

Forescout

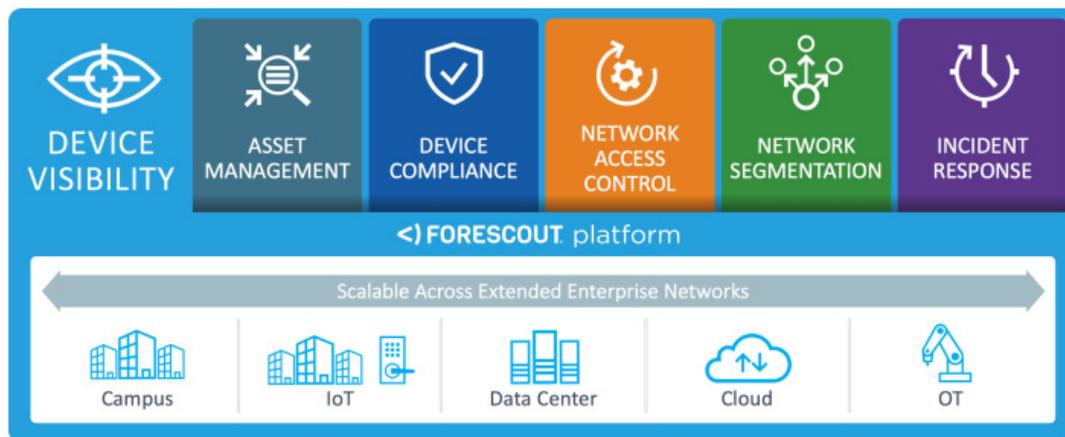
Visibilité et Contrôle de tous les devices connectés, dans tous les réseaux



D'après Gartner, en 2023, un DSI aura en charge plus du triple de endpoints qu'il n'en gérait en 2018. On estime qu'en 2021, 70% de la sécurité industrielle (OT) sera géré par les responsables sécurité IT contre la moitié aujourd'hui. Prendre la main sur la sécurité de tous les devices se connectant au réseau est devenu critique. Forescout Technologies est aujourd'hui le leader de la visibilité et du contrôle des devices du réseau. Sa plateforme unifiée permet d'avoir une vue exhaustive et contextuelle de tous les environnements de l'entreprise et d'orchestrer des actions afin de réduire les risques cyber et opérationnels liés à ces devices.

LA SECURITE COMMENCE PAR LA VISIBILITE

Pour répondre au besoin de connaissance de tout ce qui peut se connecter aux réseaux d'une entreprise, Forescout va simplement offrir 100% de visibilité sur les devices. Cette visibilité va permettre d'établir un inventaire très précis, de vérifier et d'appliquer la conformité de ces devices en continu, de contrôler leur accès en fonction de règles, et de répondre rapidement aux incidents de sécurité.



POURQUOI FORESCOUT ?

Les solutions Forescout se déploient sans intrusion et

sans agent dans le réseau, pour réaliser une découverte en temps réel et une classification de tout

device IP connecté au réseau, ainsi qu'une évaluation continue de leur posture de sécurité et de leur intégrité.



Distribué en France par MIEL

01 60 19 34 52 - www.miel.fr/forescout



Visibilité complète sans agent et sans scan actif (critique pour les devices IoT et OT)



Classification granulaire contextuelle de tout device IP connecté



Monitoring continu de l'état des devices et mise en place de règles adaptatives



Résultats rapides en utilisant l'infrastructure réseau existante et les outils de sécurité en place



