TANIUM

LIVRE BLANC

Qu'est-ce que le Zero Trust ?

Comment la sécurisation du endpoint est un élément essentiel du puzzle pour une stratégie Zero Trust réussie

SOMMAIRE

Qu'est-ce que le Zero Trust ?

Le Zero Trust est une idée simple : ne faire confiance à aucun utilisateur et aucun endpoint, et toujours vérifier En d'autres termes, ne faites confiance à rien. Ni aux personnes. Ni aux endpoints. Ni aux applications. Ni aux réseaux.

Les entreprises doivent reconnaître qu'elles opèrent dans un environnement hostile. La sécurité Zero Trust suppose qu'aucun appareil ou utilisateur ne peut être fiable sans vérification. Les organisations ne doivent pas automatiquement faire confiance à quoi que ce soit à l'intérieur ou à l'extérieur de leur périmètre. En fait, l'idée d'un périmètre, l'approche de la sécurité basée sur le principe d'un château et de douves, n'est plus d'actualité. L'endpoint est le nouveau périmètre.

Le Zero Trust a été créé pour cette nouvelle réalité. Et la clé pour que la sécurité Zero Trust fonctionne à grande échelle est la visibilité des endpoints.

Le Zero Trust est une solution, pas un produit

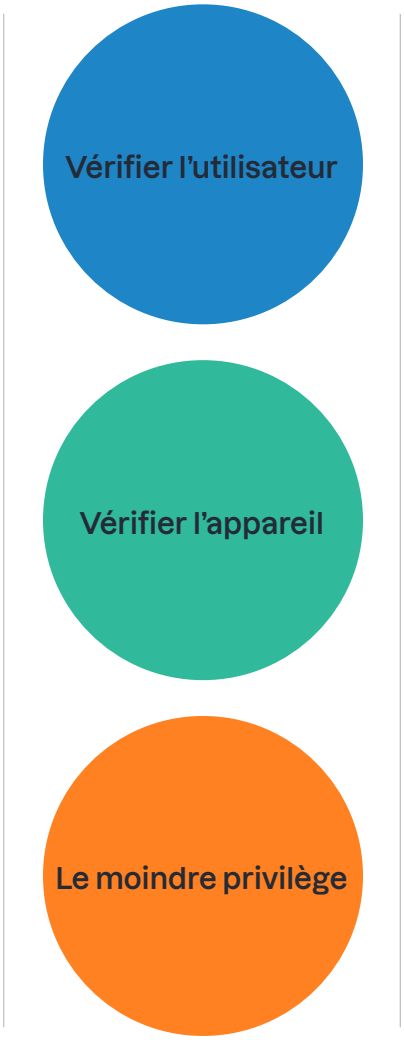
La plupart des discussions sur le Zero Trust se concentrent sur l'authentification des utilisateurs, une pièce importante du puzzle. Mais l'endpoint est tout aussi critique. Après tout, un utilisateur peut être légitime, mais qu'en est-il de l'appareil qu'il utilise ? A-t-il été compromis à son insu ? Une approche Zero Trust efficace examinera non seulement les informations d'identification de l'utilisateur et les données auxquelles la personne tente d'accéder, mais également l'appareil (c.-à-d. l'endpoint) que cette personne utilise. À une époque où la sécurité des endpoints est une préoccupation croissante dans le contexte où les employés à distance en masse travaillent sur des appareils personnels, les entreprises doivent avoir la certitude que ces endpoints n'ont pas été détournés en raison d'une mauvaise hygiène informatique. Pour ce faire, il est essentiel d'avoir une visibilité précise et en temps réel sur les données des endpoints, des appareils et des utilisateurs. La publication spéciale 800-207 du NIST souligne l'importance absolue d'une surveillance continue et d'une cyberhygiène générale pour une approche Zero Trust réussie.

Les entreprises doivent être en mesure de répondre aux questions suivantes :

- Combien d'actifs non gérés, sous-gérés et gérés possédez-vous ? Quels sont leurs systèmes d'exploitation ?
- Combien de ces systèmes ne sont pas conformes ? Avez-vous une méthode pour rétablir rapidement la conformité de ces systèmes ?
- Combien de vulnérabilités faibles, moyennes et élevées sont présentes dans votre environnement ? Combien de ces vulnérabilités sont exploitables ?
- Avez-vous mis en place des contrôles de sécurité pour vous protéger contre ces vulnérabilités exploitables ? Qu'en est-il des contrôles de sécurité courants ?
- Avez-vous en place des politiques et procédures ou des procédures opérationnelles standard pour gérer les workflows de sécurité et d'exploitation ?

