FORESCOUT

Plateforme sans agent Device Visibility and Control

Les fonctionnalités fondamentales d'une cybersécurité efficace

> « La visibilité est primordiale pour protéger toutes nos ressources de valeur. Plus vous avez de la visibilité sur votre réseau à l'échelle de votre écosystème d'entreprise, plus vous avez de chances de détecter rapidement les signes révélateurs d'une compromission en cours et de la neutraliser[1]. »
>
> **— Chase Cunningham, analyste en chef, Forrester Research**

Plateforme Device Visibility and Control : pourquoi est-ce essentiel ?

La capacité de découvrir, classifier, évaluer et contrôler chacun des appareils qui se connectent à votre réseau est la condition sine qua non pour sécuriser vos systèmes et votre entreprise. Vous avez impérativement besoin de connaissances en temps réel sur tous les terminaux physiques et virtuels de l'ensemble des segments réseau, de renseignements granulaires sur l'état de configuration et de sécurité des appareils, ainsi que d'un contrôle d'accès automatisé, basé sur des politiques. Ces éléments sont indispensables pour une protection fiable des systèmes et des données, une intervention sur incident à la fois rapide et précise, la mise en conformité, la gestion des risques pour l'entreprise et l'infrastructure, ainsi que pour optimiser l'efficacité de la sécurité. Les auteurs d'attaques sont constamment à la recherche d'appareils non gérés et mal sécurisés ; ils finiront tôt ou tard par trouver et exploiter vos angles morts. La visibilité et le contrôle sont les pierres angulaires de la sécurité et de la conformité.

Et pourquoi est-ce difficile à obtenir ?

Auparavant, la gestion des terminaux du réseau s'effectuait en général au moyen d'un agent logiciel installé sur chacun des appareils. Cette méthode a été efficace tant que la plupart des terminaux étaient des serveurs ou postes de travail statiques appartenant à l'entreprise. Mais la mobilité, la diversification des types d'appareil et la virtualisation ont fortement compliqué la visibilité et le contrôle contextualisés. Dans les environnements d'entreprise actuels, les segments dédiés au cloud et au centre de données fourmillent de charges de travail provisionnées dynamiquement qui s'exécutent sur des machines virtuelles et sont connectées par des réseaux virtualisés. Quant aux segments de réseau de campus, ils foisonnent d'appareils BYOD personnels (ordinateurs portables, tablettes et autres smartphones) dépourvus d'agents de sécurité et d'appareils de l'Internet des objets (IoT) qui ne prennent pas ces agents en charge. Et enfin, les segments des technologies d'exploitation (OT) abritent une myriade d'appareils qui ne prennent pas en charge les agents, communiquent à l'aide protocoles propriétaires, gèrent des processus stratégiques et résistent très mal aux intrusions internes. Pour les services informatiques, il y a un besoin urgent d'une solution fonctionnant sans agent et capable de fournir une visibilité totale et un contrôle complet sur tous ces environnements hétérogènes.

La solution Forescout : la plateforme sans agent Device Visibility and Control

Forescout Technologies a mis au point une approche sans agent de la sécurité réseau pour résoudre les problèmes de visibilité et de contrôle sur les appareils dans les environnements actuels, à la fois hétéroclites et dynamiques. La plateforme Device Visibility and Control de Forescout offre une vue unifiée et continue de l'ensemble des appareils connectés à vos réseaux de campus, de centre de données, cloud et OT.

La fonction de découverte de la plateforme Forescout répertorie :

- Appareils sur les réseaux de campus — Ordinateurs portables, tablettes, smartphones, systèmes BYOD/invités et appareils IoT
- Infrastructure des centres de données — Machines virtuelles, hyperviseurs, serveurs physiques et composants réseau virtuels et physiques
- Infrastructure de cloud public et privé — Machines virtuelles AWS®, Microsoft® Azure® et VMware®
- Systèmes OT et de contrôle industriel (ICS) — Équipements médicaux, industriels et immotiques
- Infrastructure réseau physique et définie par logiciel — Commutateurs, routeurs, pare-feu, VPN, points d'accès sans fil et contrôleurs

Figure 1: Forescout offre une visibilité sur les appareils à l'échelle de l'entreprise étendue.

