jamf

ZTNA et Trusted Access :

Les bonnes pratiques de conformité en matière d'identité, d'accès et de sécurité

Le concept de zero-trust est rapidement devenu incontournable dans le monde de la cybersécurité. Selon le rapport **L'État de la sécurité zero-trust 2022 d'Okta**, le pourcentage d'entreprises ayant des projets de développement ou de mise en œuvre du zero-trust sur les 12 à 18 prochains mois est passé de 16 % en 2019 à 97 % en 2022. Pendant la pandémie, la généralisation du télétravail a fait disparaître le périmètre du réseau et fait de l'architecture zero-trust, jusque-là un luxe, une véritable nécessité.

L'accès réseau zero-trust, ou ZTNA, est un pilier de la mise en œuvre du zero-trust. Si l'architecture zero-trust est la forteresse labyrinthique qui abrite votre réseau, le ZTNA est la garnison qui vérifie l'identité de tous les visiteurs, leur ouvre la porte et les escorte jusqu'aux salles dont l'entrée leur est autorisée. Si les intentions de l'invité deviennent suspectes à un moment ou à un autre, il est immédiatement expulsé des lieux et sa permission est révoquée.

Au-delà des analogies médiévales, il est essentiel de comprendre le ZTNA pour faire progresser la cybersécurité.

Dans cet article, nous abordons plusieurs aspects clés :

- Octroi des accès selon le principe du moindre privilège
- Vérification de l'identité grâce à l'authentification multifacteur (AMF) et aux fournisseurs d'identité Cloud (IdP).
- Conformité et sécurité
- Accompagnement de l'utilisateur final

Accès selon le principe du moindre privilège

Le principe du moindre privilège est simple : les utilisateurs et leurs appareils n'ont accès qu'à ce qui est nécessaire à leur fonction, et rien de plus. Certes, cela implique de tenir des registres : il faut savoir qui a besoin d'accéder à quoi et qui dispose actuellement de cet accès. En revanche, vous évitez de payer pour des licences inutiles. Mais la véritable puissance de cette approche réside dans la réduction de votre surface d'attaque : si vous limitez le nombre d'utilisateurs autorisés, vous réduisez également le nombre de comptes susceptibles de compromettre votre réseau via une ressource donnée. Et comme les utilisateurs n'ont pas accès à l'ensemble de votre réseau, vous réduisez encore le risque de mouvement latéral en cas d'infiltration par un acteur malveillant.

Le ZTNA applique le principe du moindre privilège en créant un périmètre défini par logiciel (SDP). Le SDP ne sépare pas les connexions réseau en s'appuyant sur un VLAN ou une adresse réseau : grâce au « split-tunneling », il n'accorde l'accès qu'au groupe de ressources qui lui ont été attribuées, où qu'il se trouve sur le réseau de l'entreprise. Les ressources auxquelles il n'a pas le droit d'accéder restent invisibles et inaccessibles.

Identité : authentification et autorisation

Le ZTNA repose sur l'identité. « Ne jamais faire confiance, toujours vérifier » : le mantra du zero-trust nous rappelle qu'il faut toujours contraindre les utilisateurs et les appareils à prouver leur identité lorsqu'ils se connectent à des ressources. Et ce, peu importe qu'ils se connectent souvent ou se soient récemment identifiés.

Dans un environnement de télétravail, vérifier une identité n'est pas toujours simple. Les organisations ne peuvent pas s'appuyer sur leurs configurations Active Directory (AD) ou LDAP locales – en particulier sur les appareils Apple, pour lesquels AD n'a pas été conçu. C'est là qu'interviennent les fournisseurs d'identité (IdP) cloud, comme Okta, G Suite et Microsoft Entra ID.

Les IdP cloud assurent le service d'annuaire quelle que soit la localisation de vos utilisateurs. Votre IdP conserve toutes les informations nécessaires : identité, rôle et applications autorisées. En d'autres termes, il authentifie l'utilisateur et détermine ses autorisations d'accès aux ressources de l'entreprise.

Microtunnels basés sur l'application

Quand on parle de ZTNA, on évoque régulièrement l'identité de l'utilisateur, mais celle de l'application est tout aussi importante. Ce sont les règles de microtunnels basés sur l'application qui, en coulisse, mettent en œuvre le ZTNA. Chaque application reçoit une identité indépendante du réseau ; vous obtenez une segmentation plus fine, tout en faisant en sorte que les règles restent valides, quelle que soit la localisation de l'application – serveur local ou cloud. Les règles de sécurité verticales et horizontales sont plus faciles à appliquer et vous bénéficiez d'une visibilité sur le trafic des applications.

En combinant un IdP cloud avec ce type de microtunnels, vous profitez de tout l'intérêt de votre infrastructure cloud. Vous n'avez pas à gérer les identités et à héberger les applications sur vos serveurs : votre fournisseur ZTNA redirige le trafic en fonction des besoins. Vous évitez d'avoir à maintenir ou à superviser des serveurs et du matériel superflus, tout en offrant aux utilisateurs un accès sécurisé et pratique.