L’endpoint est le nouveau périmètre

La sécurité Zero Trust exige des utilisateurs qu’ils prouvent qui ils disent être grâce à l’authentification à plusieurs facteurs (AMF). Une fois identifiés et vérifiés, les utilisateurs n’ont accès qu’aux ressources spécifiques dont ils ont besoin. Un modèle Zero Trust applique également une micro-segmentation pour diviser un réseau en zones de sécurité plus petites, limitant ainsi les mouvements latéraux. Tout cela est formidable, mais sans visibilité des endpoints, les appareils à la périphérie du réseau peuvent rester exposés de manière critique aux menaces via des vulnérabilités non corrigées et des paramètres de configuration non sécurisés. Parallèlement à l’authentification des utilisateurs, les entreprises doivent avoir les moyens de vérifier l’« identité » des endpoints en confirmant l’état de sécurité des machines distantes. Que se passe-t-il si un utilisateur accède au réseau de l’entreprise à partir d’un ordinateur personnel à domicile qui n’a pas été corrigé depuis quatre ans ? Que se passe-t-il si cet endpoint a été compromis ?



Tanium apporte la perspective de l’endpoint au Zero Trust

Avec Tanium Endpoint Identity, vous pouvez intégrer Tanium aux fournisseurs d’Identity and Access Management (IAM) pour vérifier que les appareils se connectant à vos applications cloud et aux réseaux Zero Trust sont gérés et sécurisés.

Bien que les employés accèdent généralement aux applications cloud depuis l’ordinateur fourni par l’entreprise, il peut arriver qu’un employé ait besoin d’utiliser un autre ordinateur pour se connecter aux applications cloud. Par exemple, un employé a laissé l’ordinateur fourni par l’entreprise à la maison lorsqu’il rend visite à un parent, mais une demande de travail urgente survient. Il utilise alors l’ordinateur non géré de son parent pour essayer de se connecter à l’application cloud. Lorsque l’employé essaye de se connecter, l’endpoint est vérifié par rapport aux endpoints gérés connus dans Tanium. Étant donné que l’employé tente de se connecter avec un ordinateur non géré, il n’est pas autorisé à accéder aux systèmes ou applications contenant des données sensibles ou exclusives de l’entreprise. L’approche de Tanium en matière de Zero Trust est contextuelle, ce qui signifie que tous les signaux sont combinés et évalués par rapport aux données en temps réel et aux informations sur les menaces, afin de créer une vue et une compréhension précises et complètes de ce qui se passe sur le réseau à tout moment.

En plus de la solution Endpoint Identity et en association avec celle-ci, Tanium fournit une diversité de capacités qui facilitent la planification et l’exécution Zero Trust.

Les étapes vers une stratégie Zero Trust

Identifier les attaques et protéger la surface

Identifier le chemin de communication

Concevoir et mettre en œuvre une architecture Zero Trust

Surveiller et maintenir

Solutions Tanium pour une stratégie Zero Trust

Recherche des menaces Tanium :

- Permet aux équipes de sécurité de détecter, d'enquêter sur et de corriger les incidents
- Garantit que les politiques de sécurité restent appliquées aux actifs connectés au domaine et non liés au domaine. La force principale de Tanium est sa capacité à fournir une visibilité et un contrôle des actifs connectés et mobiles à la vitesse et à l'échelle requises pour répondre aux évaluations en temps réel nécessaires pour une architecture Zero Trust efficace
- Fournit une visualisation des fiducies et des autorisations accordées aux utilisateurs et aux actifs dans un environnement Active Directory. Prendre le contrôle de ces relations est essentiel pour réduire les mouvements latéraux potentiels. Il fournit également un tremplin vers la planification Zero Trust en identifiant les utilisateurs, les comptes et les actifs nécessaires pour répondre à des exigences plus strictes en matière d'accès privilégié.