Jusqu'à 2 M de devices dans les réseaux campus, data center, cloud et OT

VISIBILITÉ

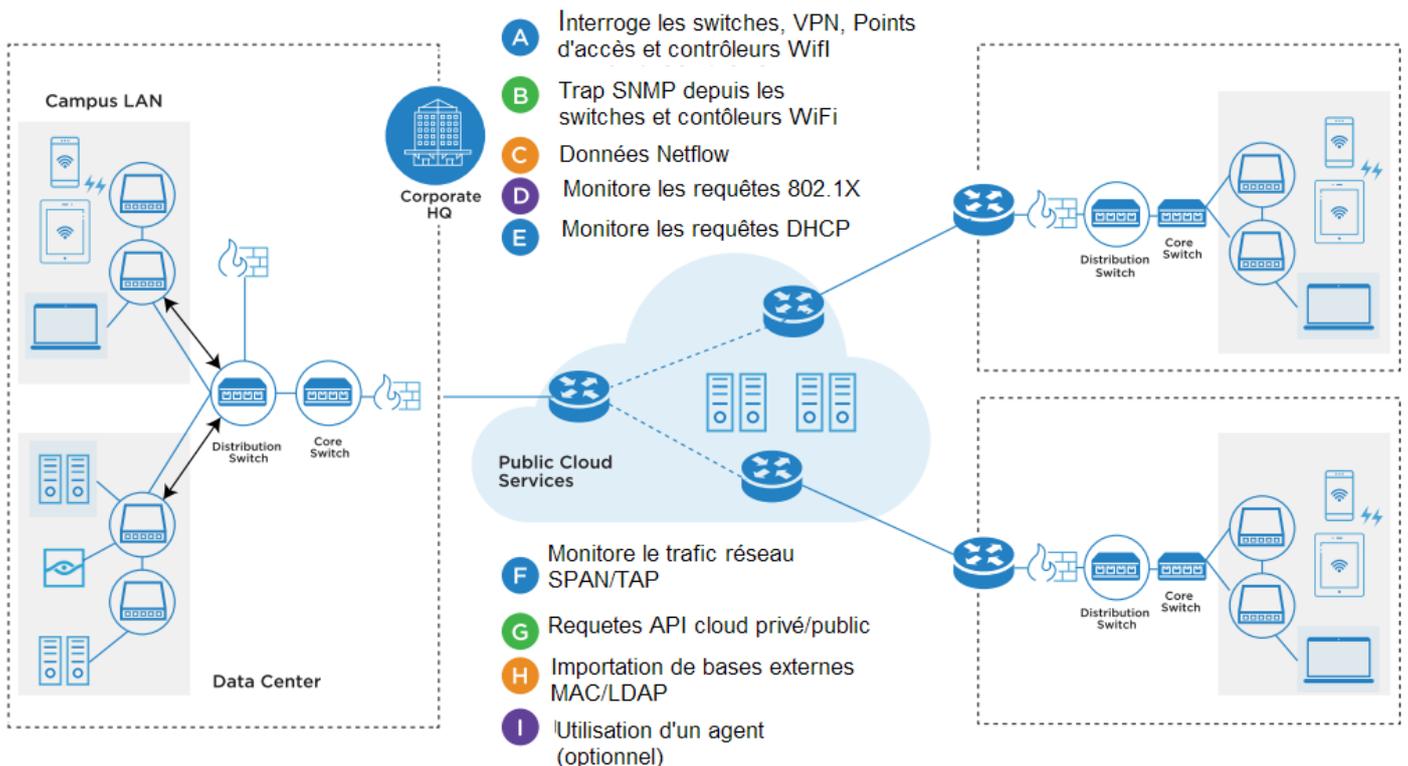
La fonctionnalité fondatrice de la plateforme Forescout est la visibilité : on ne peut contrôler que ce que l'on voit.

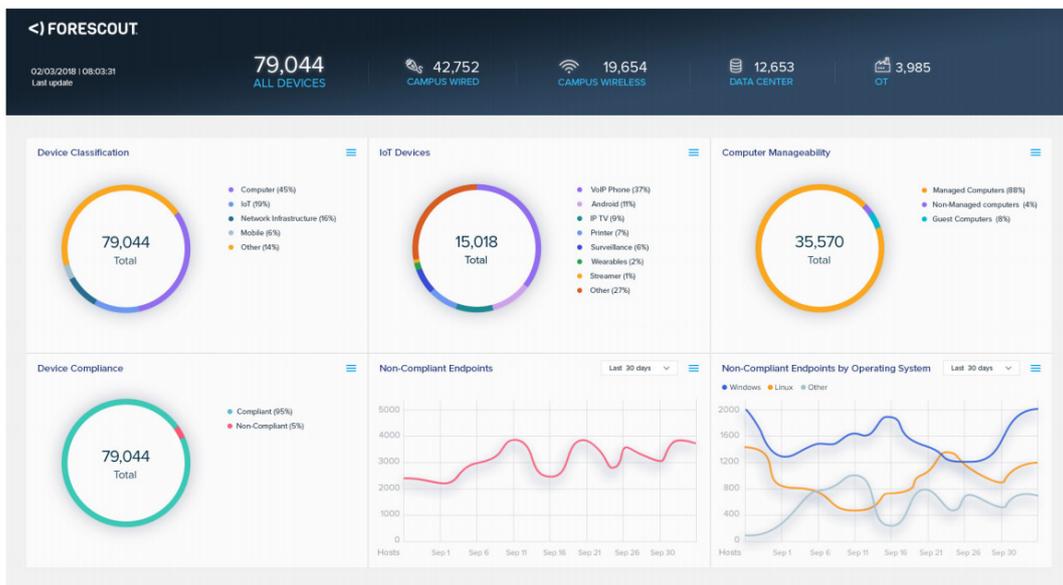
La solution Forescout :

