



FORESCOUT

Découvrir & sécuriser vos
équipements IT, IoT, OT

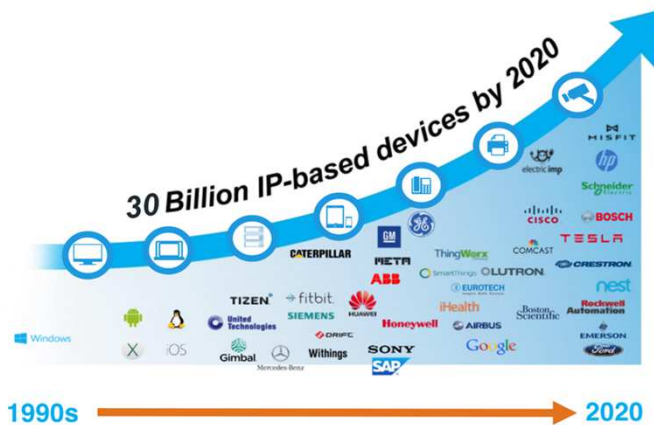
Cédric ANTOINE
System Engineer



Contexte : un Manque de visibilité croissant



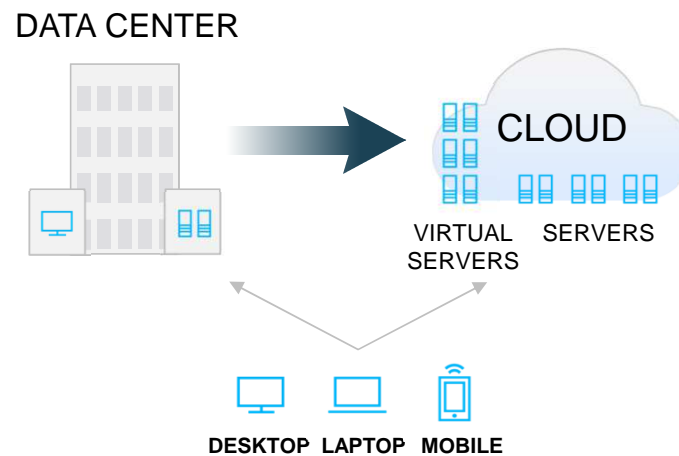
Augmentation & multiplication du type de plateforme



- < Diversification des différents types d'OS
- < Incapacité d'installer un agent sur ces nouveaux objets
- < Impossible d'avoir un agent sur tous les OS

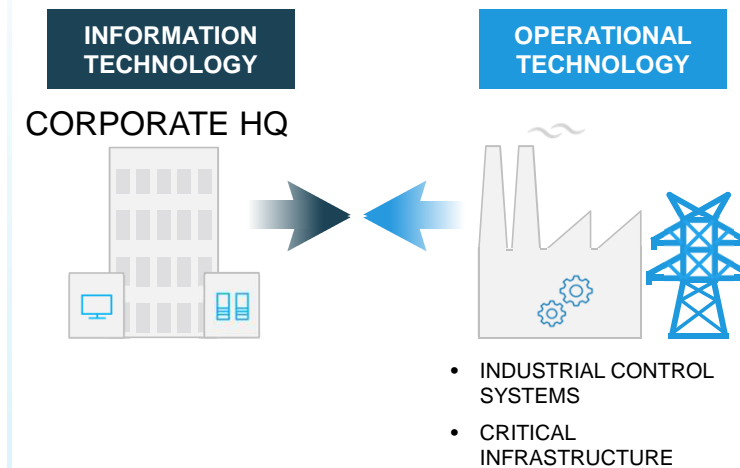
Gartner 2018 – 30 Billion Device by 2020

