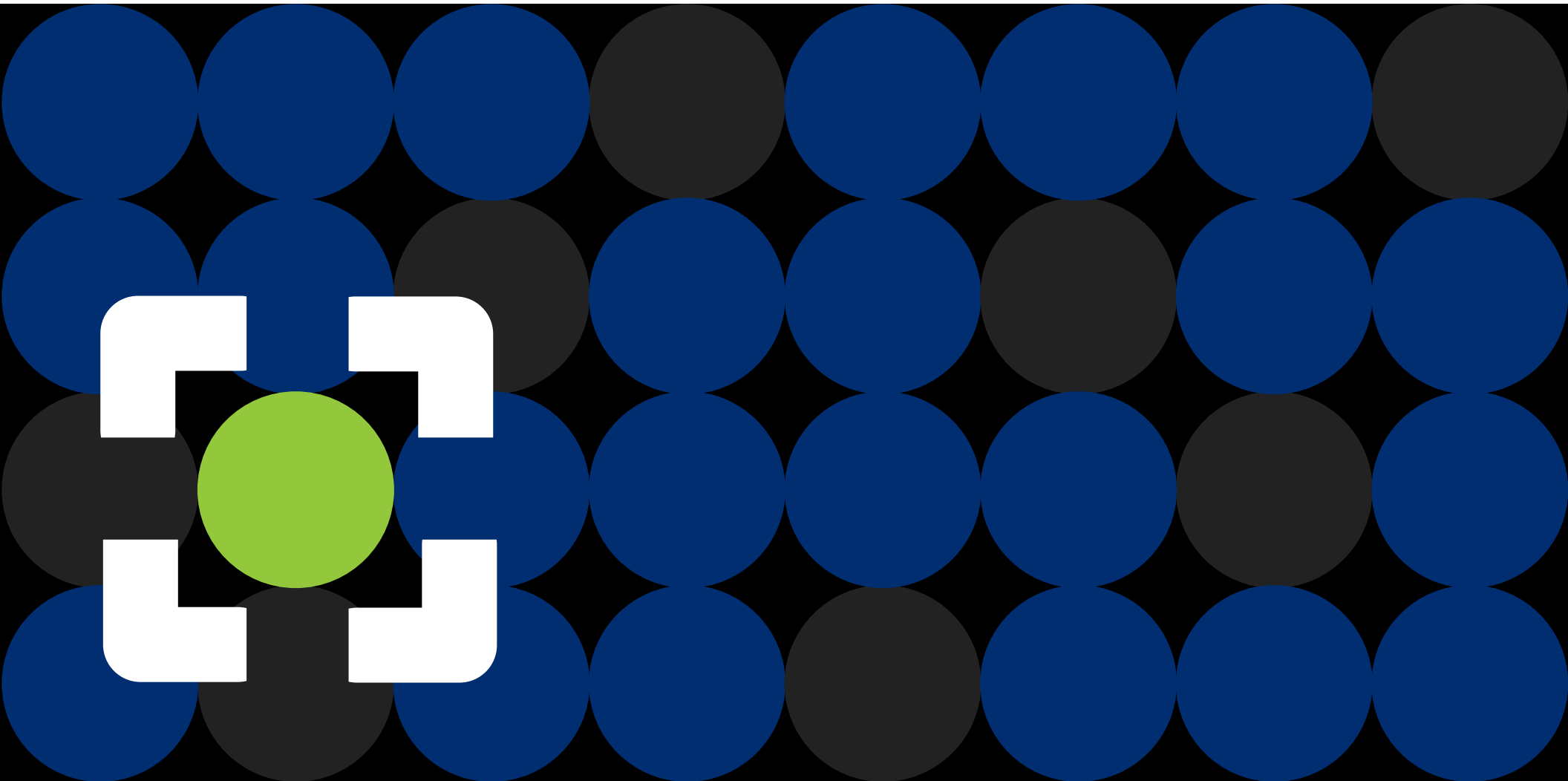
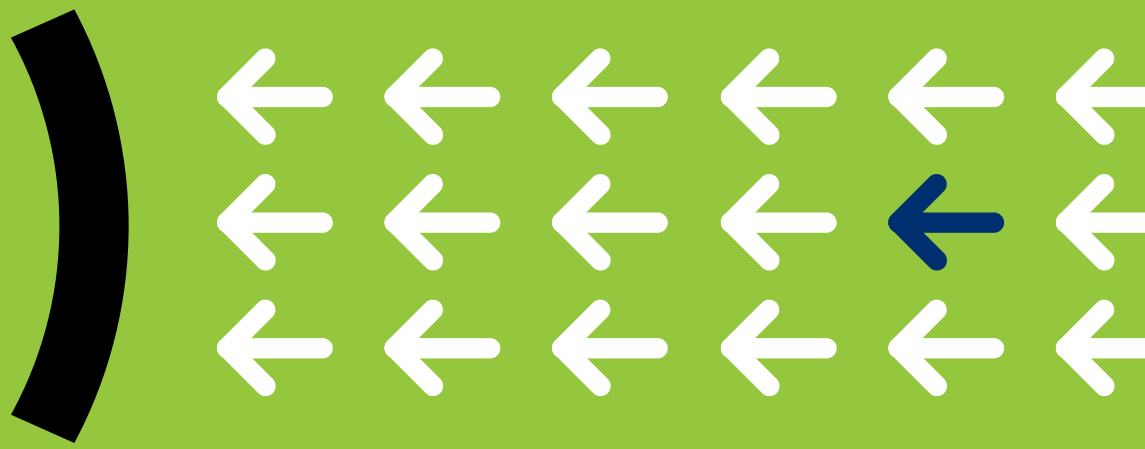
FORESCOUT
Active Defense for the Enterprise of Things™