> « Les évaluations et la visibilité sur les niveaux de risque et de fiabilité, ajoutées à l'échange d'informations contextuelles, deviennent le système immunitaire de l'entreprise numérique[2]. »
> **— Neil MacDonald, vice-président, analyste, Gartner**

Les fonctions de notre plateforme

Forescout offre une multitude d'avantages aux départements informatiques, dont les suivants :

- Découverte de tous les appareils connectés à l'aide d'une adresse IP, qu'ils soient physiques ou virtuels, sur l'ensemble des réseaux : campus, centre de données, cloud et environnement industriel
- Classification des différents appareils IT, IoT et OT/ICS ainsi que les machines virtuelles (VM) et instances cloud, en temps réel, sur la base de leurs informations d'identification : type d'appareil, fonction, fournisseur, modèle, système d'exploitation et version
- Évaluation et surveillance en continu de l'état de sécurité des appareils pour s'assurer de leur conformité aux politiques
- Respect des politiques, des obligations sectorielles et des bonnes pratiques telles que la segmentation réseau
- Restriction d'accès, blocage ou mise en quarantaine pour les appareils non conformes ou compromis
- Automatisation des actions de contrôle des terminaux, des réseaux et des éléments tiers

Notre approche pour identifier l'ensemble des appareils connectés par adresse IP et des systèmes OT sur tous les segments

La plateforme Forescout offre plus de 20 techniques configurables de collecte d'informations qui bénéficient d'une étroite intégration avec une série de produits de premier plan : équipements réseau IT et OT — commutateurs, routeurs, points d'accès sans fil, pare-feu et concentrateurs VPN — et solutions de centre de données et de cloud. Elle surveille le trafic réseau par une écoute passive, analysant de nombreux flux de protocoles, et est capable d'interagir directement tant avec l'infrastructure réseau qu'avec les terminaux.

Voici un aperçu des techniques de visibilité de Forescout :

- **Méthodes de découverte passive sur le réseau et l'appareil**. Exemples : réception de traps SNMP à partir de commutateurs et de contrôleurs sans fil, surveillance d'un port SPAN combinée à l'analyse des flux de données de protocoles au sein du trafic (Forescout offre l'inspection approfondie des paquets pour plus de 100 protocoles IT et OT), collecte et analyse des données de flux, évaluation des requêtes DHCP et du trafic associé à l'agent utilisateur HTTP. Si l'authentification basée sur la norme 802.1X est mise en œuvre, Forescout peut surveiller un serveur RADIUS, qu'il soit intégré ou externe.
- **Méthodes de découverte active portant sur l'infrastructure réseau.** Forescout recourt entre autres à l'interrogation des commutateurs, concentrateurs VPN, contrôleurs sans fil et contrôleurs de cloud privé et public pour répertorier les machines virtuelles et les appareils connectés. Afin de recueillir des données sur les utilisateurs et les appareils, la plateforme Forescout interroge les services d'annuaire, les applications Web ou les bases de données externes.
- **Méthodes de découverte active portant sur l'appareil.** Il s'agit notamment de l'analyse des segments réseau à l'aide de NMAP en vue d'identifier les appareils connectés, de l'inspection à distance des appareils Windows avec WMI ou des appareils Mac et Linux avec SSH, et du profilage des terminaux au moyen de requêtes SNMP.

Techniques de visibilité sur les appareils

DÉCOUVERTE PASSIVE
Traps SNMP
Trafic SPAN
Requêtes DHCP
Agent utilisateur HTTP
Empreintes TCP
Analyse de protocoles DICOM (dispositifs d'imagerie médicale)
Analyse de protocoles ICS / OT (plus de 60 protocoles)
Analyse des flux
Flux NetFlow
Flexible NetFlow
IPFIX
sFlow
Requêtes DHCP (via l'IP helper)
Agent utilisateur HTTP (via redirection d'URL)
Requêtes RADIUS
Identificateur OUI de l'adresse MAC

DÉCOUVERTE ACTIVE DE L'INFRASTRUCTURE
Interrogation de l'infrastructure réseau physique
Intégration de l'infrastructure réseau basée sur le contrôleur
Meraki
Cisco ACI
Intégration (de l'infrastructure virtuelle) de cloud privé
VMware
Intégration de cloud public
AWS
Azure
Interrogation de services d'annuaires (LDAP)
Interrogation d'applications Web (REST)
Interrogation de bases de données externes (SQL)
Orchestrations (ITSM, UEM, EPP, EDR, VA)

DÉCOUVERTE ACTIVE DES APPAREILS
Inspection sans agent pour Windows (WMI, RPC, SMB)
Inspection sans agent pour macOS, Linux (SSH)
NMAP
Requêtes SNMP sur les terminaux
Inspection avec agent (SecureConnector)

Figure 2: Méthodes de visibilité sur les appareils Forescout.