Adoption du Cloud



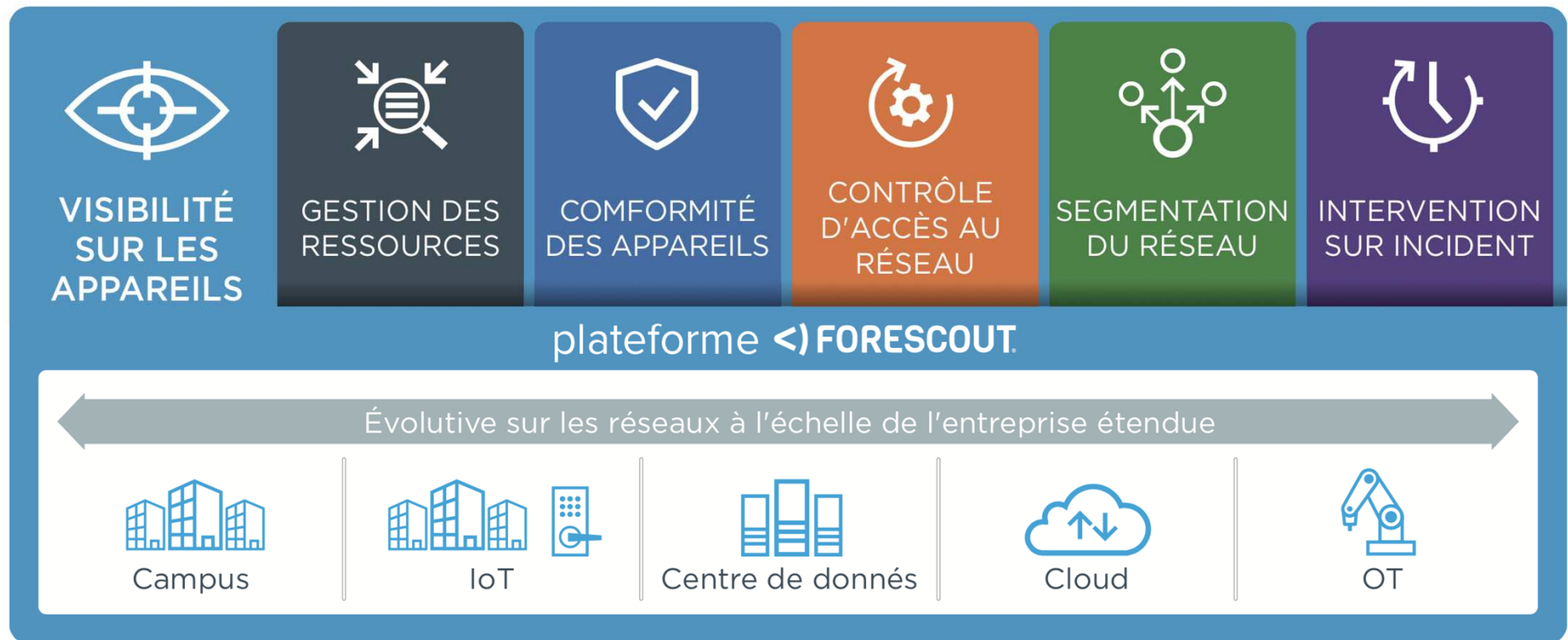
- < Environnement distribué
- < Environnement hétérogène / Multi-constructeurs
- < Manque de visibilité

Convergence des réseaux Bureautiques & Industriels



- < Le réseau OT est raccordé au réseau IT
- < Des menaces qui transitent de l'IT vers l'OT
- < Des équipements non ou peu patchables et donc très vulnérables.

Notre Mission





VISIBILITE DES
EQUIPEMENTS

Comment procédons nous ?

Que faisons nous ?

DECOUVRIR tous les équipements connectés en IP



Physique



Virtuel

CLASSIFIER tous les équipements & les catégoriser en conséquence

IoT



AxisCamHD

BYOD



HP Elite Tablet
on Windows 10

Managé



Red Hat Linux
on VMware vSphere

EVALUER la posture par



OS



App



Agent



Utilisateur



Comment le faisons nous?