Comment sécuriser l'Enterprise of Things
Cinq défis de sécurité



SOMMAIRE



INTRODUCTION

Les appareils qui se connectent aux réseaux d'entreprise sont devenus hors de contrôle. Leur nombre a explosé (on en compte désormais des milliards), tout comme leur diversité : ils peuvent être de type IT, OT, IoT ou BYOD. Certains d'entre eux sont connus et gérés, tandis que d'autres, furtifs, échappent à toute détection. Quant aux utilisateurs de ces appareils, ils proviennent de tous les horizons : employés, sous-traitants, partenaires, clients… N'importe qui peut se connecter de n'importe où à votre centre de données ou à votre cloud, de façon sécurisée ou non.

Pour toutes ces raisons, les environnements réseau sont *complexes*. Chacun d'eux constitue un véritable **Internet des objets en entreprise** (EoT, Enterprise of Things) qui nécessite une planification rigoureuse et des actions décisives afin de sécuriser les appareils et l'entreprise elle-même.

Cet ebook détaille les cinq défis liés à l'EoT que les RSSI et autres responsables de la sécurité et des opérations ne devraient en aucun cas ignorer. Il offre en outre des recommandations concrètes qui les aideront à résoudre définitivement ces problèmes.

DÉFI N° 1

Comment établir et gérer l'inventaire des appareils non gérés quand leur nombre explose ?

> **D'après les estimations des experts, 31 milliards d'appareils IoT seront installés partout dans le monde rien qu'en 2020.**
>
> ***SECURITY TODAY*, 13 JANVIER 2020[1]**

> **« 62 % des personnes interrogées affirment que la capacité de leur entreprise à mettre en place une stratégie de sécurité plus mature dépendra de plus en plus de la convergence entre l'infrastructure IT et les systèmes de contrôle OT. »**
>
> **PONEMON INSTITUTE, FÉVRIER 2019[2]**

Les appareils gérés intégrant des agents de sécurité (PC, ordinateurs portables et smartphones d'entreprise) ne pèsent pas lourd face aux milliards d'appareils IoT et OT sans agent qui se connectent aux réseaux. En parallèle, on assiste à la convergence des réseaux IT et OT, ce qui augmente la productivité et simplifie la gestion, mais accroît le risque. Dans un tel contexte, cerner la surface d'attaque des réseaux hétérogènes est devenu un véritable casse-tête.

Recommandations :

- Déterminez quels outils peuvent vous donner une visibilité complète sur vos appareils, sans zone d'ombre.
- Affinez votre processus de sélection de façon à ne retenir que les solutions capables d'offrir une évaluation sans agent et en temps réel du niveau de sécurité des appareils.
- Fournissez des capacités d'inventaire en temps réel à votre équipe informatique et à celle en charge des opérations de sécurité.

DÉFI N° 2

Dans les environnements d'entreprise actuels, où le risque se niche-t-il ?