Les avantages de la combinaison de diverses méthodes de visibilité

Le large éventail de méthodes de découverte proposé, qui plus est facile à configurer au moment de l'installation (et à modifier par la suite) : c'est notamment ce qui rend la plateforme Forescout exceptionnelle en termes de flexibilité et d'efficacité.

Des méthodes passives uniquement pour la découverte, la classification et l'évaluation dans les réseaux OT. Ces derniers sont généralement peu adaptés à l'emploi de techniques de sondage et d'analyse actives susceptibles de perturber les systèmes de contrôle des processus et le fonctionnement de l'entreprise. Une fois la compréhension de ces appareils approfondie, des méthodes actives peuvent être appliquées de façon sélective. La plateforme Forescout offre une visibilité sur les appareils des réseaux OT grâce à la combinaison de techniques entièrement passives de mise en miroir du trafic sur port SPAN et d'inspection approfondie des paquets sur près de 100 protocoles OT. Forescout prend en charge les protocoles standard tels que BACnet, CIP, DNP3, Ethernet/IP, ICCP, CEI 60870-5-104, CEI 60850, IEEE C37.118, Modbus/TCP, OPC, PROFINET et Siemens S7. Nous gérons également les protocoles propriétaires des principaux fabricants d'équipements, comme ABB, Emerson, GE, Honeywell, Rockwell/Allen-Bradley, Schneider Electric et Yokogawa.

Un déploiement économique dans les environnements de grande taille. L'usage de techniques de visibilité à distance contribue à réduire le coût global du déploiement en permettant de surveiller les sites de petite taille sans qu'une appliance en local soit nécessaire.

Au-delà de la découverte : la visibilité éclairée par la classification et l'évaluation. Comme elle peut combiner différentes techniques de profilage passives et actives, la plateforme Forescout offre bien plus que la simple identification des appareils qui se connectent à l'aide d'une adresse IP ou MAC. Elle met en œuvre deux processus. D'une part, la classification, qui consiste à collecter et mettre en corrélation de nombreuses couches de données contextuelles afin de créer un profil détaillé et pertinent de chaque appareil. D'autre part, l'évaluation, qui vérifie si les propriétés d'état mises au jour pour chaque appareil sont conformes à la politique de sécurité, afin d'orienter les décisions en matière de contrôle d'accès et de correction. Ces deux processus méritent que nous les analysions plus en profondeur.

Auto-classification intelligente

Des données contextuelles exhaustives sur chaque appareil sont essentielles à la création de politiques granulaires. Vous devez connaître le contexte ou l'objectif opérationnel de chaque appareil pour déterminer comment le protéger et le gérer de manière optimale. La multiplication et la diversification des appareils rendent presque impossible la collecte manuelle de ces données contextuelles, et la création de politiques sans contexte met en péril les opérations. Forescout classifie automatiquement les appareils traditionnels, IoT et OT à l'aide d'une taxonomie de classification multidimensionnelle permettant d'identifier la fonction et le type d'appareil, le système d'exploitation et la version, ainsi que le fabricant et le modèle.

Ainsi, la plateforme Forescout classifie automatiquement :

- Plus de 500 versions de système d'exploitation
- Plus de 5 000 produits et modèles de fabricants d'appareils
- Les équipements médicaux de plus de 350 fournisseurs de technologies médicales
- Des milliers d'appareils de contrôle et d'automatisation industriels utilisés dans divers secteurs (fabrication, énergie, pétrole et gaz, services publics, exploitation minière et autres infrastructures critiques)

Optimisée par **Forescout Device Cloud**, la fonctionnalité d'auto-classification de la plateforme bénéficie de cette précieuse source de données contextuelles pour s'adapter à la multiplication et à la diversification des appareils. Le programme Forescout Research and Intelligent Analytics exploite les données des quelque 8 millions d'appareils réels* répertoriés dans ce référentiel cloud et publie fréquemment de nouveaux profils afin d'améliorer l'efficacité, la couverture et la vitesse de la classification pour l'ensemble de vos appareils.

