composants doivent fonctionner ensemble : la gestion des identités, bien sûr, mais aussi les antivirus, la gestion des configurations de sécurité, la détection des terminaux et la réponse de sécurité.

Les organisations ne peuvent pas attendre que des logiciels malveillants, publicitaires ou indésirables se manifestent. Quant aux outils de sécurité qui ralentissent l'appareil plus qu'ils ne le protègent, ils ne font qu'entraver la productivité de l'utilisateur final. Elles doivent envisager d'implémenter un antivirus qui identifie et résout efficacement les attaques spécifiques aux Mac, sans perdre des ressources à rechercher des menaces conçues pour Windows. La sécurité englobe d'innombrables facteurs, mais nous avons une bonne nouvelle : Jamf peut vous aider dans tous ces domaines.

En plus des capacités de gestion des identités de Jamf Connect et des outils de sécurité intégrés de Jamf Pro, Jamf Protect s'intègre de manière transparente au paysage de sécurité de votre entreprise. Notre solution prévient les logiciels malveillants, vous protège contre les menaces spécifiques à Apple et surveille la conformité de vos terminaux.

Pour les environnements sont plus complexes, qui disposent d'une grande variété d'outils de sécurité, penchons-nous à nouveau sur la combinaison de Microsoft et de Jamf. Pour les administrateurs informatiques et les équipes de sécurité, elle offre une visibilité complète sur les activités de sécurité de l'ensemble de la flotte Mac, à partir d'un seul et même écran. Jamf Protect transfère nativement toutes les données et alertes de sécurité spécifiques aux Mac dans Azure Sentinel, sans configuration complexe. Toutes les activités malveillantes ou suspectes sur Mac, notifications de logiciels malveillants incluses, s'intègrent aux workflows préexistants, ne demandant ainsi que très peu de travail à votre équipe de sécurité. Grâce à la détection des attaques et aux informations de journal fournies par Jamf Protect, Azure Sentinel peut identifier et remédier à de larges attaques ciblant tous les appareils Mac de l'environnement d'un client, tout renforçant la sécurité de l'ensemble de l'organisation.

RÉALIGNEZ VOTRE POSTURE DE SÉCURITÉ AVEC L'IDENTITÉ

C'est une évidence : il est temps de repenser le modèle de sécurité traditionnel, basé sur le périmètre. En s'appuyant sur les partenaires qui fournissent déjà les identités, les organisations peuvent mettre en place une sécurité moderne et appliquer le principe zero-trust. Les gens ont changé, les données aussi, et les organisations ont besoin de solutions modernes pour faire face à ces évolutions. La sécurité basée sur l'appareil, la sécurité basée sur l'utilisateur, l'authentification multifacteur... toutes ces approches doivent être envisagées. Il faut sécuriser les terminaux.

L'offre Jamf permet de faire le lien entre tous ces éléments. L'amélioration de la sécurité commence ici.

Commencez avec un essai gratuit

ou contactez votre distributeur habituel pour commencer.