> **« Les bâtiments intelligents, les appareils médicaux, les équipements de mise en réseau et les téléphones VoIP représentent les groupes d'appareils IoT les plus à risque. »**
>
> **FORESCOUT RESEARCH, MAI 2020[3]**

> **« Les technologies d'appareils IoT et réseau sont source de risques de compromissions des réseaux et des entreprises (...) Les équipes de sécurité doivent isoler, sécuriser et contrôler en permanence chaque appareil sur le réseau. »**
>
> **FORRESTER RESEARCH, JUIN 2020[4]**

Le concept d'analyse des risques évolue et s'élargit en même temps que votre surface d'attaque. Une récente analyse menée par Forescout sur l'Enterprise of Things montre que les appareils IoT représentent le risque le plus élevé. « Non seulement ils sont difficiles à surveiller et à contrôler, mais ils créent aussi des vulnérabilités en établissant des ponts entre l'environnement virtuel et le monde physique, qui n'existaient pas auparavant. Avec ce potentiel à servir de passerelles clandestines entre les réseaux, les appareils IoT constituent une cible de choix pour les logiciels malveillants spécialisés[3]. »

Recommandations :

- Utilisez l'analyse multifactorielle des risques pour cerner votre surface d'attaque.
- Passez à une stratégie de défense active basée sur une approche Zero Trust.
- Accélérez la réponse aux menaces en hiérarchisant les alertes en fonction de leur niveau de risque.
- Bénéficiez d'un avantage primordial : une visibilité complète sur les appareils.

DÉFI N° 3

La notion de périmètre réseau n'existe plus. Par quoi faut-il la remplacer ?

> **« Les acteurs du secteur doivent mettre en place des bonnes pratiques inédites afin de sécuriser la périphérie des réseaux d'entreprise. »**
>
> **GARTNER, MAI 2020[5]**

Des réseaux ouverts, mais sûrs : est-ce possible ? La question se pose surtout lorsqu'on sait qu'un réseau peut rassembler les appareils utilisés sur des environnements hétérogènes (campus, centre de données, cloud et OT). Maintenant que les réseaux d'entreprise atteignent n'importe quelle région du monde, à partir du moment où des charges de travail et des employés s'y trouvent, la notion de périmètre de défense autour d'une organisation a bel et bien disparu. Ou alors, il faudrait qu'un périmètre entoure chaque appareil connecté et chaque charge de travail. En conclusion, la sécurité commence à la périphérie des ressources.

Recommandations :

- Limitez l'accès aux ressources d'entreprise à l'aide d'un modèle basé sur le principe du moindre privilège, tel que la sécurité Zero Trust.
- Procédez en continu à la découverte et à l'évaluation du niveau de sécurité de tous les appareils accédant au réseau, où qu'ils se trouvent.
- Appliquez une stratégie de conformité stricte basée sur des politiques à tous vos sites, appareils BYOD et ressources distantes.

DÉFI N° 4

La segmentation est indispensable, mais comment la mener à bien sans perturber les activités de l'entreprise ?

> **« D'après nos estimations, 90 % des entreprises interrogées vont lanc er un projet de segmentation dans l'année. Ce genre d'initiative se généralise, mais il peut être compliqué de savoir par où commencer, quels sont les risques encourus, ou si l'investissement financier et les efforts requis en valent la peine. »**
>
> **FORESCOUT RESEARCH, JANVIER 2019[6]**

Pendant des années, la segmentation réseau a eu mauvaise presse. Jusqu'à récemment, les outils de segmentation disponibles étaient non seulement lourds à déployer, mais ils étaient aussi incapables de passer d'un domaine réseau à un autre, ce qui générait des perturbations des activités et une fragmentation de l'environnement. Les problèmes ont empiré lorsque les entreprises ont commencé à ajouter de nouveaux appareils et à étendre leurs réseaux. Aujourd'hui cependant, des solutions de segmentation solides existent, rendant obsolètes les réseaux sans hiérarchie, trop vulnérables.

Recommandations :

- Visualisez la segmentation et simulez des politiques avant le déploiement pour éviter les perturbations inutiles.
- Vérifiez que votre solution principale est capable de simplifier la segmentation Zero Trust de n'importe quel appareil, où qu'il se trouve (y compris les appareils IT, IoT et OT).
- Accélérez l'implémentation du modèle Zero Trust à l'échelle de l'environnement d'entreprise.
- Sélectionnez une plateforme de contrôle d'accès au réseau (NAC) moderne et conçue pour faciliter la segmentation du réseau.

DÉFI N° 5

Comment aborder le paradoxe du « en faire plus avec moins » ?