Évaluation du niveau de sécurité des appareils

La classification des appareils fournit un contexte opérationnel concernant l'objectif de chacun d'entre eux. Toutefois, pour obtenir des données contextuelles exhaustives, il est nécessaire d'adopter une autre approche afin d'évaluer le niveau de sécurité et d'intégrité de chaque appareil. Forescout surveille le réseau en continu et évalue la configuration, l'état et le niveau de sécurité des appareils connectés pour déterminer leur profil de risque et s'ils respectent les politiques de sécurité et de conformité réglementaire.

La plateforme répond à diverses questions cruciales, notamment :

- Les systèmes d'exploitation des appareils sont-ils approuvés et sont-ils dotés des correctifs les plus récents ?
- Un logiciel de sécurité est-il installé, opérationnel et à jour avec les derniers correctifs ?
- Certains appareils exécutent-ils des applications non autorisées ou enfreignent-ils les normes de configuration ?
- Certains appareils utilisent-ils des mots de passe faibles ou par défaut (ce qui est particulièrement dangereux pour les appareils IoT) ?
- Des appareils non approuvés ont-ils été détectés, notamment des équipements qui se font passer pour des appareils légitimes à l'aide de techniques d'usurpation ?
- Parmi les appareils connectés à votre réseau, lesquels sont les plus vulnérables aux dernières menaces ?

Classification et évaluation des appareils

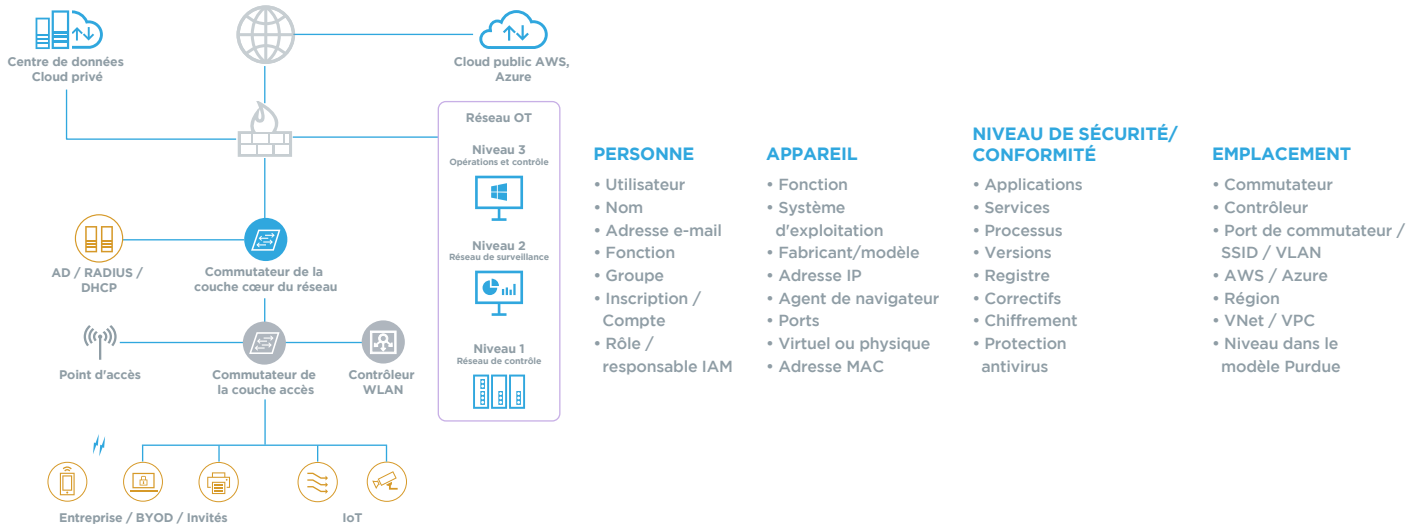

Figure 3: La plateforme Forescout classifie rapidement les appareils par type, précise s'il s'agit d'équipements gérés par l'entreprise ou non gérés, IoT ou OT, physiques ou virtuels, et vous aide à évaluer leur statut de conformité.