- Découvre et classe les devices automatiquement – pas d'agent requis
- Évalue la posture de sécurité du device et son intégrité, que le device soit managé, non managé, ou un device IOT/OT. Le tout se fait sans risquer une interruption de service
- Monitore en continu le profil et la conformité des devices qui entrent et sortent du réseau

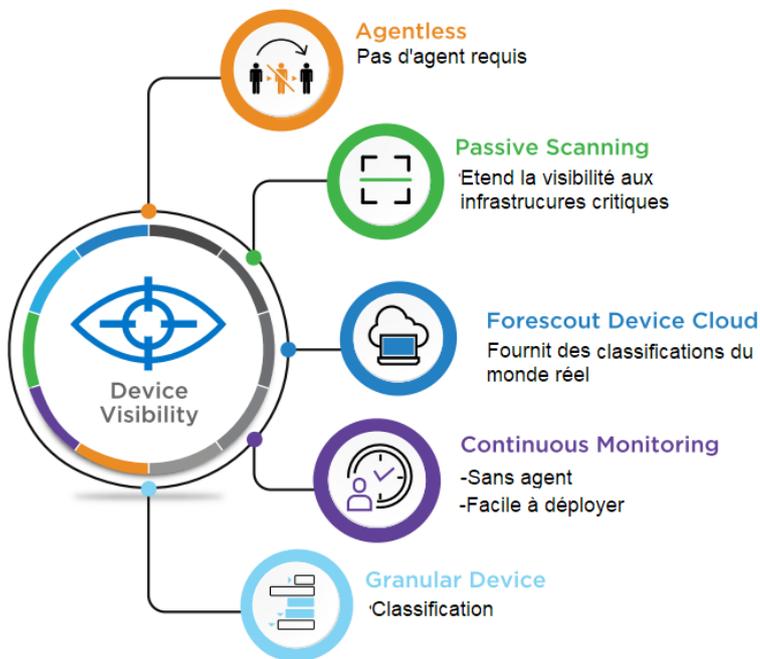
LES TECHNIQUES DE VISIBILITÉ

Forescout utilise une combinaison unique de techniques pour avoir une vue exhaustive de tout type de device.



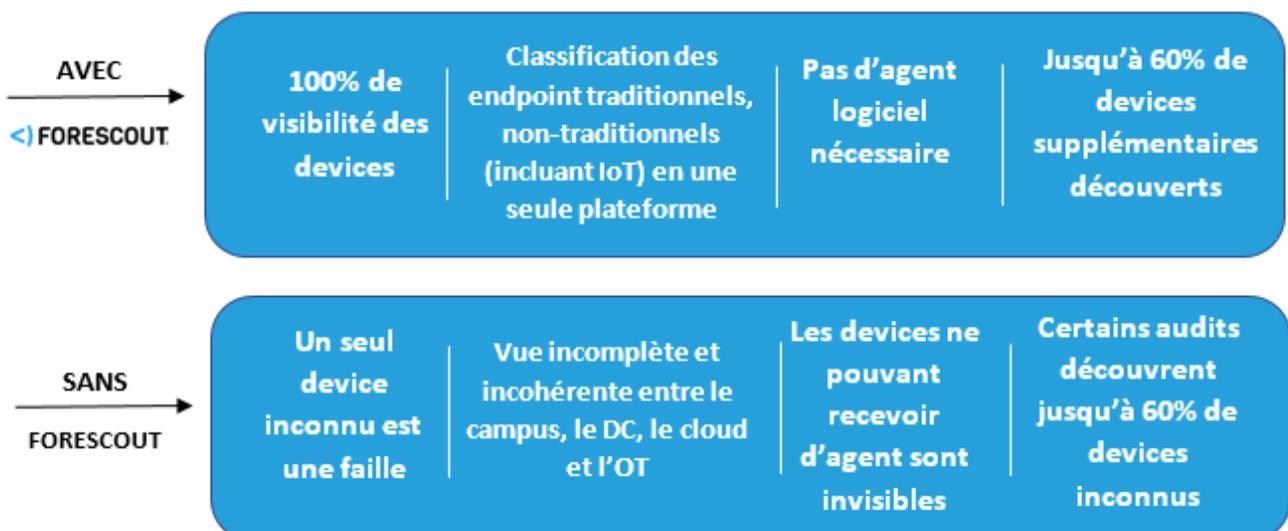


LA DIFFERENCE DE FORESCOUT : LA VISIBILITÉ



Forescout va permettre de découvrir jusqu'à 60% de devices en plus des devices déjà connus.

