FORESCOUT
Active Defense for the Enterprise of Things.

Sécurité de l'Internet des objets

Adoptez une approche Zero Trust de la protection des appareils non traditionnels de l'IoT en entreprise

Les appareils de l'Internet des objets (IoT) sont généralement invisibles sur les réseaux d'entreprise et, contrairement aux systèmes traditionnels, ils sont souvent difficiles à surveiller et prennent rarement en charge les agents logiciels. Ces appareils ont pour effet d'étendre la surface d'attaque et augmentent de manière importante les risques pour les entreprises, dans la mesure où ils peuvent être compromis et utilisés comme points d'entrée sur les réseaux vulnérables. Les entreprises ont besoin d'une solution de sécurité capable d'identifier, de segmenter et d'assurer la conformité de chacun des appareils IoT, et ce de manière continue et sur des réseaux hétérogènes.

Appareils IoT : le jeu en vaut-il la chandelle?

Les appareils IoT constituent souvent des ressources précieuses, voire critiques, pour les entreprises, en ce sens qu'ils permettent d'améliorer la productivité, de renforcer la qualité des produits et services, et de générer de meilleurs résultats. Ainsi, 63 % des entreprises estiment pouvoir amortir leurs projets IoT en seulement trois ans[2]. De nombreux pirates particulièrement astucieux et disposant de fonds conséquents sont toujours à l'affût de failles à exploiter dans la sécurité des entreprises, comme des lacunes dans la visibilité et la protection des ressources IoT, lesquelles sont susceptibles d'entraîner des interruptions d'activité, la compromission de données, la perte de propriété intellectuelle ou encore des atteintes à l'image de marque. Figurez-vous par exemple que :

- une récente étude du Ponemon Institute révèle que près de 9 répondants sur 10 s'attendent à ce que leur entreprise soit victime d'une cyberattaque ou d'une violation de données provoquée par l'utilisation d'applications ou d'appareils IoT non sécurisés au cours des deux prochaines années[3] ;
- d'ici 2023, les DSI devront gérer plus de trois fois plus de terminaux qu'en 2018[4].

UNE NOUVELLE APPROCHE ZERO TRUST

Le modèle Zero Trust de Forrester appliqué à la sécurité des informations constitue une approche à la fois conceptuelle et architecturale de la sécurité d'entreprise. Ce modèle consiste essentiellement à établir un certain niveau de confiance par la création d'un environnement où utilisateurs, appareils et accès sont tous approuvés. L'accès est alors limité aux ressources d'entreprise dont chaque utilisateur a besoin pour mener à bien ses missions. Selon Forrester[1], pour implémenter des politiques Zero Trust efficaces, vous devez :

- segmenter les réseaux en micro-périmètres sécurisés ;
- renforcer la sécurité des données à l'aide de techniques de dissimulation ;
- réduire les risques associés aux privilèges utilisateur et aux accès excessifs ;
- améliorer considérablement la détection des menaces et l'intervention sur incident grâce à l'analyse et à l'automatisation.

À l'heure de l'Internet des objets en entreprise (EoT), où un nombre incalculable de technologies d'exploitation (OT), de dispositifs informatiques et d'appareils IoT se connectent et interagissent, les entreprises ont besoin d'une solution de sécurité qui leur offre une visibilité et un contrôle complets sur tous les appareils IoT et IP, et qui s'appuie sur une approche Zero Trust de la gestion des réseaux. Sans une telle solution, elles courent le risque que n'importe quel appareil soit un jour compromis et exploité à des fins malveillantes.