Sans Agent

- ✓ Pas d'agent nécessaire
- ✓ Utilisation de techniques passives & actives

Hétérogène

- ✓ Intègre >70 technologies réseau & sécurité
- ✓ Etendu > Campus, DC, Cloud, OT

Intelligent

- ✓ Device Cloud ~1500 clients qui contribuent / 7M profils
- ✓ Taxonomie Complète de l'IT & l'OT

Continue

- ✓ Temps réels, pas besoin de scan programmés
- ✓ Notre moteur vérifie en permanence l'état des machines

Forescout eyeExtend

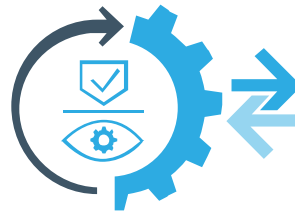
Plus de 300 intégrations de réseau/sécurité



Supprimer le
fonctionnement en silo

Maximiser vos investissements

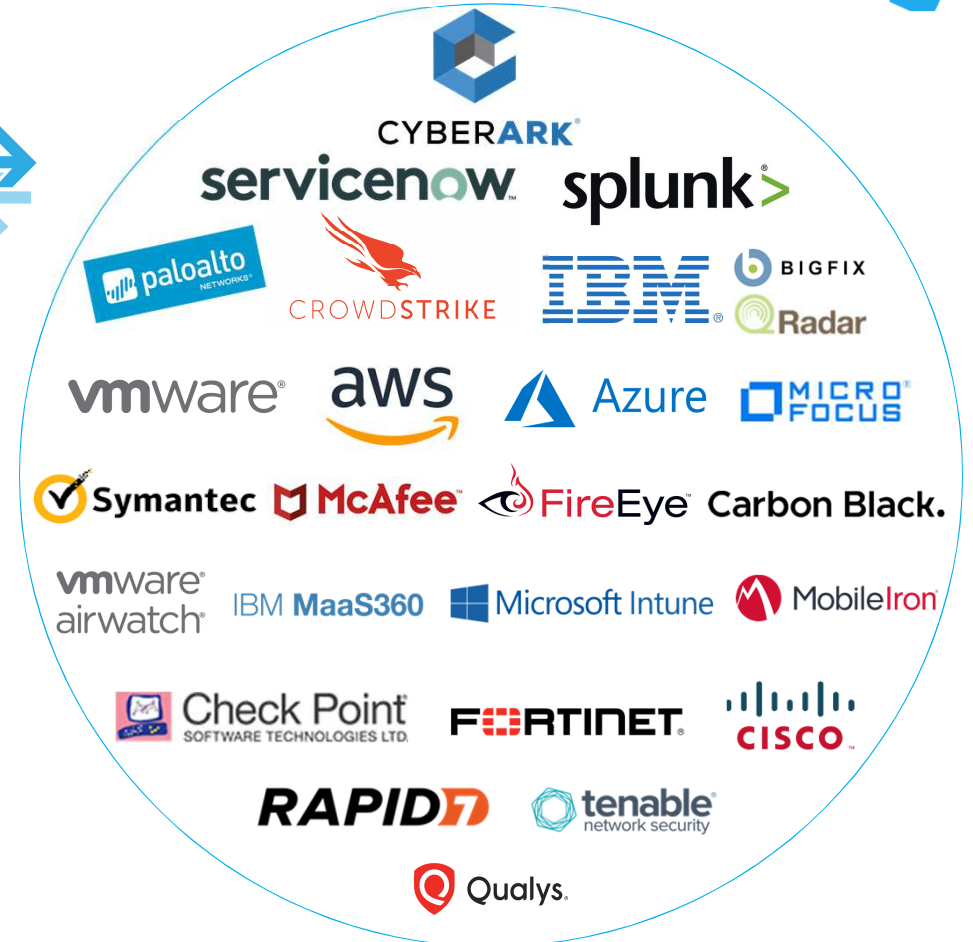
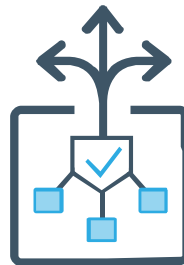
<) Echange
d'information



<) Automatisation



<) Automatiser
les réponses
à Incident



To learn more, visit: www.forescout.com/platform/eyeextend/



<) Réduire le risque lié aux
équipements IoT et P

Réduire le risque lié aux équipements IoT et Réseaux



Les challenges

Challenge Client

Equipements IoT avec des identifiants connu ou faible sur votre réseau

Des « Malware » exploitent cette faiblesse

Comment identifiez-vous ces équipements et comment les segmentez-vous ?