L'écart avec les solutions du marché de fait dès le début du déploiement. Forescout est la seule plateforme qui unifie la gestion de tous les types de device tout en étant sans agent :



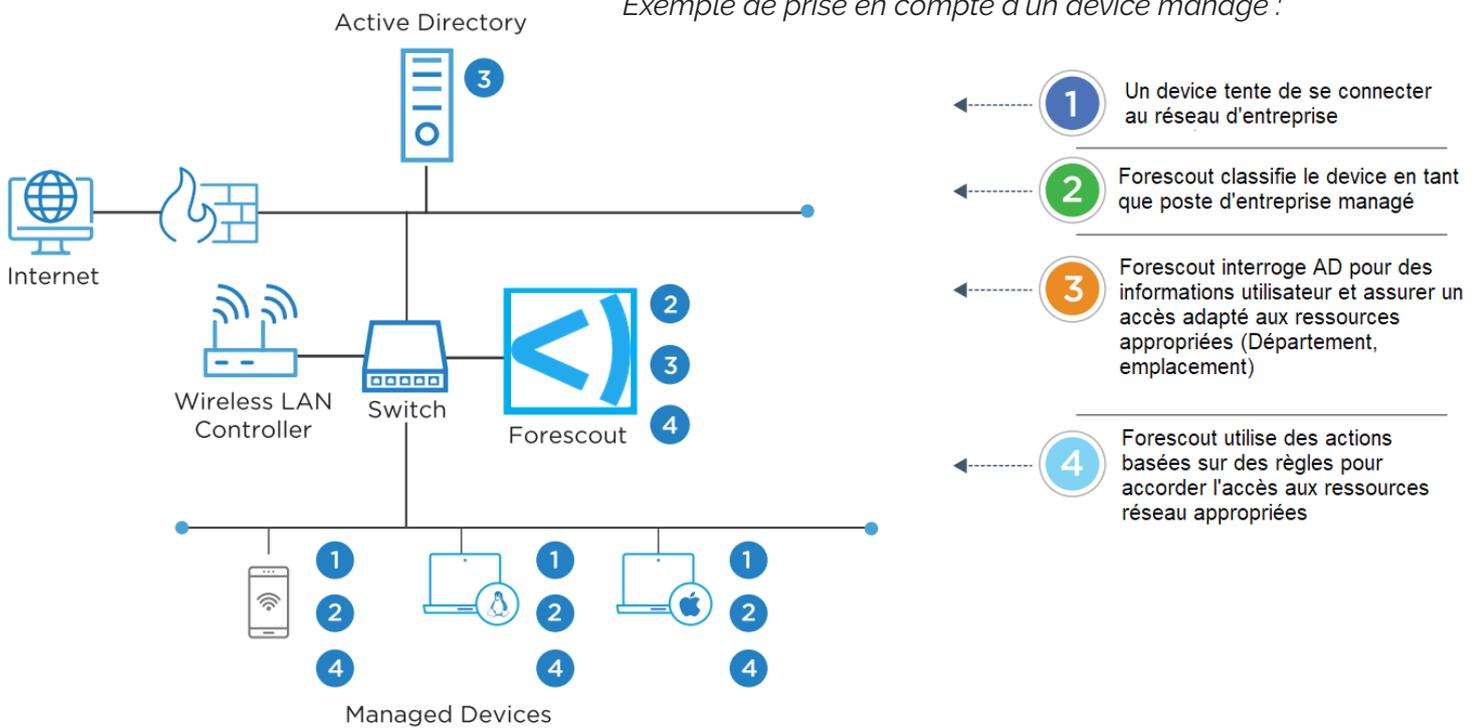
NAC : CONTRÔLE D'ACCÈS AU RÉSEAU

La visibilité exhaustive de Forescout va directement impacter une fonctionnalité clé : le NAC (Contrôle d'accès au réseau). Forescout va contrôler l'accès au réseau des devices qui entrent et sortent du réseau, qu'ils soient physiques ou virtuels, managés ou non managés