La visibilité au service du contrôle

La plateforme Forescout intègre un moteur de politiques qui vérifie en continu les appareils par rapport à un ensemble de politiques personnalisables, lesquelles dictent et régissent le comportement des appareils sur le réseau. Elle peut ainsi surveiller en continu et en temps réel jusqu'à deux millions d'équipements. Les politiques sont déclenchées en temps réel par des événements se produisant soit sur un appareil spécifique soit sur le réseau. Il peut s'agir d'événements d'admission sur le réseau, comme un branchement à un port de commutateur ou un changement d'adresse IP, ou d'événements d'authentification tels que ceux reçus par les serveurs RADIUS. Les politiques peuvent également être déclenchées par une modification des attributs d'appareil. La figure 4 montre l'éventail des actions de contrôle que peut exécuter la plateforme Forescout lors du déclenchement d'une politique.

Actions de contrôle de Forescout

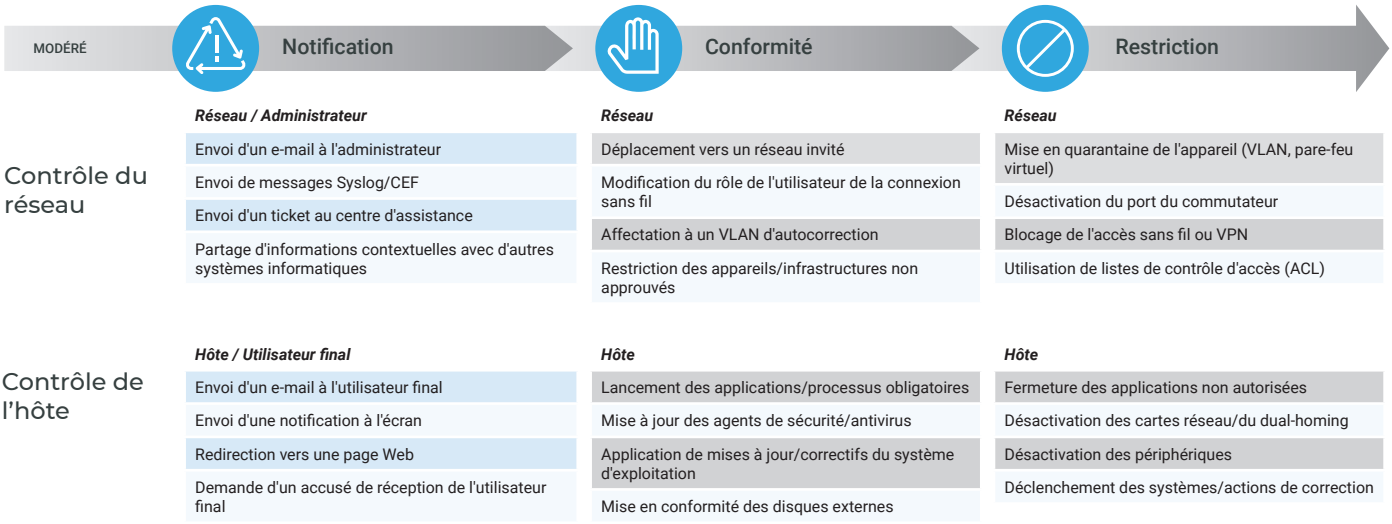

Figure 4: Les actions de contrôle personnalisables vous permettent d'appliquer le niveau de contrôle approprié (de modéré à rigoureux) en fonction de vos politiques de sécurité.

Le moteur de politiques recourt à deux ensembles de fonctions de contrôle : des fonctions natives de Forescout et des fonctions auxquelles il a accès grâce aux intégrations en matière d'échange de données et d'orchestration des contrôles entre la plateforme et les principaux produits de gestion de la sécurité et des ressources informatiques.