Réponse ForeScout



Identifie les équipements avec de faibles identifiants par :

- Type d'équipement
- Localisation
- Port réseau



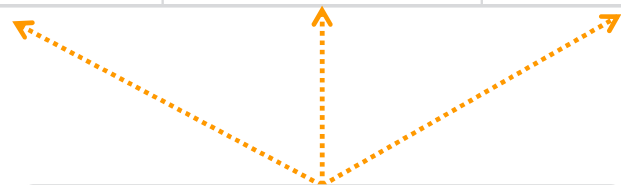
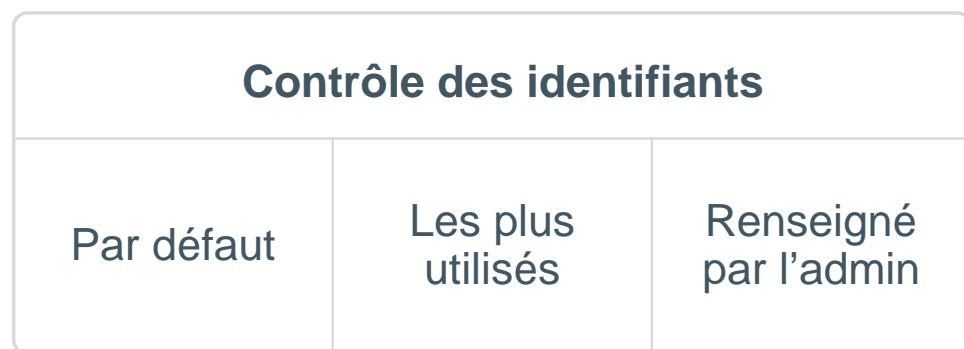
Soyez averti en temps réels des équipements IoT
Email, Ouverture d'un ticket, etc



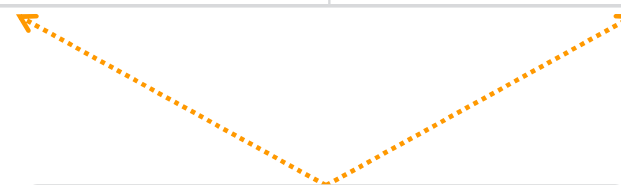
Limiter / bloquer l'accès au réseau si besoin