> **« Les entreprises parviennent de plus en plus à limiter la fragmentation des outils de gestion des réseaux. Cependant, 64 % d'entre elles utilis ent toujours entre quatre et dix outils pour surveiller et dépanner leurs réseaux. »**
>
> **NETWORK MANAGEMENT MEGATRENDS 2020, AVRIL 2020[7]**

> **« Les conseils d'administration ne se sont jamais autant intéressés à la gestion de la sécurité et des risques. »**
>
> **GARTNER RESEARCH, JUILLET 2019[8]**

Difficile de prouver que votre équipe chargée des opérations de sécurité (SecOps) est un rempart efficace et générateur d'économies quand le système de gestion de la sécurité et du réseau de votre entreprise est composé d'un méli-mélo d'outils hérités et fragmentés, spécifiquement adaptés à votre activité. Cela dit, même les plans de transformation les mieux conçus peuvent provoquer des problèmes : déploiement fastidieux, retour sur investissement trop lent, courbes d'apprentissage abruptes et choix de solutions peu satisfaisantes. Heureusement, en sélectionnant la plateforme adéquate, vous pouvez satisfaire tous les acteurs concernés, y compris les directeurs financiers.

Recommandations :

Choisissez une plateforme capable d'orchestrer les outils existants et répondant aux critères ci-dessous :

- Déploiement rapide et flexible, qui assure la continuité des activités
- Rentabilité et retour sur investissement accélérés
- Compatibilité avec tous les fournisseurs : utilisez votre infrastructure existante
- Fin des mises à niveau logicielles et matérielles forcées
- Intégration à des produits informatiques et de sécurité de premier ordre
- Découverte et évaluation sans agent du niveau de sécurité et de risque des appareils
- Élimination de la complexité ainsi que des coûts et retards de déploiement liés à l'authentification 802.1X
- Adaptation de la croissance à l'évolutivité de l'entreprise
- Hausse de la productivité des opérations de sécurité
- Visibilité, contrôle, segmentation et Zero Trust sans agent

Derrière ces cinq défis s'en cache un autre, redoutable

Les cinq défis que nous venons de décrire peuvent sembler insurmontables. Néanmoins, chacun d'entre eux doit être résolu, sans quoi c'est l'écueil ultime qui vous guette : une cyberattaque, sans compter les problèmes opérationnels, le vol de données, l'atteinte à la réputation de la marque, les amendes sévères, les préoccupations de sécurité publique et autres répercussions potentielles.

La prévention est la clé. Mais comment la concrétiser ? À l'aide d'une solution capable de fournir des capacités 100 % sans agent sur les appareils : visibilité, surveillance en continu et réponse aux menaces automatisée.

*Notes

1. *The IoT Rundown for 2020: Stats, Risks, and Solutions* (L'évolution de l'IoT en 2020 : statistiques, risques et solutions), Security Today, 13 janvier 2020
2. *Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT* (Sécurité et confidentialité dans le monde interconnecté de l'IT, de l'OT et de l'IIoT), rapport de recherche du Ponemon Institute, février 2019
3. *The Enterprise of Things Security Report, The State of IoT Security in 2020* (Rapport de sécurité sur l'Enterprise of Things, l'état de la sécurité de l'IoT en 2020), Forescout Research Labs, mai 2020
4. *Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles and Techniques* (Réduction des risques liés aux ransomwares grâce au modèle Zero Trust : renforcer votre protection grâce aux techniques et aux principes Zero Trust), Forrester Research, 8 juin 2020
5. *Securing the Enterprise's New Perimeters* (Protection du nouveau périmètre des entreprises), Gartner, 27 mars 2020
6. *Network Segmentation* (Segmentation réseau), blog Forescout, janvier 2019
7. *Network Management Megatrends 2020* (Rapport 2020 sur les grandes tendances en matière de gestion des réseaux), rapport de recherche d'Enterprise Management Associates, avril 2020
8. *Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer* (Cinq questions du conseil d'administration auxquelles les responsables de la sécurité et de la gestion des risques doivent savoir répondre), Gartner Research, juillet 2019

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

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

À PROPOS DE FORESCOUT

Leader de la sécurité de l'Enterprise of Things, Forescout offre une plateforme globale qui identifie et segmente en continu tous les objets connectés des réseaux hétérogènes, en appliquant une politique de conformité. La plateforme Forescout est une solution d'entreprise ultra-évolutive et très populaire, qui offre une visibilité et un contrôle sans agent sur les appareils. Elle peut être déployée rapidement dans votre infrastructure existante, sans nécessiter d'agent, de mise à niveau ou d'authentification 802.1X. Les entreprises du classement Fortune 1000 et les organismes publics font confiance à Forescout pour réduire le risque de perturbation des activités due à des incidents ou à des compromissions, pour assurer leur conformité et en donner la preuve, ainsi que pour augmenter la productivité des opérations de sécurité.

forescout.fr

info-france@forescout.com

Tél. (international) +1-408-213-3191

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