FORESCOUT

Visibilité totale : la clé de la sécurité Zero Trust

Forescout offre une plateforme de visibilité des appareils pour la sécurité Zero Trust

> « La visibilité est primordiale pour protéger tous nos actifs de valeur. Une bonne protection exige une parfaite visibilité. 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[3]. »

Ne faites confiance à personne

Ce n'est pas par hasard si le modèle de sécurité Zero Trust fait maintenant partie intégrante des stratégies des équipes de sécurité et des feuilles de route des développeurs de solutions de sécurité. Les architectures de sécurité axées sur le périmètre qui attribuent par défaut des niveaux de confiance élevés au réseau interne continuent d'échouer de manière désastreuse et coûteuse. Une analyse récente de l'Online Trust Alliance a révélé que le nombre de cyberincidents signalés par les entreprises avait presque doublé en 2017. En effet, au cours des trois premiers trimestres de 2017, les violations de données ont entraîné la divulgation de plus de 7 milliards d'enregistrements, soit quatre fois plus qu'en 2016[1]. Le Ponemon Institute estime le coût de chaque enregistrement volé à 141 dollars et le coût total moyen d'une violation de données à 3,62 millions de dollars[2].

Les multiples échecs de la sécurité basée sur le périmètre

Les environnements d'entreprise actuels sont extrêmement dépendants des services et des infrastructures cloud, ce qui entraîne la disparition du périmètre réseau. La mobilité des charges de travail, des données et du personnel nécessite une protection agile. Les utilisateurs exigent également des options d'accès supplémentaires à davantage de comptes, données et ressources. En parallèle, les solutions traditionnelles de gestion des terminaux sont dépassées par le volume et la diversité des appareils qui se connectent aux ressources réseau. Étant donné que bon nombre de ces appareils n'exécutent pas d'agents de gestion (appareils des visiteurs, systèmes BYOD, appareils IoT et technologies d'exploitation), il est possible que les équipes de sécurité ne parviennent pas à les détecter sur leurs réseaux. Dans ce cas, elles seront incapables d'identifier leurs utilisateurs, d'évaluer leur état de sécurité ou de contrôler leurs activités.

Ces défaillances systémiques de la sécurité basée sur le périmètre ont conduit les analystes de Forrester Research à développer le modèle Zero Trust comme alternative. Introduit en 2010, le modèle conceptuel et architectural Zero Trust décrit la manière dont les équipes de sécurité doivent segmenter les réseaux en micro-périmètres sécurisés ; renforcer la sécurité des données à l'aide de techniques de dissimulation ; réduire les risques associés aux privilèges utilisateur et aux accès excessifs ; ainsi qu'améliorer considérablement la détection des menaces et l'intervention sur incident grâce à l'analyse et à l'automatisation.

Zero Trust : d'un modèle conceptuel à un cadre complet

Au départ, le modèle Zero Trust se concentrait sur les concepts de segmentation protectrice et de contrôle d'accès selon le principe du moindre privilège. Il fournissait peu de directives spécifiques sur la manière dont les contrôles de sécurité existants pouvaient être exploités dans les implémentations pratiques. Au fil du temps, le modèle de base a évolué jusqu'à devenir ce que Forrester appelle l'écosystème Zero Trust eXtended (ZTX). Il s'agit d'un cadre complet qui associe des technologies de sécurité pertinentes à sept dimensions clés d'un environnement d'entreprise classique au sein duquel les principes Zero Trust s'appliquent : réseaux, données, utilisateurs, charges de travail, appareils, visibilité et analyse, et enfin automatisation et orchestration.

Le cadre ZTX aide les équipes de sécurité à comprendre comment procède une technologie pour :

- permettre l'isolation, la segmentation et la sécurisation des réseaux ;
- permettre la catégorisation, l'isolation, le chiffrement et le contrôle des données ;
- protéger les utilisateurs des ressources réseau et d'infrastructure, tout en protégeant ces ressources contre leurs utilisateurs ;
- protéger les piles applicatives des charges de travail dans les clouds publics et privés ;
- automatiser et orchestrer des contrôles et des processus Zero Trust dans les environnements hétérogènes ;
- fournir la visibilité et les fonctions d'analyse nécessaires pour éliminer les zones d'ombre et sécuriser l'environnement d'entreprise étendu dans ses moindres recoins.