Réduire le risque lié aux équipements IoT et Réseaux

Plusieurs contrôles disponibles



Protocole SSH et Telnet

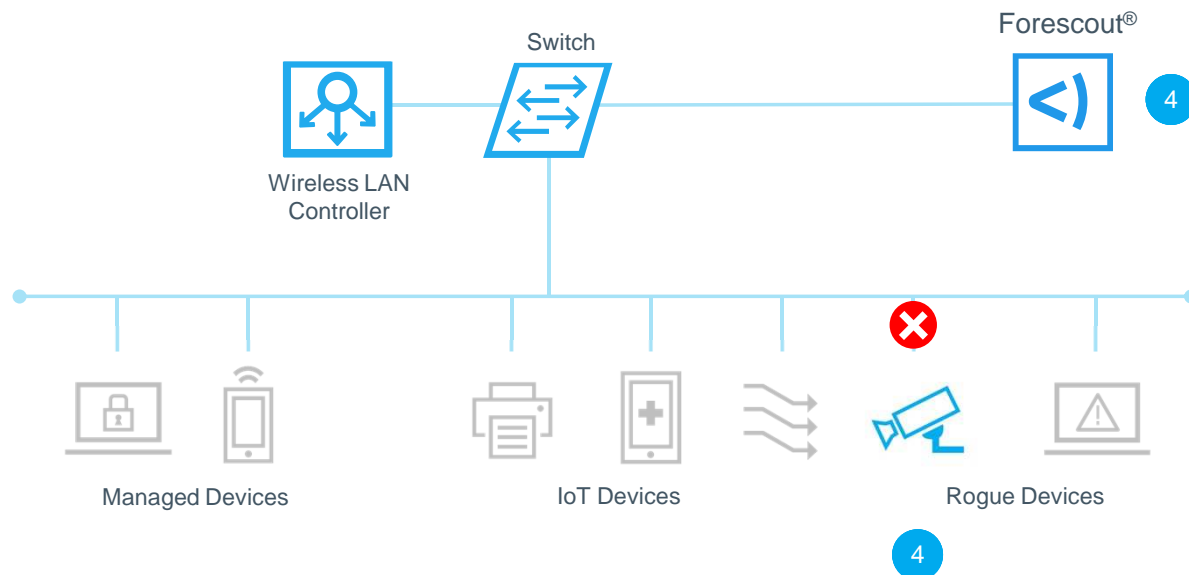


Protocole SNMPv2

Les librairies « par défaut » et « les plus utilisés »
sont mis à jour par Forescout lors de mise à jour

Réduire le risque lié aux équipements IoT

Cas d'usage



- 1 Forescout découvre un équipements et le classeifie comme un équipement de type IoT.
- 2 Utilisant **sa base d'identifiant par défaut***, Forescout effectue un contrôle SSH, Telnet et SNMP de l'équipement. Si l'équipement accepte l'identifiant, Forescout peut contenir alerter l'administrateur, limiter l'action de l'équipement ou encore bloquer l'équipement de façon automatique.
- 3 Utilisant **sa base d'identifiant les plus connus****, Forescout effectue un contrôle SSH, Telnet et SNMP de l'équipement. Si l'équipement accepte l'identifiant, Forescout peut contenir alerter l'administrateur, limiter l'action de l'équipement ou encore bloquer l'équipement de façon automatique.
- 4 Utilisant **sa base d'identifiant personnalisable*****, Forescout effectue un contrôle SSH, Telnet et SNMP de l'équipement. Si l'équipement accepte l'identifiant, Forescout peut contenir alerter l'administrateur, limiter l'action de l'équipement ou encore bloquer l'équipement de façon automatique.

* Fourni par Forescout

** Fourni par Forescout

*** Personnalisable par l'administrateur

<) Evaluer la conformité de vos
équipements

Evaluer la conformité de vos équipements

Les challenges



Challenge Client

Contrôle de Conformité réel vs attendu

Gestion de la conformité sur des équipements non-traditionnels

Avez vu une visibilité sur vos VM / PC?
Sont-elles conformes à votre politique d'entreprise ?



Réponse Forescout



Évaluez vos équipements en temps réels :

- Modèle d'Antivirus, Date des signatures AV
- Version OS
- Applications Cloud, P2P,
- Disque chiffré, Clé USB branché



