Réduire les risques dus aux postes compromis lors du télétravail

L'après confinement ...

Beaucoup d'entreprises ont géré en grand nombre et massivement la transition de leurs employés vers le télétravail. Mais qu'en est-il du retour ? La plupart des responsables sécurité ont conscience que l'utilisation d'un grand nombre de postes dans un environnement physique autre que professionnel, génèrent des risques car la vérification de conformité et le contrôle de sécurité des postes ne peuvent matériellement pas se faire à un niveau suffisant.

Avec un retour massif au bureau des télétravailleurs après des semaines d'utilisation de leur poste à distance, donc avec moins de contrôle de sécurité et moins de mise-à-jour, l'**exposition aux risques** de l'entreprise va immédiatement et fortement augmenter.

Vu l'augmentation du nombre d'attaques constatée durant cette période, être "cryptolocké" et avoir ses outils IT impactés juste après le confinement serait dévastateur pour l'activité de l'entreprise, et au pire moment possible.

L'augmentation de la surface d'attaque, due à la multiplication des brèches créées lorsque les employés, les sous-traitants et les partenaires se reconnectent au réseau d'entreprise à travers le monde, va être **soudaine**, **rapide et sera difficile à gérer** pour les équipes sécurités et opérationnelles.

Forescout est un éditeur américain de cybersécurité qui fournit une solution pour imposer la conformité et réduire les risques en automatisant les contrôles de sécurité, la quarantaine, et le process de remédiation (« check-list » de sécurité, scan de vulnérabilité « à la demande », et « patching à la demande »). Forescout est un spécialiste de sécurité et le leader mondial dans ce marché (selon Gartner).

La solution Forescout est centralisée et peut être déployée très rapidement pour avoir un premier niveau de **visibilité** et de **contrôle** (solution Non-intrusive) avant la reconnexion massive des devices potentiellement compromis. Dans un "Mode post-connecté" (voir les détails ci-dessous), les prérequis pour un déploiement rapide sont largement acceptables dans la mesure où aucun changement de configuration réseau n'est nécessaire.