L'approche de Forescout pour le NAC (Network Access Control) est simple :

- Déploiement rapide d'une plateforme unifiée de visibilité et contrôle à travers des réseaux hétérogènes
- Contrôler l'accès aux ressources sensibles sur la base du profil du device et de l'utilisateur, sans mise-à-jour réseau et sans dépendance vis-à-vis du fabricant réseau
- Appliquer des règles sur les switches filaires et sans fil, les firewalls physiques ou virtuels, avec ou sans authentification 802.1X

Exemple de prise en compte d'un device managé :



AVEC FORESCOUT.

Visibilité et classification sans agent	Visibilité avec évaluation des configurations	Gestion des accès cohérente	Segmentation dynamique	Monitoring continu	Remédiation automatique pour un accès réseau approprié	Moteur de règles flexible et simple	Déploiement et administration simples	Orchestration réseau via de multiples intégrations
---	---	-----------------------------	------------------------	--------------------	--	-------------------------------------	---------------------------------------	--

SANS FORESCOUT.

Visibilité IoT limitée	Agent requis (conduisant à une visibilité limitée)	Contexte limité pour un contrôle d'accès adéquat	Design complexe (802.1X requis + autres technologies nécessaires)	États des lieux ponctuels	Remédiation automatique limitée	Moteur de règles complexe à gérer	TCO et complexité de déploiement élevés	Intégration limitée avec des systèmes tiers
------------------------	--	--	---	---------------------------	---------------------------------	-----------------------------------	---	---

SEGMENTATION RÉSEAU

La plateforme Forescout va coordonner des technologies disparates pour concevoir et déployer une segmentation dynamique du réseau de l'entreprise. L'approche multicouches de Forescout couvre tous les domaines réseaux, et permet une mise en place de règles multi-éditeurs granulaires et unifiées, réduisant ainsi la complexité, les coûts et l'impact sur l'activité.

- Visualisation des flux identifiés par users, applications, services et appareils
- Conception et simulation de règles de segmentation logique pour mesurer l'impact des règles avant application
- Suivi temps réel de l'hygiène de segmentation et réponse aux violations des règles
- Application dynamique de règles de contrôle entre différentes technologies et domaines réseau

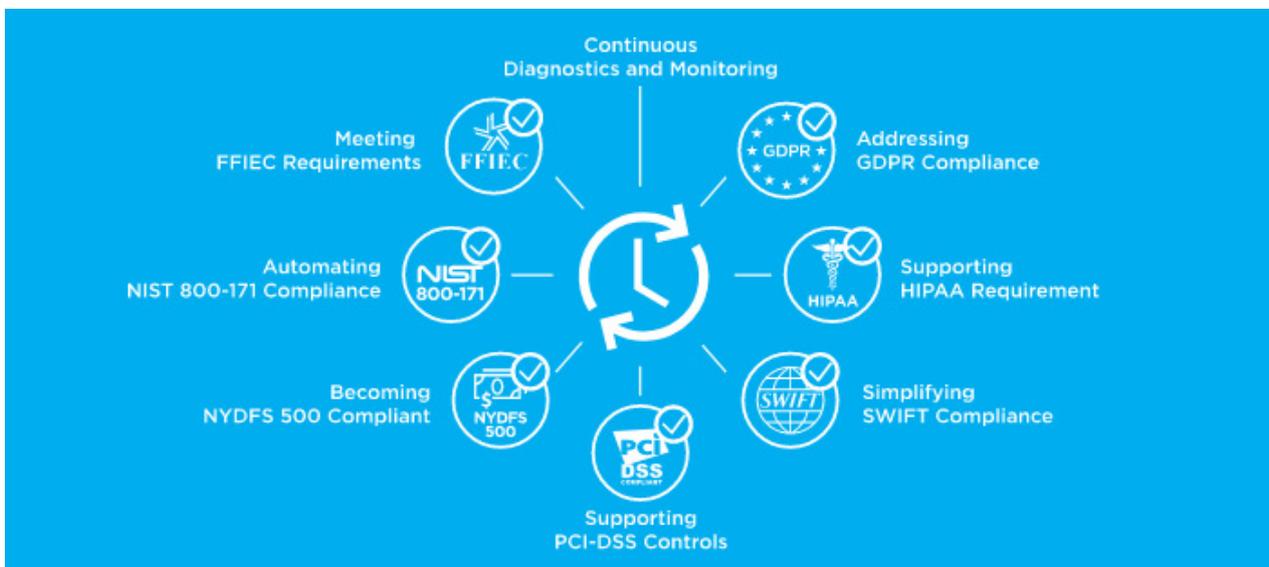


CONFORMITÉ

La plateforme Forescout permet d'automatiser la mise en conformité des devices et de prendre des actions immédiates dès que des devices virtuels ou physiques ne remplissent pas les critères associés.