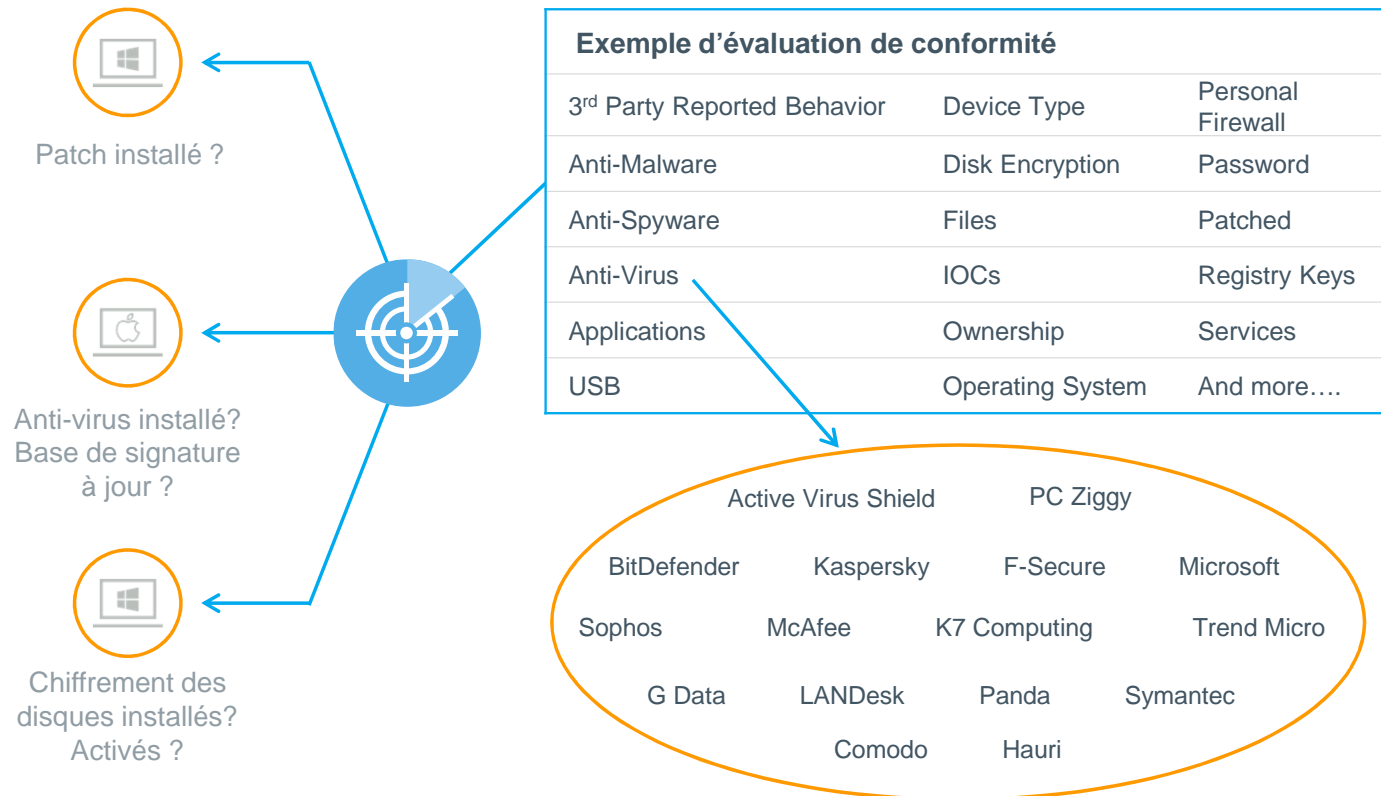
Soyez averti en temps réels, ou agissez automatiquement
Lancer MAJ, désinstallation d'application

