FORESCOUT
Active Defense for the Enterprise of Things™

Approche NAC moderne

Sécurité Zero Trust sans agent, flexible et transparente pour votre environnement EoT

Les entreprises actuelles ont besoin d'un moyen d'implémenter et de maintenir l'accès Zero Trust pour leurs nombreux types de réseaux et la multitude d'objets connectés : ordinateurs du campus, appareils des visiteurs, ordinateurs portables de télétravail, appareils intelligents ou encore appareils IoT et OT. Elles ont besoin d'une plateforme de contrôle d'accès au réseau (NAC) leur permettant de réaliser de nombreux objectifs :

- Identifier en continu tous les objets connectés
- Évaluer leur niveau de sécurité
- Appliquer les politiques d'accès
- Implémenter automatiquement des contrôles visant à détecter la non-conformité ou les comportements inhabituels

Le modèle Zero Trust, un chemin semé d'embûches

Le contrôle de tous les objets qui se connectent au réseau d'entreprise relève de la gageure. Les architectes informatiques et en sécurité qui implémentent les systèmes de contrôle d'accès sont confrontés à de nombreux défis, notamment :

- Les solutions de contrôle d'accès au réseau antérieures n'étaient pas satisfaisantes en raison de leur complexité ou des risques d'impact négatif sur les opérations métier.
- Les appareils IoT et OT qui prolifèrent sur les réseaux d'entreprise ne peuvent pas être authentifiés ou contrôlés à l'aide des agents traditionnels.
- Les contrôles basés sur la norme 802.1X sont impossibles sur les réseaux multifournisseurs.
- Les analyses réseau planifiées ne tiennent pas compte des tentatives d'usurpation d'identité et des autres menaces susceptibles de surgir à tout moment.

> **On nous a expliqué que la plateforme Forescout se déployait en une après-midi. J'ai regardé un membre de mon équipe : nous n'y croyions pas. Mais nous avons effectivement réalisé le déploiement en quelques heures à peine !**
>
> **MIKE ROLING**
> **RSSI, ÉTAT DU MISSOURI**

- De nombreuses alternatives d'accès Zero Trust sont trop coûteuses et/ou nécessitent trop d'efforts manuels.

Forescout : une solution de contrôle d'accès au réseau de pointe

Si ces défis ne vous sont pas étrangers, le moment est venu d'évaluer l'approche de contrôle d'accès au réseau de Forescout. Nous pouvons répondre à vos besoins et dépasser vos attentes en vous offrant les avantages suivants :

Visibilité totale

Bénéficiez d'une visibilité totale en temps réel sur tous les appareils connectés à vos réseaux étendus grâce à plus de 20 techniques de surveillance active et passive.

Modèle Zero Trust pour tous les appareils connectés

Limitez l'impact des compromissions grâce à une surveillance continue sans agent et à un moteur de politiques unifié qui segmente et isole dynamiquement tous les objets qui se connectent à votre entreprise.

Déploiement sans interruption des activités assurant un ajout de valeur rapide à votre réseau

Bénéficiez d'une visibilité totale en quelques jours et d'un contrôle automatisé en quelques semaines grâce à un logiciel sans agent ne nécessitant aucune mise à niveau de l'infrastructure ni configuration de l'authentification 802.1X.

Protection éprouvée pour les réseaux d'entreprise étendus

Plusieurs milliers de clients du Fortune 1000 satisfaits, dont certains possèdent jusqu'à 2 millions de terminaux, peuvent témoigner des fonctionnalités et de la confiance que leur procure Forescout quant à la sécurité de leurs réseaux.

MAXIMISEZ LA VALEUR DE VOS INVESTISSEMENTS DE SÉCURITÉ ET INFORMATIQUES

La plupart des outils de sécurité se contentent de signaler les violations et d'alerter votre équipe. La plateforme Forescout inclut des modules prêts à l'emploi qui étendent les fonctionnalités de visibilité et de contrôle :

- Partagez en temps réel les données contextuelles sur les appareils avec vos outils de sécurité et de gestion informatique.
- Orchestrez les flux de travail et automatisez les actions d'intervention.
- Évaluez en continu le niveau de sécurité des appareils et obligez ceux qui ont été corrigés automatiquement à être conformes à vos politiques.