Pour la mise en conformité, la plateforme Forescout :

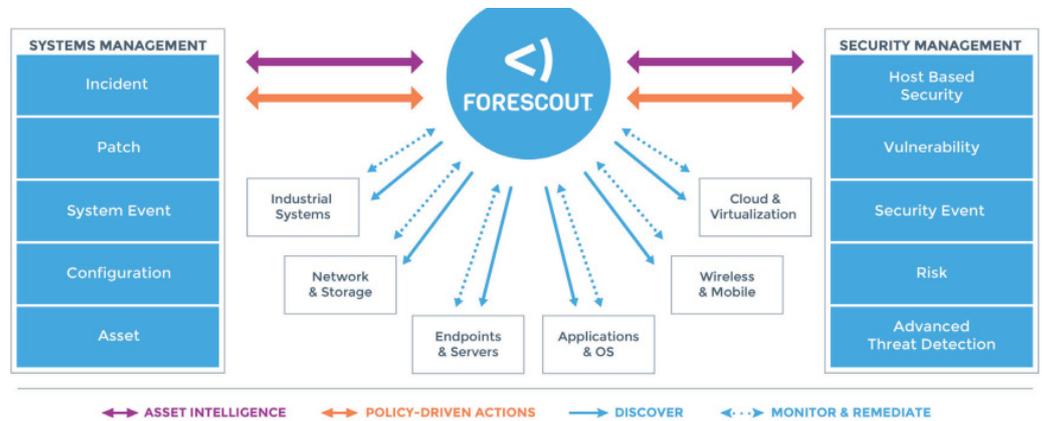
- Identifie Qui, Quoi, Où, la version d'OS, etc. des appareils en quelques secondes
- Contrôle les configurations système et gère les mots de passe faibles ou par défaut
- Détecte/restaure les agents, logiciels ou services manquants/défectueux sur les endpoints
- Valide l'adhésion à une norme établie



GESTION DES ACTIFS (ASSET MANAGEMENT)

La plateforme Forescout fournit un inventaire temps-réel des devices du réseau sans requérir d'agent. On dispose ainsi d'une liste constamment à jour des actifs, indépendante d'erreurs humaines de classification, et permettant ainsi de prendre des décisions de sécurité et d'organisation sans approximation.

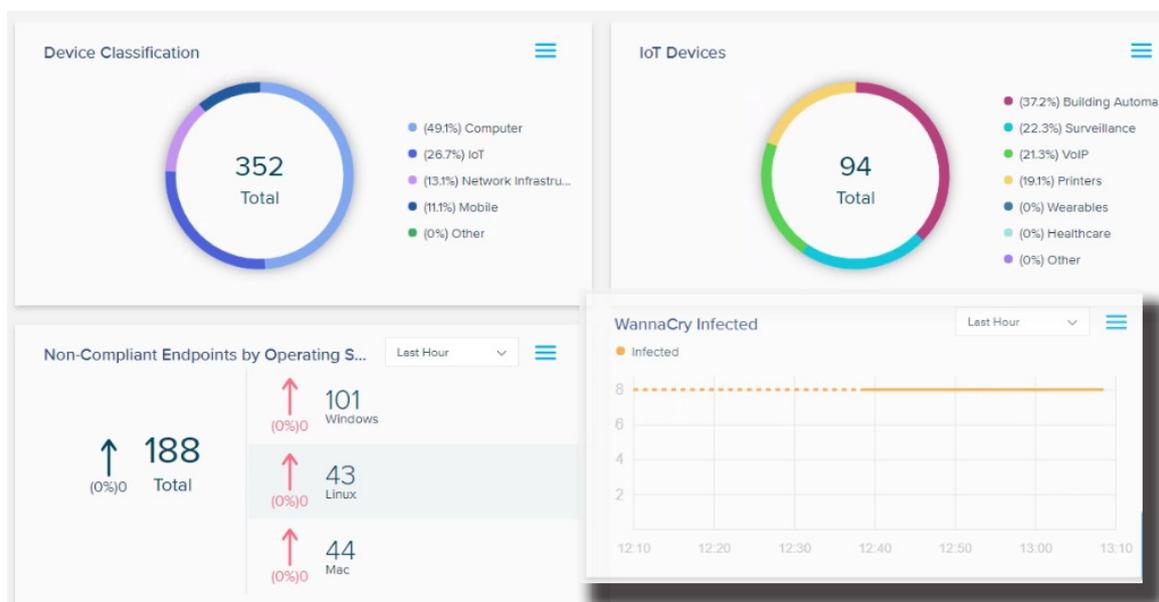
- Élimine les angles morts créés par les outils de scan périodiques grâce à un inventaire et un monitoring continus
- Gère efficacement la posture de sécurité et le cycle de vie des devices
- Partage les informations contextuelles avec les équipes opérationnelles, le helpdesk, et les outils ITSM comme ServiceNow®