Evaluer la conformité de vos équipements

Evaluation continue des équipements

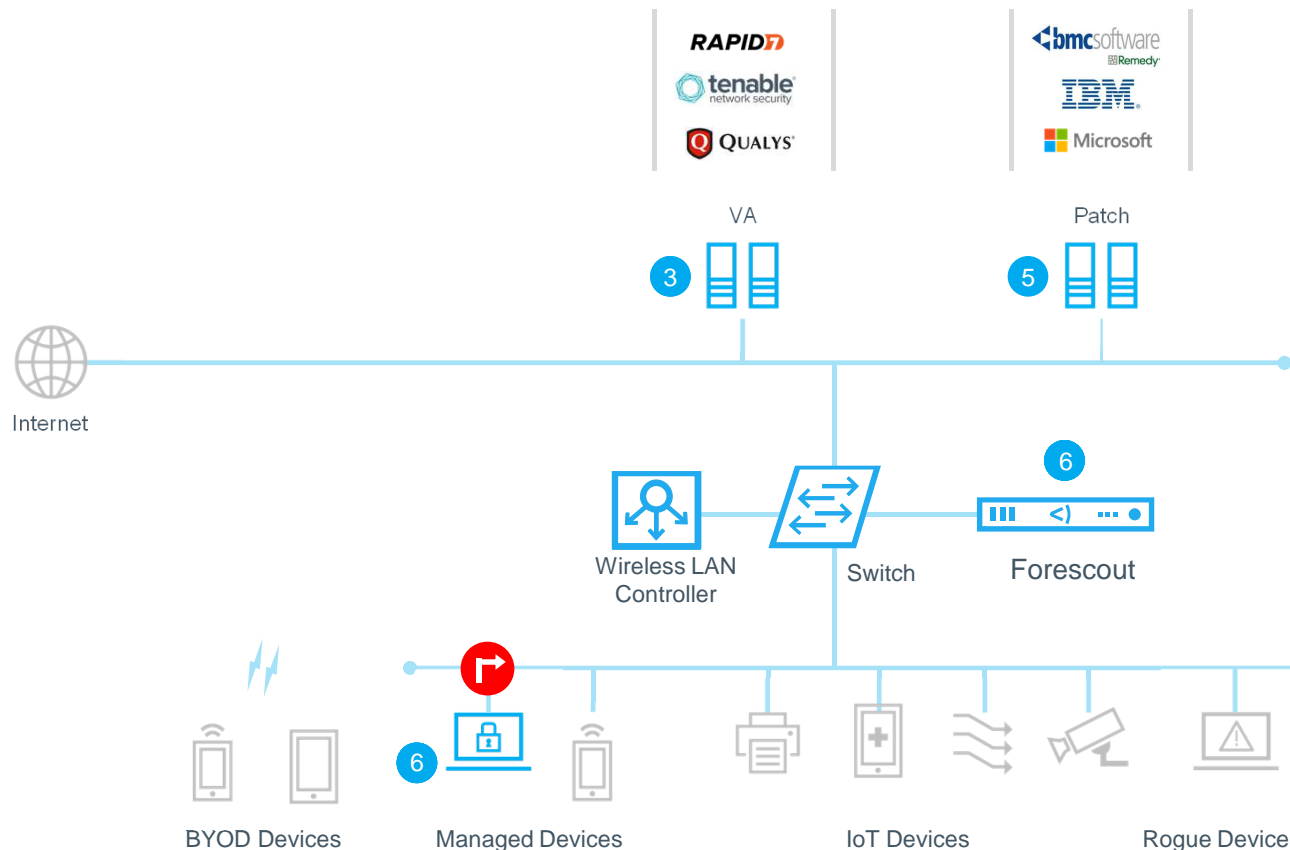


- <> Vérifier que vos équipements sont conformes à vos politiques de sécurité
- <> Examiner vos équipements avant de fournir un accès complet
- <> Notification, Remédiation, Restriction automatique en cas de non-conformité



Evaluer la conformité de vos équipements

Cas d'usage



- 1 ForeScout détecte en temps réel un équipement qui se connecte au réseau
- 2 ForeScout demande au système de gestion des vulnérabilités (VA) de lancer un scan de l'équipement
- 3 Le système de vulnérabilités envoie les résultats du scan à ForeScout
- 4 Suite au résultat du scan, ForeScout place l'équipement dans un VLAN de remédiation.
- 5 ForeScout demande au système de gestion des patches d'effectuer une mise-à-jour des patches
- 6 Après remédiation, ForeScout fournit à l'équipement les droits d'accès réseau appropriés.

- ➔ **Limiter l'accès réseau des terminaux identifiés à risque par le système de gestion des vulnérabilités.**
- ➔ **Correction des vulnérabilités ou failles de sécurité**



<) Diminuer les risques avec
segmentation dynamique

Diminuer les risques avec la segmentation dynamique



Les challenges

Challenge Client

Pour chaque changement / ajout d'équipement, l'équipe IT doit être avertie en amont.

Comment garantir que l'équipement raccordé est bien celui autorisé ?