Fonctions de contrôle natives

Forescout propose en natif des contrôles au niveau du réseau et des contrôles au niveau de l'hôte. Les contrôles sur le réseau assurent la segmentation fondée sur les politiques, accordant ou refusant l'accès en fonction de l'état de l'appareil, de l'identité de l'utilisateur et de son rôle. Les contrôles sur l'hôte veillent à l'intégrité des appareils en régissant le démarrage et l'arrêt d'applications, la mise à jour des antivirus et autres agents de sécurité sur l'hôte ou la désactivation des périphériques. Le moteur de politiques applique automatiquement ces ensembles de règles à l'appareil, peu importe son emplacement et ses déplacements dans tout l'environnement – du réseau d'entreprise au centre de données et jusqu'au cloud.

Fonctions de contrôle étendues

La plateforme Forescout automatise la mise en œuvre des politiques, accélère la prise de mesures à l'échelle du système et limite les risques en assurant le partage en temps réel des données contextuelles sur les appareils et l'orchestration des workflows entre différents types de produits de gestion de la sécurité et des ressources informatiques. Forescout propose des intégrations avec les principaux fournisseurs de solutions de ces catégories :

- Détection des menaces avancées
- Outils de gestion clients
- Gestion de la mobilité en entreprise
- Protection des terminaux, détection et intervention sur incident
- Gestion des services informatiques
- Pare-feu de nouvelle génération
- Gestion des accès avec privilèges
- Gestion des événements et des informations de sécurité
- Gestion des vulnérabilités

Par le biais de ces intégrations, Forescout orchestre la sécurité à l'échelle de l'infrastructure, offrant des contrôles fondés sur des politiques et sur la classification des utilisateurs, des appareils, des applications et du trafic. La plateforme applique des politiques d'accès granulaires permettant un contrôle précis et flexible des ressources. Les départements informatiques peuvent ainsi implémenter une segmentation dynamique du réseau et créer des politiques de sécurité sensibles au contexte qui s'appuient sur la connaissance situationnelle en temps réel.

Les différentes actions de contrôle de la plateforme

Puisant dans une tradition bien ancrée dans le contrôle d'accès au réseau (NAC), Forescout propose une combinaison de fonctions de contrôle natives et étendues. Celles-ci confèrent à sa plateforme un ensemble impressionnant de capacités de contrôle des appareils, qui constituent pour les départements informatiques un puissant arsenal d'outils de sécurité réseau.

La plateforme Forescout contrôle l'accès au réseau pour les ressources de l'entreprise en fonction du profil de l'utilisateur (invité, employé, sous-traitant), de la classification de l'appareil et de son niveau de sécurité. Pour ce faire, elle :

- Met en place un accès différencié pour les appareils invités et BYOD
- Applique des politiques d'accès au réseau avec ou sans authentification basée sur la norme 802.1X
- Applique des mesures à l'encontre des appareils suspects, non approuvés ou relevant du Shadow IT qui sont connectés au réseau
- Restreint ou bloque l'accès au réseau pour les appareils compromis ou malveillants
- Met en quarantaine ou isole les appareils non conformes jusqu'à ce que les écarts de conformité aient été résolus

La plateforme Forescout améliore la conformité des appareils en automatisant les évaluations de conformité et en appliquant des contrôles de correction afin que les appareils soient en adéquation constante avec les politiques de sécurité internes, les normes externes et les réglementations sectorielles. Elle est notamment capable d'exécuter ces actions :

- Vérifier que les terminaux sont correctement configurés et appliquer des mesures correctives pour les violations de configuration critiques, comme l'usage de mots de passe faibles ou par défaut
- S'assurer que les applications et les agents de sécurité requis sont installés, en cours d'exécution et à jour
- Désactiver ou bloquer les applications non autorisées qui pourraient engendrer des risques, solliciter inutilement la bande passante du réseau ou peser sur la productivité des ressources
- Identifier les vulnérabilités à haut risque et les correctifs critiques manquants, puis prendre les mesures correctives adéquates
- Cibler de manière proactive les actions de correction nécessaires, telles que l'installation des logiciels de sécurité requis, la mise à jour des agents ou l'application de correctifs de sécurité
- Implémenter des politiques et automatiser des contrôles pour garantir la conformité des configurations dans les déploiements cloud, notamment AWS, Azure et VMware

La plateforme Forescout implémente une segmentation dynamique du réseau en appliquant des politiques de segmentation aux technologies de contrôle disparates dans votre entreprise étendue, grâce à un cadre de politiques commun. Ainsi, la plateforme :