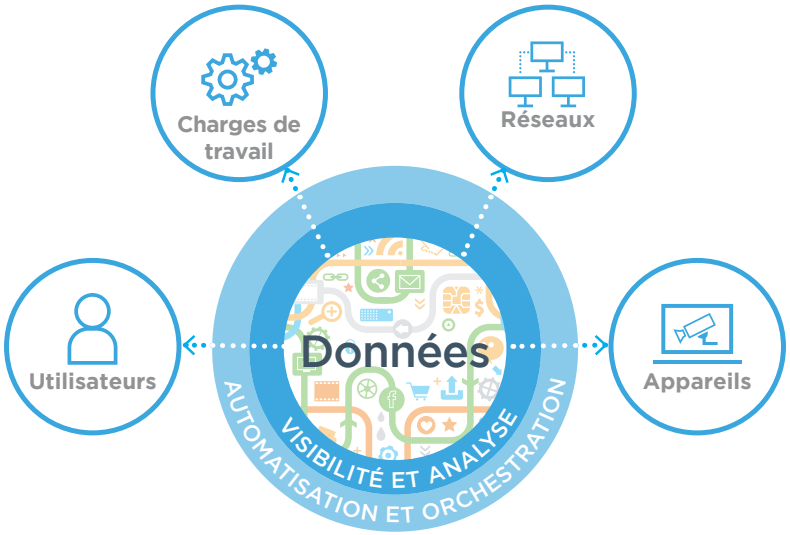

Figure 1. Les sept dimensions de l'écosystème Zero Trust eXtended de Forrester Research.

La plateforme idéale pour une visibilité optimale

Une stratégie Zero Trust peut avoir un double objectif, par exemple. D'une part, découvrir et classifier la totalité des appareils qui se connectent au réseau — et pas seulement ceux sur lesquels des agents de terminaux sont installés et opérationnels. D'autre part, appliquer une politique stricte de contrôle d'accès selon le principe du moindre privilège, basée sur une analyse granulaire de l'appareil, de l'identité et des autorisations de l'utilisateur, de la pile logicielle, de la conformité des configurations et de l'état de sécurité. Pour appliquer une politique restrictive de contrôle d'accès, il est nécessaire de visualiser, d'évaluer et de contrôler l'ensemble des éléments du réseau.

Forrester insiste sur l'importance de la visibilité pour la sécurité Zero Trust. Selon Chase Cunningham, analyste chez Forrester :

Une telle stratégie nécessite une solution complète de visibilité et de contrôle sur les appareils. Celle-ci doit être capable de visualiser et de contrôler des systèmes de tous types : appareils des visiteurs et BYOD, terminaux d'entreprise avec agents désactivés, appareils non approuvés, appareils IoT, commutateurs réseau et routeurs, systèmes d'usine et autres systèmes OT, et machines virtuelles dans les clouds publics. Une tâche impossible pour les dispositifs traditionnels de gestion des terminaux.

La plateforme Forescout : visibilité sur les appareils et contrôle des risques

Forescout illustre l'évolution des principales technologies réseau sur les plateformes Zero Trust. La plateforme Forescout est une solution de sécurité sans agent qui identifie et évalue de manière dynamique les terminaux dès leur connexion à votre réseau étendu, hétérogène et multicloud. Elle identifie rapidement l'utilisateur, le propriétaire, le système d'exploitation, la configuration de l'appareil, les logiciels, les services, l'état des correctifs et la présence d'agents de sécurité. Elle effectue ensuite des actions de correction, de contrôle et de surveillance continue sur ces appareils.