« Les outils NAC d'aujourd'hui sont conçus pour repérer les appareils et les entités non approuvés (utilisateurs, segments, périphériques, etc.), et les empêcher d'entrer en contact avec le réseau. Grâce à ces toutes nouvelles technologies, proposées par des fournisseurs tels que Forescout, vous pouvez interdire aux éléments inconnus et probablement non corrigés d'accéder à vos réseaux de type Zero Trust[1]. »

CHASE CUNNINGHAM

ANALYSTE EN CHEF, FORRESTER RESEARCH

IDENTIFICATION

Découvrir, classifier et répertorier tous les appareils connectés

Avec la plateforme Forescout, les équipes en charge de la sécurité et des opérations informatiques gagnent une visibilité complète en temps réel sur tous les appareils IP dès l'instant où ceux-ci accèdent au réseau. Elles disposent ainsi d'un inventaire des actifs précis et en temps réel.

- Choisissez parmi plus de 20 méthodes actives et passives de découverte et de profilage celle qui correspond à votre environnement professionnel et garantira la disponibilité en continu de votre réseau.
- Avec plus de 12 millions d'empreintes matérielles, Forescout Device Cloud offre des fonctionnalités enrichies de classification des appareils en trois dimensions et permet de déterminer différentes informations les concernant : fonction, système d'exploitation, fournisseur, modèle, etc.
- Bénéficiez d'une couverture complète sur tous les emplacements, réseaux et types d'appareils, sans zones d'ombre, avec ou sans authentification 802.1X.

CONFORMITÉ

Évaluer le niveau de sécurité et la conformité

Les outils de sécurité avec agents ne sont pas en mesure de détecter les appareils gérés dont les agents sont manquants, défectueux ou dysfonctionnels. En outre, comme les appareils IoT ne prennent pas en charge les agents de sécurité, ces outils ne peuvent pas les évaluer, ce qui étend davantage encore la surface d'attaque. Avec la plateforme Forescout, vous pouvez automatiser l'évaluation du niveau de sécurité et la correction de tous les appareils IP dès qu'ils se connectent, mais aussi de manière continue après leur connexion.

- Détectez et corrigez à l'aide de vos outils de sécurité existants les appareils gérés dont les agents sont défectueux ou manquants.
- Détectez les appareils non conformes, les changements de niveau de sécurité, les vulnérabilités, les identifiants faibles, les indicateurs de compromission, les tentatives d'usurpation et les autres indicateurs à haut risque, le tout sans utiliser d'agents.
- Évaluez et surveillez en continu les appareils non gérés, y compris ceux qui n'acceptent pas les agents, afin d'assurer la conformité aux politiques de sécurité.

> **La quantité d'informations que nous recevons de la plateforme Forescout est incroyable. C'est de loin la meilleure pour détecter, identifier et contrôler les systèmes correctement. Elle s'est avérée un outil inestimable pour nous.**
>
> **JOSEPH CARDAMONE**
> **ANALYSTE EN SÉCURITÉ INFORMATIQUE, HAWORTH INTERNATIONAL**

CONNECTER

Mettre en œuvre des politiques d'accès sur des réseaux hétérogènes

La plateforme Forescout applique une sécurité Zero Trust basée sur l'identité des appareils et des utilisateurs, l'intégrité des appareils et leur conformité en temps réel, sans mise à niveau matérielle ou logicielle de l'infrastructure.

- Fournissez l'accès aux ressources d'entreprise selon le principe du moindre privilège, en fonction du rôle des utilisateurs, du type des appareils et de leur niveau de sécurité.
- Empêchez les appareils non autorisés, non approuvés et faussement légitimes de se connecter.
- Mettez en œuvre des contrôles flexibles sur les infrastructures filaires, sans fil et VPN, avec ou sans authentification 802.1X.

1. The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook (L'écosystème Zero Trust eXtended : Plan stratégique des réseaux – Feuille de route de l'architecture de sécurité et des opérations), Forrester Research, 2 janvier 2019
2. Forrester Wave™: Zero Trust eXtended Platform Providers (Fournisseurs de plateformes Zero Trust eXtended), 4e trimestre 2019

> **a plateforme et les fonctionnalités [Forescout] destinées à la sécurité IoT/OT dépassent largement celles de la concurrence.**
> **La visibilité complète, qui offre un contrôle opérationnel maximal et, au final, une sécurité optimale, est le fondement même de l'approche Zero Trust de Forescout[2].**
>
> **FORRESTER RESEARCH**

Détecter, c'est bien. Sécuriser, c'est mieux.

Contactez-nous dès aujourd'hui pour protéger efficacement votre Internet des objets en entreprise.

forescout.com/platform/eyeControl

info-france@forescout.com

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 (États-Unis)

Email info-france@forescout.com
Tél (Intl) +1-408-213-3191
Support 1-708-237-6591

Pour en savoir plus, consultez le site Forescout.fr