- Attribue dynamiquement des appareils à des groupes de segmentation en se basant sur les propriétés, la classification et le niveau de sécurité des appareils
- Applique des contrôles de segmentation via des VLAN, des listes ACL, des WLAN et un marquage sur les réseaux de campus et OT
- Applique des contrôles de segmentation via des groupes/marqueurs de sécurité dans des environnements cloud publics et privés tels qu'AWS et VMware NSX®
- Place les appareils non conformes et vulnérables dans des zones de segmentation distinctes afin d'assurer la continuité des activités tout en réduisant votre surface d'attaque (en particulier les appareils auxquels il n'est possible d'appliquer des correctifs ou des mesures de correction qu'au cours des périodes de maintenance planifiées)
- Applique des politiques de segmentation pour isoler les appareils et les flux de données critiques du reste du réseau, comme l'exigent des réglementations telles que la loi HIPAA, la norme PCI et le programme CSP de SWIFT

La plateforme Forescout accélère l'intervention sur incident en assurant rapidité et efficacité lors de la neutralisation des menaces et de la résolution des incidents de sécurité, afin de limiter les interruptions d'activité et le préjudice causé à l'entreprise. Cette solution de visibilité et contrôle des équipements :

- Identifie les appareils à haut risque qui n'ont pas été isolés ou corrigés
- En collaboration avec des solutions de détection des menaces avancées, identifie les indicateurs de compromission sur les appareils dès qu'ils se connectent au réseau afin de réduire le délai moyen d'intervention
- Isole rapidement les appareils compromis ou malveillants pour éviter la propagation latérale de logiciels malveillants
- Automatise l'intervention sur incident et initie des flux de travail de correction sur les appareils compromis
- Réduit le délai moyen d'intervention en fournissant des données contextuelles précieuses sur les appareils (connexion, emplacement, classification et niveau de sécurité) aux équipes interfonctionnelles d'intervention sur incident et aux technologies isolées

La sécurité commence par la visibilité

Ce n'est pas sans raison si les chefs militaires cherchent toujours à occuper des positions surélevées ; être posté en hauteur permet en effet de voir de loin les forces ennemies s'approcher et donc d'organiser sa riposte avant qu'elles ne lancent l'attaque. La plateforme Forescout offre aux départements informatiques un poste d'observation de l'environnement réseau qu'ils doivent protéger. Poursuivant sans relâche la découverte, la classification, l'évaluation et le contrôle de tous les appareils, quel que soit l'endroit d'où ils se connectent, elle fait du champ de bataille de la cybersécurité un espace visible, intelligible et gérable.

Essayez par vous-même la plateforme Forescout

Le meilleur moyen de mieux comprendre les fonctionnalités de la plateforme sans agent Device Visibility and Control de Forescout est de les découvrir par soi-même. Pour en apprendre plus, vous avez diverses possibilités :

Participez à un Test Drive : Découvrez les avantages qu'offre l'implémentation de la plateforme Forescout grâce à une session d'évaluation pratique au cours de laquelle vous passerez en revue six scénarios d'utilisation.

Demandez votre rapport Forescout sur la visibilité absolue et les risques : Bénéficiez d'une évaluation approfondie de la visibilité sur les appareils et des risques connexes. Pour plus d'informations, contactez votre représentant Forescout local.

Demandez une démonstration : Rendez-vous sur le site de Forescout pour demander une démonstration personnelle de la plateforme et obtenir plus d'informations.

Utilisez l'outil de ROI / valeur métier de Forescout (en anglais) : Quantifiez, en seulement 10 minutes, la valeur ajoutée que la plateforme Forescout pourrait apporter à votre entreprise (calculée selon le modèle Business Value Model d'IDC).

* Au 31 mars 2019

1 The Zero Trust eXtended (ZTX) Ecosystem (L'écosystème Zero Trust eXtended), Forrester Research, janvier 2018

2 Zero Trust Is an Initial Step on the Roadmap to CARTA (Le modèle Zero Trust est un premier pas dans l'adoption de l'approche CARTA), Gartner, décembre 2018

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 (États-Unis)

Email info-france@forescout.com
Tél. (international) +1-408-213-3191
Support +1-708-237-6591

Pour en savoir plus, consultez le site Forescout.com