Forescout met en œuvre ces fonctionnalités sur les appareils d'entreprise gérés, les appareils des visiteurs non gérés, les serveurs physiques et virtuels, l'infrastructure réseau, les systèmes de contrôle industriels et les appareils IoT, sans nécessiter d'agent logiciel ni de connaissance préalable des appareils. La plateforme se déploie rapidement dans votre environnement existant et nécessite rarement des modifications d'infrastructure, des mises à niveau ou une reconfiguration des terminaux. Elle fonctionne en toute transparence dans les environnements physiques, virtuels et cloud hybrides.

La plateforme Forescout permet la découverte et la classification de la totalité des appareils IP, ainsi que l'évaluation continue sans agent des risques et du niveau de protection, afin de déterminer la connaissance situationnelle en temps réel de chaque appareil connecté. Elle s'appuie ensuite sur ces informations pour automatiser des contrôles basés sur des politiques et orchestrer des actions sur les appareils. Ces fonctionnalités sont la base d'une sécurité Zero Trust efficace.

Forrester a désigné Forescout parmi les leaders dans son rapport relatif aux fournisseurs de l'écosystème Zero Trust eXtended. Selon le bureau d'études, Forescout propose des fonctionnalités de pointe dans cinq catégories de composants Zero Trust[4].

Visibilité, analyse et contrôle des appareils Zero Trust

Découverte sans agent de tous les appareils — La plateforme Forescout emploie une combinaison de méthodes actives et passives sans agent pour découvrir l'ensemble des appareils sur le réseau étendu et hétérogène d'une entreprise, du campus et du centre de données au cloud en passant par les réseaux OT. Elle détecte les ordinateurs portables et de bureau, les serveurs physiques et virtuels, les appareils mobiles et IoT, les instances cloud et les systèmes de technologies d'exploitation, sans nécessiter d'équipement réseau spécifique au fournisseur, de mise à niveau de l'infrastructure existante ni de reconfiguration des commutateurs ou des ports de commutateur, avec ou sans authentification 802.1X.

Figure 2. Forescout offre une plateforme de visibilité et de contrôle des appareils pour l'entreprise étendue.

De la découverte des appareils aux informations sur les actifs — Les différentes techniques de découverte et de profilage employées par Forescout produisent rapidement d'importants volumes d'informations concernant l'identité, l'état et le comportement des appareils, et les actualisent en permanence. La couche d'abstraction adaptative de la plateforme ingère des milliards de paquets de données brutes provenant d'un large éventail de systèmes réseau hétérogènes. Elle met en corrélation et consolide ces données afin de créer une vue unifiée de l'ensemble des appareils et de fournir des informations granulaires détaillées sur chaque appareil. La couche d'abstraction s'adapte et évolue avec l'environnement IT. Elle enrichit en permanence la vue des appareils à mesure que de nouvelles sources de données sont disponibles. Ses données offrent une vue détaillée de tous les actifs dans l'environnement. Elles vous permettent de prendre des décisions et d'appliquer des actions et servent de point de départ aux contrôles de réduction des risques.

En outre, la plateforme Forescout permet la surveillance et la visualisation des communications entre les appareils et les sources de données, ainsi que les interdépendances entre les systèmes. Ce point est particulièrement important pour le mappage de segmentation, la planification et la création de politiques.

The Forescout platform allows monitoring and visualization of communications between devices and data sources as well as system interdependencies. This is particularly important for segmentation mapping, planning and policy creation.