RÉPONSE AUX INCIDENTS

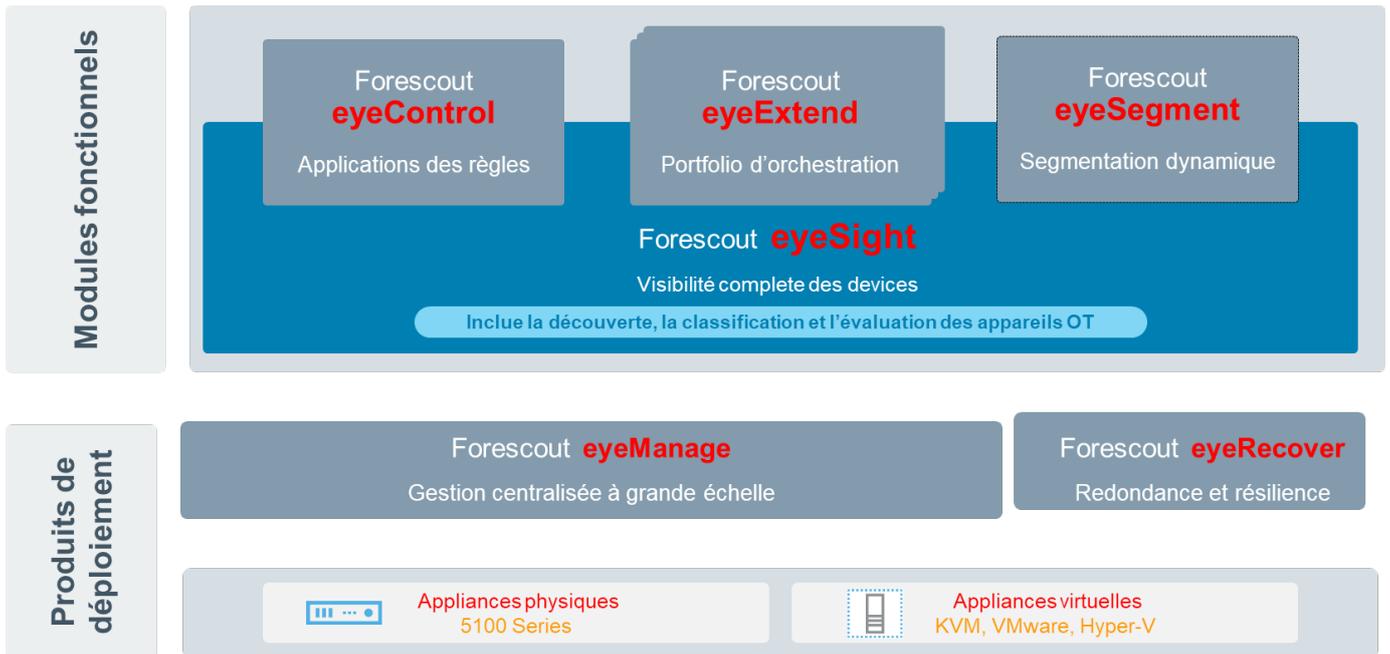
La plateforme Forescout détecte et évalue l'intégrité du poste dès la première connexion. Elle orchestre ensuite la réponse éventuelle à une anomalie en temps réel en coordonnant tous les outils de management et de sécurité existants. L'ensemble réduit la fenêtre d'exposition aux menaces, et optimise l'utilisation de l'infrastructure de sécurité en place.