Règle d'accès unifiée

Toutes ces méthodes convergent vers une règle d'accès unifiée. Cette règle doit couvrir tous les hôtes exploités dans votre organisation – sur site, dans un cloud privé ou public, dans une application SaaS, sur un OS moderne ou autre paradigme de gestion. Une règle efficace comprend :

- Des services d'annuaire et des capacités d'authentification unique (SSO) via un IdP dans le cloud
- L'authentification multifacteur
- Le contrôle des accès basé sur le rôle, selon les principes du moindre privilège
- Un référentiel d'applications autorisées protégé par SSO
- Un système de contrôle pour acheminer le trafic vers les différentes parties du réseau (trafic sur site, cloud, SaaS et trafic web non professionnel).

Conformité et sécurité

En matière de ZTNA, l'identité n'est que la première moitié de la bataille – l'autre, c'est la conformité. Vous devez empêcher les appareils à risque d'accéder aux ressources de l'entreprise, même si vous avez mis en place d'autres mesures de protection.

Comment garantir la conformité des appareils qui se connectent à vos ressources ? Comment l'implique la locution « zero-trust », vous ne pouvez jamais avoir confiance dans la santé des appareils, des serveurs et des applications. Vos règles d'accès doivent inclure des méthodes pour identifier les appareils vulnérables et/ou compromis.

Votre logiciel de conformité doit rechercher :

- Les versions non patchées ou vulnérables de système d'exploitation et d'application
- Les logiciels de protection des terminaux actifs
- Les activités suspectes inhabituelles pour l'utilisateur
- Les menaces présentes sur l'appareil ou les accès à des sites malveillants

Au moindre doute concernant la conformité d'un appareil, vous pouvez lui interdire l'accès aux ressources de l'entreprise. La mise en œuvre de ces contrôles de conformité diffère selon le type d'appareil et selon qu'il s'agit d'un appareil professionnel ou personnel. Dans tous les cas, l'appareil doit être doté d'un logiciel de gestion lorsqu'il se connecte à des applications d'entreprise. Mais il faut également respecter la confidentialité de l'utilisateur. Quand ils appartiennent à l'employé (modèle BYOD), les appareils doivent acheminer le trafic personnel directement, sans passer par les logiciels de surveillance de l'entreprise. Les données personnelles et professionnelles doivent être totalement séparées pour des raisons de sécurité et de confidentialité.

Vérification continue

La vérification de la conformité des appareils ne se fait pas uniquement au moment de la connexion. Toujours selon le principe « ne jamais faire confiance, toujours vérifier », il faut garder en tête que l'appareil peut être compromis à tout moment. Il est primordial de vérifier en continu l'état d'un appareil : même l'utilisateur le mieux intentionné peut être victime d'une tentative de phishing ou d'un logiciel malveillant.

L'expérience de l'utilisateur final

Un service ZTNA peu pratique, difficile à utiliser et peu fiable a peu de chances d'avoir du succès. Si le système est une gêne pour les utilisateurs, ceux-ci risquent d'être tentés de contourner les mesures de sécurité mises en place.

Quelle que soit l'approche choisie pour mettre en œuvre le ZTNA, elle doit être à peine perceptible par les utilisateurs, qui doivent profiter d'un accès constant aux applications professionnelles. L'application installée sur l'appareil ne doit pas affecter l'autonomie de la batterie. Elle doit créer sur demande des tunnels vers les applications métier et rétablir la connexion en cas d'interruption. Non seulement cela facilite (et embellit sans doute) la vie de vos utilisateurs, mais cela décourage la pratique du shadow IT, ces applications utilisées clandestinement et qui peuvent introduire des vulnérabilités dans votre infrastructure.

Et en utilisant l'authentification unique (SSO) avec votre IdP cloud, vous pouvez rationaliser davantage le processus : un même mot de passe permet à l'utilisateur d'accéder à toutes ses applications après un processus d'authentification simplifié. Il est beaucoup plus simple de se souvenir d'un seul mot de passe et de s'authentifier à l'aide de la biométrie ou d'une autre forme d'AMF que d'en mémoriser un par application.

Un logiciel ZTNA qui :

- Utilise la puissance du SSO et des IdP cloud pour simplifier l'authentification
- Fonctionne quelle que soit la localisation des ressources sur les réseaux internes et externes
- Crée des microtunnels sécurisés vers chaque application sans fournir d'accès global aux réseaux de l'entreprise
- Donne rapidement et facilement accès aux applications une fois que la conformité de l'utilisateur et de l'appareil est vérifiée.
- Protège la confidentialité des utilisateurs tout en sécurisant les données de l'entreprise
- Et passe inaperçue aux yeux de l'utilisateur final : voilà le secret d'une mise en œuvre réussie qui garantit satisfaction et productivité aux utilisateurs comme aux équipes informatiques et de sécurité.

C'est là qu'intervient Trusted Access.

Si vous ne pouvez pas faire aveuglément confiance aux appareils de votre réseau, vous pouvez compter sur vos contrôles d'accès pour garantir la sécurité de vos utilisateurs et de votre entreprise. La solution ZTNA de Jamf est entièrement conçue pour permettre à votre organisation de mettre en œuvre le Trusted Access. Explorez le Trusted Access, qui réunit la gestion des appareils, des identités et des accès, et la sécurité des terminaux. Découvrez pourquoi la solution ZTNA de Jamf est aussi appréciée des administrateurs que des utilisateurs avec un essai gratuit.

Demander une version d'essai

Ou contactez votre revendeur préféré pour commencer.

jamf

www.jamf.com/fr