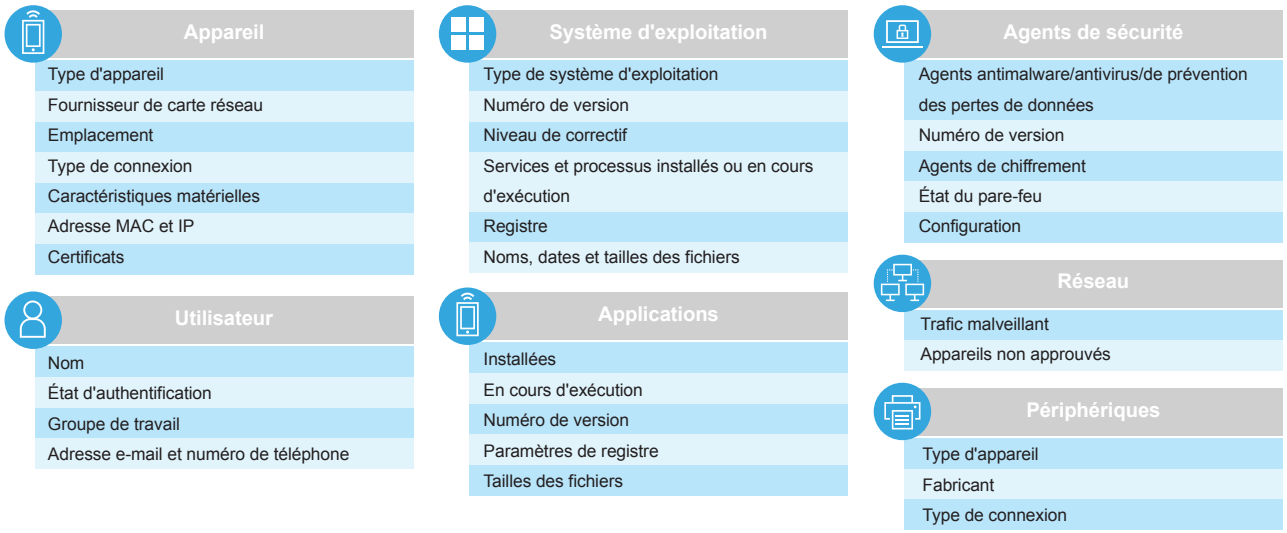

Figure 3. Le processus de classification Forescout extrait des données détaillées sur tous les appareils IP.

Visibilité et contrôle continus sur les appareils basés sur des politiques — Le moteur de politiques en temps réel de la plateforme Forescout s'appuie sur ces informations sur les actifs pour évaluer en continu les appareils par rapport aux politiques qui régissent le comportement attendu. Il déclenche des politiques en temps réel en fonction de l'admission sur le réseau d'un appareil, de son authentification et d'autres attributs personnalisables. Par exemple, la plateforme Forescout est capable d'identifier un nouvel appareil IoT sans accès Internet sortant et de l'affecter automatiquement à un segment de réseau à accès restreint. Elle permet de détecter les changements de l'état de sécurité d'un appareil, par exemple les agents antivirus ou les logiciels de chiffrement qui ont été désactivés ou qui ne fonctionnent plus. La plateforme réévalue les appareils tant qu'ils sont sur le réseau et à chaque fois qu'ils s'y connectent ou s'en déconnectent. Elle partage des informations contextuelles en temps réel sur les appareils et déclenche des actions d'évaluation du niveau de protection, telles que la nouvelle analyse des appareils à la recherche de vulnérabilités et d'indicateurs de compromission, conjointement avec des systèmes tiers.

Forescout peut exécuter des actions de contrôle directement sur l'appareil ou sur l'infrastructure réseau (voir ci-dessous). Les contrôles au niveau de l'hôte comprennent le démarrage et l'arrêt d'applications, la mise à jour d'agents de sécurité antivirus, la désactivation de périphériques et la demande d'un accusé de réception de l'utilisateur final. Le moteur de politiques applique ces politiques automatiquement, quel que soit l'emplacement de l'appareil. Si nécessaire, la plateforme Forescout peut automatiser des actions de correction, telles que l'application de correctifs ou la réinstallation de logiciels d'évaluation des vulnérabilités, de protection des terminaux, de chiffrement ou d'autres logiciels de sécurité, par le biais de l'orchestration avec des outils tiers (voir ci-dessous).

Informations personnalisables sur les appareils pour les opérations de sécurité et l'intervention sur incident — Les équipes des opérations de sécurité nécessitent une vue complète des appareils connectés et de leur classification, caractéristiques de connexion et contexte de conformité. Dans le cas contraire, l'intervention sur incident et la génération de rapports de conformité s'en trouvent entravées. Outre la console, la plateforme Forescout intègre désormais un tableau de bord Web personnalisable qui fournit une vue consolidée de vos appareils et de l'état de conformité à l'échelle de l'entreprise étendue. Le tableau de bord fonctionne conjointement avec Forescout eyeManage pour fournir des renseignements sur les divers types d'appareils connectés à votre réseau hétérogène.