Etes-vous averti lors du remplacement d'une imprimante (ou autre) par un PC



Réponse Forescout



Affectation des VLAN dynamiquement et **sans agent**.



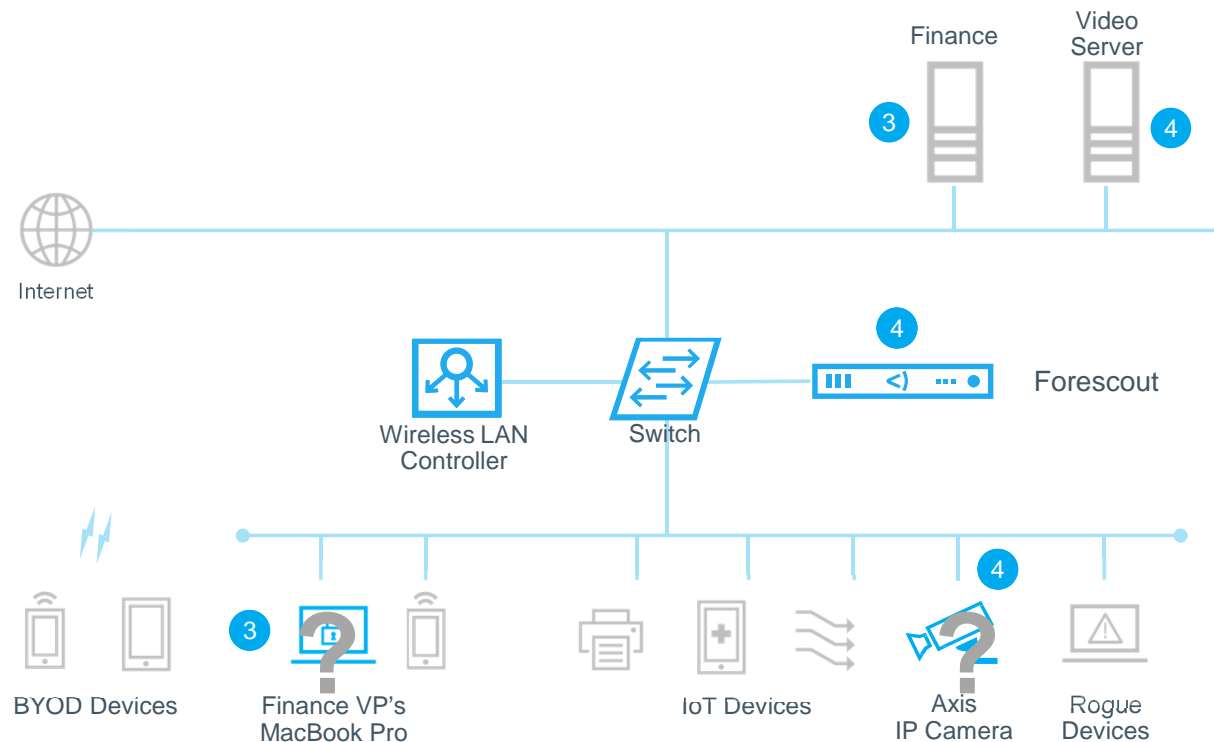
Classification **multicritère**, permettant de garantir la fonction de l'équipement



Notification des équipes IT Action (VLAN, ACL, ...)

Diminuer les risques avec la segmentation dynamique

Cas d'usage



- 1 Fore Scout découvre les périphériques se connectant au réseau.
- 2 Fore Scout classe ces périphériques sur la base du type, de son propriétaire et du rôle de l'utilisateur.
- 3 Fore Scout place l'utilisateur du service "finance" détenteur d'un PC d'entreprise dans le VLAN "finance"
- 4 Fore Scout segmente les caméras d'entreprises afin de ne les faire communiquer qu'avec le serveur vidéo, sur base d'ACL et/ou de VLAN.



Merci

Cédric ANTOINE

Mail: cedric.antoine@forescout.com