Solutions de détection et de recensement des actifs Tanium et Tanium Client Management :

- Fournit une visibilité sur les actifs gérés et non gérés connectés à l'entreprise. L'obtention d'une visibilité sur les actifs non gérés est un défi pour de nombreuses entreprises. Nous constatons régulièrement que 15 à 20 % des actifs d'une organisation sont inconnus, non surveillés et non gérés.
- Non seulement elle maintient un inventaire des endpoints en ligne et hors ligne, mais elle peut également être utilisée pour associer des données à des « systèmes informatiques fantômes », des éléments BYOD approuvés et d'autres endpoints qui peuvent se connecter aux ressources de l'entreprise tout en étant gérés différemment des actifs de base de l'entreprise.
- Fournit une visualisation du service applicatif depuis plusieurs points de vue afin que les dépendances du service de bout en bout puissent être identifiées et incluses dans la planification Zero Trust.

Gestion des risques et de la conformité de Tanium :

- Effectue des évaluations des vulnérabilités et de la conformité relativement aux systèmes d'exploitation, aux applications et aux configurations et politiques de sécurité. Il fournit les données nécessaires pour aider à éliminer les risques de sécurité, améliorer l'hygiène globale de l'infrastructure informatique et simplifier la préparation des audits.
- Évite les failles de sécurité en maintenant les endpoints à jour avec les correctifs les plus récents.

Le Zero Trust s'appuie sur ces domaines pour créer une architecture de sécurité robuste, car vous ne pouvez pas mettre en œuvre une architecture de sécurité efficace si vous ne comprenez pas parfaitement votre environnement. Si vous ne disposez pas d'un programme de gestion de la conformité efficace, il est difficile de déterminer quels systèmes sont autorisés à communiquer sur certains ports et protocoles. Chaque composant prend en charge les fonctions de l'autre composant et une mise en œuvre Zero Trust.

Conclusion

Nous vivons à une époque compliquée. Alors qu'il existait autrefois un modèle clair pour la sécurité réseau (lorsque vous saviez qui vous laissiez entrer), aujourd'hui, les choses sont plus complexes. Pour rester en sécurité, les organisations distribuées d'aujourd'hui doivent surveiller et contrôler facilement toutes les activités sur le réseau des utilisateurs et des endpoints. Les entreprises ont besoin d'un modèle de sécurité transparent conçu pour la nouvelle réalité du travail à distance, des services cloud et des communications mobiles. Le Zero Trust a été créé pour cette nouvelle réalité. Et la clé pour que la sécurité Zero Trust fonctionne à grande échelle est la visibilité des endpoints.

Tanium est le partenaire idéal pour votre parcours Zero Trust. Il fournit :

- La visibilité en temps réel de vos actifs, sur le réseau et hors réseau
- La visibilité des dépendances entre les actifs, les applications et les services
- La visibilité des fiducies et des permissions accordées aux utilisateurs et aux actifs dans un environnement Active Directory
- L'assurance que les politiques de sécurité d'entreprise restent appliquées aux endpoints, qu'ils soient connectés au domaine ou mobiles
- L'amélioration de la cyberhygiène générale et de la visibilité des appareils connectés au réseau

Par-dessus tout, Tanium reste la plateforme la plus flexible de votre inventaire, prenant en charge plusieurs systèmes d'exploitation (Windows, Linux, Mac, etc.), du contenu développé par l'opérateur et des modèles de mise à disposition sur site, dans le cloud ou en tant que service.

Découvrez comment Tanium peut vous aider à obtenir une visibilité, un contrôle et une source unique de vérité sur vos données d'asset à grande échelle, qui sont tous essentiels pour adopter une stratégie Zero Trust dans votre entreprise.

Contactez-nous sur le site **www.tanium.com.**

Tanium est la plateforme à laquelle les entreprises font confiance pour gagner en visibilité et en contrôle sur l'ensemble des endpoints dans des environnements hybrides, sur site, sur le Cloud. Notre approche répond aux défis informatiques croissants d'aujourd'hui en fournissant des données précises, complètes et à jour sur les endpoints, ce qui donne aux équipes chargées des opérations informatiques, de la sécurité et des risques la confiance nécessaire pour gérer, sécuriser et protéger rapidement leurs réseaux à grande échelle. La mission de Tanium est d'aider à voir et à contrôler chaque endpoint partout.

Rendez-nous visite sur www.tanium.com et suivez-nous sur LinkedIn et Twitter.