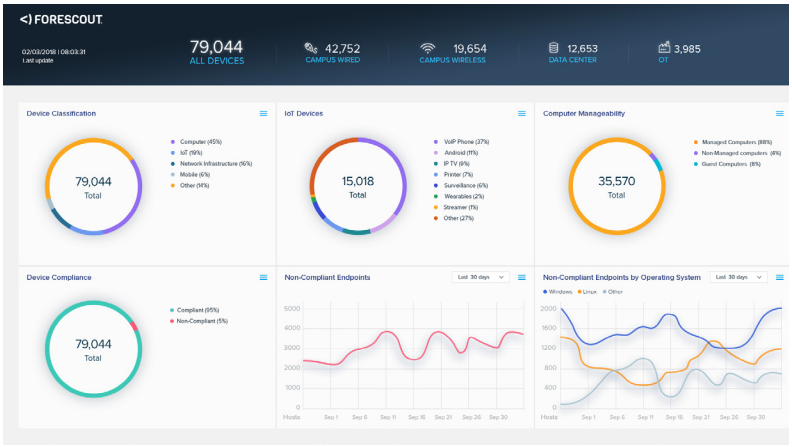

Figure 4. Vue consolidée des appareils pour les SOC.

Zero Trust pour les réseaux

Broker d'accès Zero Trust — La plateforme Forescout exécute des actions de contrôle des appareils au sein de l'infrastructure réseau. Elle offre un service de brokerage centralisé et permet de configurer les accès réseau grâce à sa vue intégrée de l'identité de l'utilisateur, de son rôle, de son authentification et de l'état de l'appareil. Elle s'intègre de façon native avec les produits de plus de 30 fournisseurs de contrôleurs sans fil et de commutateurs, et permet une intégration directe avec les routeurs qui exécutent le système d'exploitation Linux. En fonction du fournisseur, différentes méthodes sont utilisées seules ou conjointement, notamment les traps SNMP, l'interface de ligne de commande et le protocole NETCONF. Au niveau d'un commutateur réseau, cette technologie peut changer l'affectation d'un VLAN, ajouter une liste de contrôle d'accès (ACL) ou désactiver un port de commutateur. Au niveau d'un contrôleur sans fil, elle peut mettre une adresse MAC sur liste noire ou modifier le rôle d'un utilisateur. En outre, notre technologie est capable de restreindre des utilisateurs VPN distants.

En cas d'implémentation réelle du modèle Zero Trust, la plateforme Forescout sans agent permet de découvrir, d'évaluer et de configurer l'accès à n'importe quel appareil IP ancien. Forescout visualise et contrôle la totalité des appareils IP et s'intègre avec toutes les infrastructures réseau IT et OT, sans exception.

En cas d'implémentation réelle du modèle Zero Trust, la plateforme Forescout sans agent permet de découvrir, d'évaluer et de configurer l'accès à n'importe quel appareil IP ancien.

Grâce à l'acquisition de SecurityMatters, Forescout étend également sa connaissance situationnelle basée sur le réseau au-delà de l'IT, dans les environnements des technologies d'exploitation (OT) et des systèmes de contrôle industriels (ICS). Les fonctionnalités combinées incluent désormais la capture et l'inspection approfondies des paquets de plus de 100 protocoles IT/OT, le mappage du réseau, l'analyse des flux, la surveillance des politiques et des comportements, l'investigation du réseau, l'évaluation des menaces et l'attribution de notes de risque.

Segmentation dynamique du réseau — Forescout est également compatible avec les pare-feux de nouvelle génération, afin que vous puissiez prendre des décisions et appliquer une segmentation dynamique basée sur des politiques. Les pare-feux de nouvelle génération offrent un contrôle sur le réseau basé sur la classification des utilisateurs, des appareils, des applications et du trafic. Ils s'appuient sur les informations contextuelles sur les utilisateurs et les appareils issues de diverses sources, dont la plateforme Forescout, pour appliquer 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 au sein de leurs pare-feux de nouvelle génération, en s'appuyant sur les données contextuelles des terminaux fournies par Forescout.