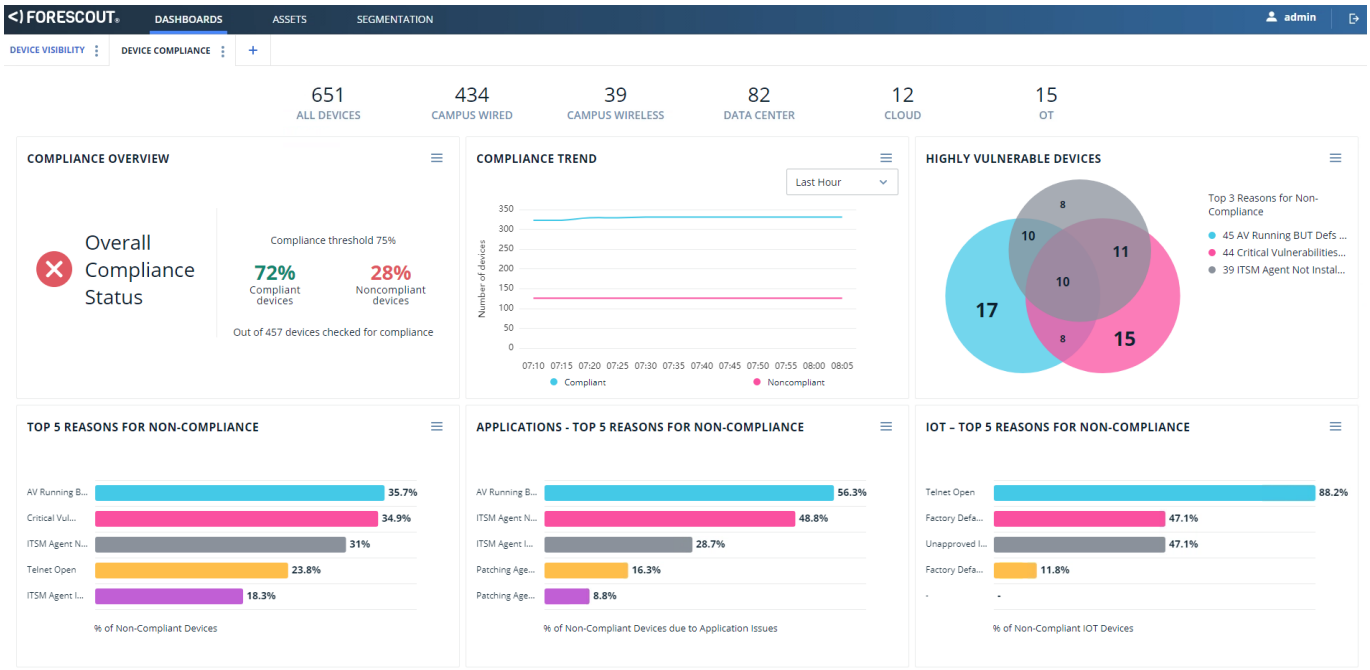
Distribué en France par MIEL

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

L'approche de Forescout

Court terme : Conformité

Forescout découvre en continu tous les appareils connectés sans avoir besoin d'aucun agent (solution non-intrusive). En utilisant les informations de Visibilité, Forescout peut déclencher une vérification de la posture de sécurité sur la base de critères multiples. Les plus communs sont l'antivirus (installé, actif, mis-à-jour), l'OS (patch installés) et même les audits de vulnérabilités fournis par des solutions tierces comme Rapid7.



Déploiement en Post-Connexion

Le déploiement en "post-connexion" est une stratégie de visibilité réseau et de contrôle d'accès à travers laquelle les endpoints sont initialement autorisés à accéder au réseau pendant que Forescout réalise leur profil afin de déterminer leur catégorie et leur niveau de conformité. L'accès au réseau est alors ajusté conformément au profilage obtenu et aux règles de sécurité.

Avantages

- Facile et rapide à déployer
- Accès réseau ouvert à priori puis contrôlé (fail open)
- Productivité et expérience utilisateur optimales

Challenges

- Délai avant la mise sous contrôle du endpoint (secondes)
- Besoin de gérer des exceptions

Déploiement en Pré-Connexion

Le déploiement en "Pré-connexion" est une stratégie de contrôle d'accès à travers laquelle les appareils se connectent initialement à un réseau filaire limité en accès pendant que Forescout réalise leur profil afin de déterminer leur catégorie et évaluer leur conformité. Les appareils en transit sont alors admis dans le réseau de production avec un niveau d'accès dépendant de l'utilisateur et des propriétés de l'appareil.

Avantages

- Quarantaine initiale par défaut

Challenges

- Expérience utilisateur
- Plus complexe à implémenter
- Plus lent à déployer
- Utilisation du réseau existant

Comme de nombreuses entreprises ne seront certainement pas en mesure de déployer les solutions Forescout à temps dans 100% de leurs sites, Forescout introduit le concept de "**Sanity Check Center**" : Les sociétés vont cibler des sites physiques ou des zones spécifiques, où des Appliances Virtuelles Forescout seront déployées. Ces sites constitueront une zone de transit où l'on demandera aux employés de faire leur première connexion.