L'approche Zero Trust de Forescout

Forescout considère que la sécurité IoT doit s'appuyer sur une approche Zero Trust alliant une visibilité complète sur les appareils, une segmentation réseau proactive et un contrôle d'accès des ressources numériques selon le principe du moindre privilège appliqué à l'ensemble des appareils, utilisateurs, applications et charges de travail. La plateforme Forescout vous permet de gérer efficacement les risques opérationnels, de conformité et de cybersécurité sur l'ensemble de votre environnement EoT, et ce :

- en assurant une visibilité complète sur les appareils IoT, IoMT (Internet des objets médicaux) et OT non gérés, ainsi que sur tous les systèmes à connexion IP ;
- en évaluant et en identifiant les appareils IoT avec identifiants d'usine par défaut ou faibles, et en automatisant les actions déclenchées par des politiques afin de mettre en œuvre des mots de passe complexes ;
- en fournissant des informations en temps réel sur les communications des appareils IoT et sur les comportements dangereux dans l'environnement étendu ;
- en segmentant les appareils en zones de confiance par la mise en place d'un accès selon le principe du moindre privilège par l'application d'une politique Zero Trust ;
- en automatisant l'orchestration d'une politique Zero Trust unifiée sur plusieurs environnements fournisseurs et sur différents domaines réseau ;
- en décloisonnant la gestion de la sécurité afin d'améliorer la réactivité et d'optimiser la valeur de vos investissements dans d'autres solutions de sécurité ; et
- en aidant les prestataires de soins de santé à détecter et limiter de manière proactive l'exposition aux vulnérabilités ou aux menaces, à appliquer des règles de segmentation et d'accès au réseau de manière granulaire, et à neutraliser immédiatement les menaces ciblant les appareils médicaux tout en simplifiant la mise en œuvre de mesures correctives, le tout via une intégration étroite à la plateforme Medigate.

"Forescout est le fournisseur par excellence de solutions de sécurité des appareils IoT/OT axées sur une approche Zero Trust. La sécurité des appareils IoT/OT est l'un des problèmes les plus difficiles à gérer pour une entreprise. Or il s'agit du domaine de prédilection de Forescout, et les fonctionnalités de sa plateforme dédiées à la sécurité IoT/OT dépassent largement celles de la concurrence."

THE FORRESTER WAVE: ZERO TRUST EXTENDED ECOSYSTEM PLATFORM PROVIDERS (THE FORRESTER WAVE : FOURNISSEURS DE PLATEFORMES ZERO TRUST EXTENDED), FORRESTER RESEARCH, OCTOBRE 2019

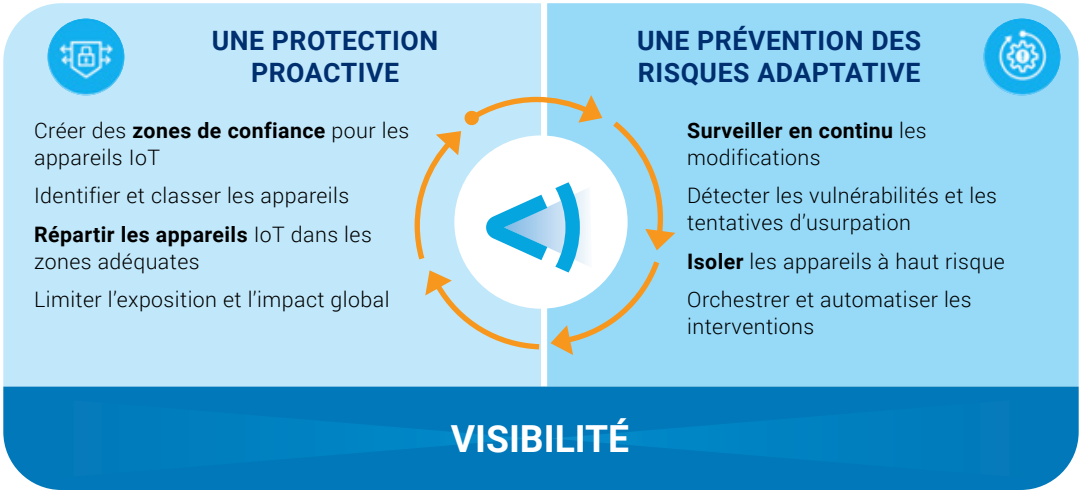

Figure 1. Forescout défend activement tous les appareils de votre environnement EoT en identifiant, en segmentant et en assurant la conformité de chaque objet connecté.