- Unifie les règles de sécurité entre le campus, le data center, le cloud et les environnements OT, sans agent
- Automatise la détection, la recherche et l'endiguement des menaces pour accélérer la réponse à incident.
- Exploite une interopérabilité native avec + de 20 solutions de sécurité grâce aux produits Forescout eyeExtend

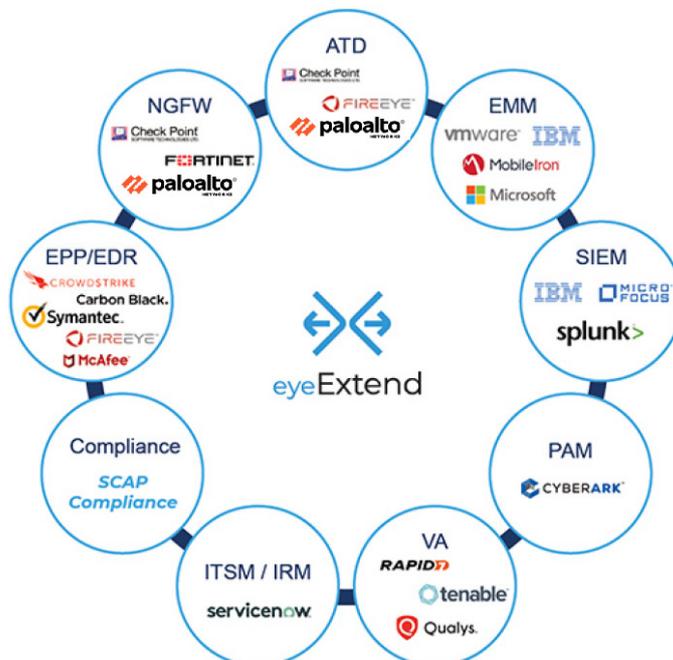


L'OFFRE PRODUIT FORESCOUT

La plateforme Forescout se déploie de manière transparente dans le réseau au travers d'appliances matérielles ou virtuelles, auxquelles s'associent des modules correspondant aux différents cas d'usage de visibilité et de contrôle. Les solutions assurant la haute disponibilité du service et la gestion centralisée complètent l'offre.



eyeExtend représente l'offre technologique d'intégration la plus complète du marché, permettant d'exploiter au maximum l'infrastructure existante et de répondre à tous les cas d'usage de contrôle des devices.



FORESCOUT TEST DRIVE

METTEZ-VOUS AUX COMMANDES DE LA PLATEFORME FORESCOUT



Les Tests Drives sont des sessions virtuelles de prise en main de la plateforme ForeScout durant laquelle l'utilisateur est guidé par un expert tout au long de six cas d'utilisation tirés de situations réelles.

Le Test Drive est l'occasion de constater par soi-même la puissance de la solution.

Contactez-nous pour plus d'informations au **01 60 19 02 30**

LES 6 ÉTAPES DU TEST DRIVE

N°1 Visibilité Comment découvrir et classer les devices	N°2 Gestion des Actifs Réaliser un audit / inventaire matériel et logiciel	N°3 Conformité des appareils Vérifier une conformité et notifier en cas de non-conformité
N°4 Intervention sur incident Faire une règle automatisée contre un ransomware	N°5 Contrôle d'accès au réseau Blocage, mise en quarantaine de postes non à jour	N°6 Segmentation du réseau Règles d'accès en fonction du type et du niveau du poste

MIEL ACADEMY FORMATIONS FORESCOUT

Miel est un centre de formation ForeScout depuis de nombreuses années.

Nos formateurs ont tous une très solide expérience avant-vente et après-vente afin de délivrer la formation la plus pertinente possible et possèdent le plus haut niveau possible de certification ForeScout.

FORESCOUT FSCA

Nos sessions inter-entreprises se déroulent à Paris, à Bièvres (91) et ponctuellement en région.

Nous proposons aussi des sessions sur-mesure en « intra » pour un minimum de 3 participants. Il est également possible de suivre des formations virtuelles avec formateurs, en ligne, pour toutes les dates à Paris et Bièvres.

La durée de la formation est de 4 jours

Elle permet de maîtriser tous les concepts de la plateforme, en particulier la notion de détection et de règles de contrôle.



Distribué en France par MIEL

Appelez le 01 60 19 34 52