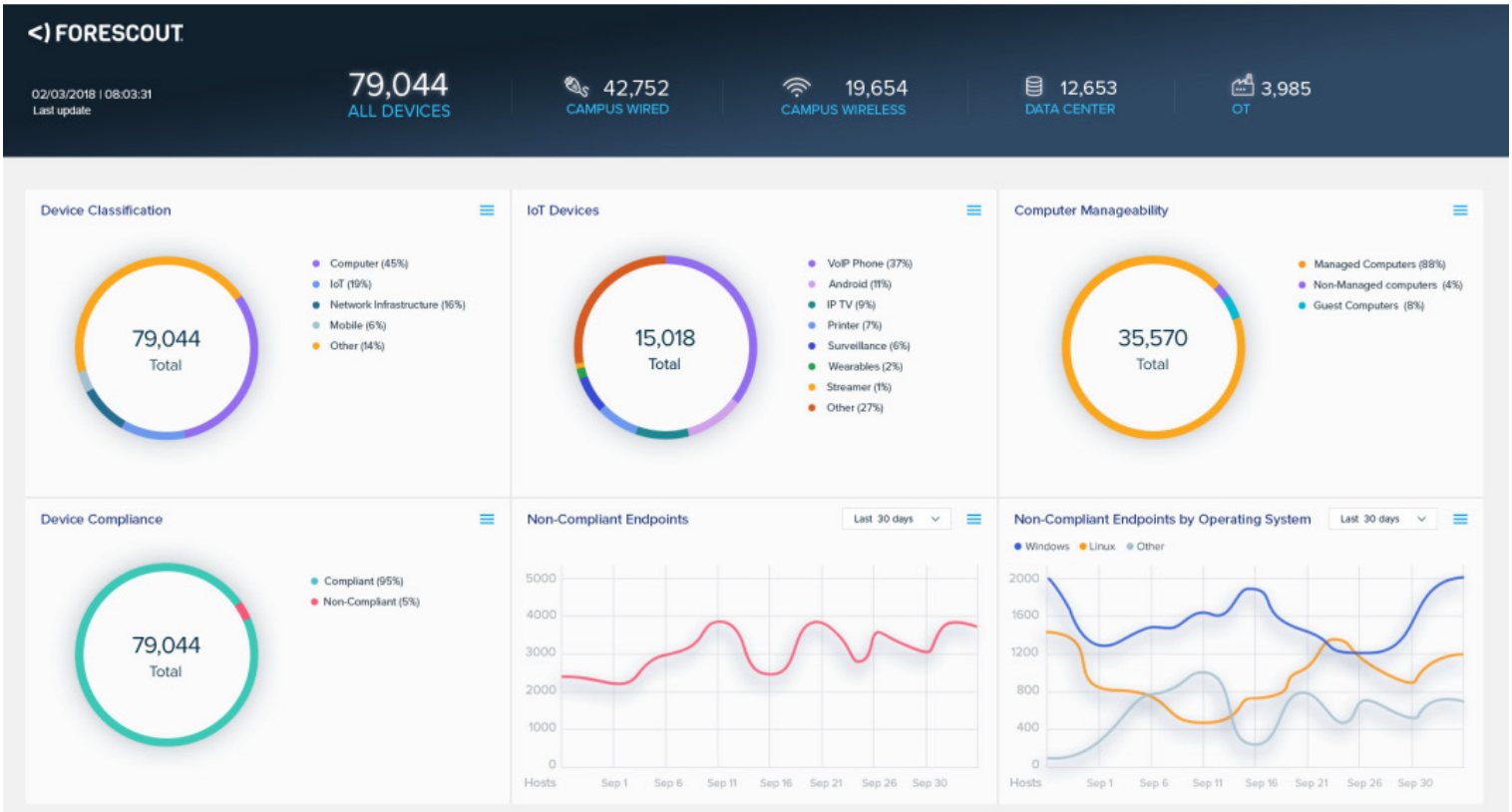
Afin de gérer une "**transition progressive**" au niveau IT, il sera demandé à tous les employés de se rendre physiquement dans un de ces "Sanity Check Center" pour la première connexion au réseau d'entreprise (pour les patchs et les vérifications de mises-à-jour) avant d'être autorisés à se rendre à son bureau habituel. On pourra demander à des groupes spécifiques d'employés de se rendre sur ces sites à une date donnée uniquement, pour gérer un volume quotidien.

Ces "Sanity Checks Center" peuvent être des sites spécifiques par région/pays, un bâtiment dans un campus, ou simplement un étage dans un bâtiment. Ce serait un moyen efficace d'accueillir de manière sécurisée la vague de télétravailleurs « potentiellement compromis » entrant simultanément dans le réseau.

Forescout est la solution adéquate pour réduire drastiquement les **risques critiques** en peu de temps, mais cette solution fait sens pour le futur, car elle peut être vue comme le cœur d'un projet « Zero trust » détaillé plus loin dans le document.