Découvrez et classifiez 100 % des appareils IP

Il est primordial de pouvoir bénéficier de données contextuelles et d'une visibilité complète sur l'ensemble des terminaux IoT, OT et d'infrastructures critiques, et ce pour l'ensemble de votre environnement hétérogène. La plateforme Forescout :

- assure la découverte en continu de tous les appareils IP, physiques comme virtuels, au moment même où ils se connectent à votre réseau, sans nécessiter d'agent logiciel ;
- garantit une visibilité en profondeur sur tous les appareils grâce à la combinaison d'une vingtaine de techniques de découverte active et passive, de profilage et de classification ;
- tire parti de Forescout Device Cloud, le plus grand référentiel au monde de données collaboratives sur les appareils, lequel offre une source unique et multisectorielle d'informations approuvées sur les profils d'empreintes digitales, de comportements et de risques de plus de 12 millions d'appareils.

Implémentez une segmentation dynamique du réseau et automatisez les contrôles

Dans les environnements EoT hétérogènes actuels, toute entreprise qui adopte le modèle Zero Trust doit être en mesure de segmenter le réseau et d'orchestrer une intervention sur incident sur l'ensemble des domaines EoT. Grâce à Forescout, vous pouvez :

- mettre en corrélation les accès avec les identités utilisateur (et déterminer ainsi qui fait quoi, où et pourquoi) ;
- provisionner des appareils pour les différents segments de réseau dynamique en fonction des politiques en place et du contexte en temps réel ;
- cartographier les flux de données afin de concevoir des politiques de segmentation et simuler leur application pour un déploiement qui ne nuit pas à la continuité des activités ;
- automatiser la segmentation dans le but de réduire les risques opérationnels et de cybersécurité.

Orchestrez votre sécurité et assurez votre conformité

La plupart des entreprises disposent de plus de solutions de sécurité qu'il ne leur en faut, des solutions généralement onéreuses et spécialisées incapables de partager des informations ou de se coordonner pour les interventions sur incident. Forescout constitue une solution idéale face à ce manque d'efficacité. Les produits Forescout eyeExtend assurent le partage des données contextuelles sur les appareils entre la plateforme Forescout et d'autres produits informatiques et de sécurité afin d'automatiser les flux de travail et l'application des politiques sur des solutions hétérogènes. Ces fonctions d'orchestration peuvent ainsi vous aider à :

- améliorer la sécurité IoT et la conformité globale de vos appareils ;
- réduire le délai moyen de détection et d'intervention ;
- augmenter le retour sur investissement de vos outils existants ;
- automatiser la mise à jour de votre base de données de gestion de la configuration (CMDB), éliminant ainsi les opérations manuelles d'inventaire généralement fastidieuses et sources d'erreurs.

"Aujourd'hui, nous avons l'œil sur tous les éléments de notre réseau, y compris les appareils IoT comme les imprimantes, les téléphones VoIP et les caméras de sécurité. Forescout classe chaque appareil et le place dans le segment VLAN approprié."

– KEN COMPRES, INGÉNIEUR RESPONSABLE DE LA SÉCURITÉ DES RÉSEAUX / DIRECTEUR DE LA SÉCURITÉ, HILLSBOROUGH COMMUNITY COLLEGE

1 Five Steps to a Zero Trust Network (Cinq étapes pour un réseau zero trust), Roadmap Report, Forrester Research, octobre 2018

2 A New Roadmap for Third Party IoT Risk Management, Benchmark Study (Étude de référence - Une nouvelle feuille de route pour la gestion des risques IoT tiers), Ponemon Institute, Sabine Zimmer, 3 juin 2020

3 Internet of Things: Unlocking True Business Potential (Internet des objets : libérer le vrai potentiel des entreprises), Gartner

4 Gartner Top Strategic IoT Trends and Technologies Through 2023 (Principales tendances Gartner en matière de technologies IoT stratégiques jusqu'en 2023), septembre 2018

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/IoT info-france@forescout.com Tel (Intl) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Pour en savoir plus, consultez le site Forescout.fr