Observation

- Manque de visibilité dans tout le réseau et les filiales
- Etant donné la précipitation de la décision de confinement, les utilisateurs n'ont pas été « éduqués » au télétravail (et aux bonnes pratiques de sécurité)
- Les utilisateurs distants ont le plus souvent des accès séparés qui permettent la navigation Internet hors des systèmes de sécurité périmétrique de l'entreprise => Navigation Internet avec un **niveau de sécurité** faible
- Certaines applications ne requièrent pas de connexion VPN, avec des postes qui ne sont donc pas forcés à se connecter à l'infrastructure, ce qui augmente les risques à cause de l'**absence** de :
  - Patch d'OS et d'Application
  - Mise-à-jour de GPO
  - Mise-à-jour d'AV



Actions

Forescout peut déclencher diverses actions. Pour les grandes entreprises, et étant donné le peu de temps imparti pour déployer, 3 options sont recommandées. Il peut s'agir d'une action unique ou d'un mix de ces actions, en fonction de critères diverses (Users, users VIP, sites, pays, type d'appareils, etc.).

Notification des admins et/ou des utilisateurs finaux
Les notifications peuvent prendre la forme d'un email envoyé à des administrateurs spécifiques, en fonction de la non-conformité. Les utilisateurs peuvent également être informés des critères non-conformes.

Remédiation automatique
Après avoir évalué la posture de sécurité (l'intégrité du poste), Forescout peut agir automatiquement par plusieurs actions de remédiation spécifiques :

- **Mises-à-jour spécifiques** : Si l'Antivirus n'est pas actif ou si les signatures ne sont pas à jour, Forescout peut déclencher la mise-à-jour de l'Antivirus.
- **Scan de vulnérabilité "à la demande"** : Associé à des outils de gestion de vulnérabilités comme Rapid7 par exemple, Forescout peut vérifier de quand date le dernier scan et en forcer un si l'ancienneté est supérieure à X jours.
- **Patching "à-la-demande"** : Si un patch obligatoire est manquant, Forescout peut forcer la mise-à-jour.

Isolation automatique de l'appareil
Forescout peut déplacer un appareil compromis dans un réseau « isolé ». Cet appareil aura un accès limité ou pas d'accès au reste du réseau tant qu'il ne sera pas conforme (vlan de quarantaine ou de remédiation).

Architecture

Pour exécuter ces actions, Forescout recommande 2 possibilités de déploiement, qui vont dépendre du temps, du budget et des ressources alloués :

Déploiement Global (Tous les sites)
Dès qu'un appareil atteint le réseau (où qu'il soit), une vérification de conformité sera effectuée, et des actions de quarantaine et/ou de remédiation seront effectuées si nécessaire.
Cette architecture offre la meilleure expérience utilisateur mais nécessite plus de prérequis et de temps pour être complètement opérationnelle.

Déploiement partiel : Action de « Device Sanity Check » dans des lieux spécifiques
Afin de gagner du temps et de réduire le nombre de sites à déployer, seuls certains sites sélectionnés constitueront le déploiement initial. Il sera demandé aux utilisateurs de se connecter la première fois depuis ces emplacements avant d'être autorisé à retourner dans leur emplacement habituel. Ces sites peuvent être virtuels comme un vlan de quarantaine, ou un emplacement physique spécifique.

Prérequis

Endpoint
Forescout peut travailler avec ou sans agent installé sur l'appareil. On peut avoir une combinaison de ces 2 options dans le réseau. Si Forescout dispose d'un identifiant d'administrateur vers un endpoint, pas besoin d'agent.

Réseau
L'accès en management aux appareils réseaux (switches, routeurs) sera nécessaire pour exécuter automatiquement l'isolation.

Moyen Terme : Politique Zero Trust

La plateforme Forescout permet aux organisations d'adopter une architecture Zero Trust pour tous les systèmes connectés en IP, qu'ils soient gérés ou non gérés, physiques ou virtuels, et à travers tout le réseau d'entreprise. La solution Zero Trust de Forescout offre entre autres les possibilités suivantes :

- Eliminer les risques en identifiant, comprenant et contrôlant les accès de tous les appareils, users, applications et workloads.
- Cartographier les flux de données pour concevoir les règles de segmentation puis les simuler pour un déploiement non disruptif
- Optimiser le retour sur investissement et étendre l'architecture Zero Trust au campus, au cloud, au data center et aux environnements OT/IOT en utilisant les technologies déjà présentes.

Scannez ce QR Code pour trouver plus d'informations sur l'approche Zero Trust de Forescout