Automatisation et orchestration Zero Trust

La plateforme Forescout orchestre la gestion de la sécurité à l'échelle de l'infrastructure afin que les produits de sécurité auparavant disjoints travaillent à l'unisson. Son ensemble unique de technologies d'interopérabilité réseau, de sécurité et de gestion est étendu via les produits Forescout eyeExtend au moyen d'API qui permettent l'intégration avec plus de 70 produits tiers de gestion de la sécurité et des ressources informatiques*. Cela permet au système combiné d'accélérer l'intervention sur incident, d'améliorer l'efficacité opérationnelle et de renforcer la sécurité.

Forescout permet l'automatisation et l'orchestration de la sécurité de trois manières :

- **Partage en temps réel d'informations contextuelles —** Forescout surveille en continu et partage dynamiquement les informations concernant l'identité, la configuration et la sécurité des terminaux avec les autres systèmes de sécurité et de gestion que vous possédez et utilisez. Cet échange de données bidirectionnel s'ajoute aux propriétés globales qui peuvent être appliquées aux moteurs de règles d'autres outils afin d'optimiser les politiques et les actions.
- **Automatisation des flux de travail —** Forescout permet aux systèmes de partager des décisions basées sur des politiques qui nécessitaient jusque-là une analyse et une application manuelle sur tous les systèmes. L'automatisation de ces flux de travail et de ces processus permet une intervention coordonnée et instantanée.
- **Automatisation des actions d'intervention —** De nombreux produits de sécurité, tels que les systèmes de détection des menaces avancées, les SIEM et les outils d'évaluation des vulnérabilités, peuvent signaler des problèmes de sécurité au personnel informatique. Forescout exploite instantanément ces informations de sécurité pour déclencher une réponse automatisée et applique son large éventail de contrôles basés sur des politiques, tels que l'isolation de l'appareil et la correction du terminal afin d'éliminer les menaces.

Zero Trust pour les charges de travail

La plateforme Forescout découvre, classifie et profile les serveurs physiques et virtuels dans les environnements de centre de données/cloud hybrides, en exploitant différents composants d'infrastructure et les charges de travail elles-mêmes. En outre, la plateforme Forescout suit et surveille les variations des charges de travail au sein de l'environnement de centre de données/cloud hybride, ce qui évite toute faille de visibilité potentielle. Forescout collecte des propriétés cloud ou d'hyperviseur de niveau inférieur à partir des applications installées/en cours d'exécution sur les charges de travail, puis utilise ces données contextuelles pour garantir que seuls les utilisateurs et les appareils autorisés peuvent accéder à des charges de travail spécifiques, conformément aux politiques Zero Trust.

Zero Trust pour les utilisateurs

La plateforme Forescout s'intègre avec les principaux systèmes d'annuaire et d'identité pour collecter les informations disponibles sur les utilisateurs, notamment leur rôle et leurs autorisations d'accès aux ressources. Elle met en corrélation ces informations avec les données découvertes sur la configuration des appareils, leur état de sécurité et leur conformité, ce qui vous permet de prendre des décisions concernant l'accès aux ressources basées sur les données relatives aux appareils et aux utilisateurs. Le comportement des utilisateurs est surveillé en permanence et l'intégration avec les systèmes de gestion des accès à privilèges permet de découvrir les comptes d'utilisateur aux autorisations non conformes.

Zero Trust pour les données

Forescout prend en charge la sécurité des données sur tous les appareils IP en offrant une visibilité sur la présence et l'état opérationnel des logiciels de chiffrement, de dissimulation et de sécurité des informations requis par les politiques. Si de telles applications sont manquantes ou inactives, Forescout peut exécuter des actions basées sur des politiques, par exemple alerter l'utilisateur, notifier un administrateur ou mettre l'appareil en quarantaine jusqu'à sa correction.

La sécurité Zero Trust nécessite une visibilité totale sur les appareils

Pour en savoir plus sur la plateforme Forescout, diverses possibilités s'offrent à vous :

- **Testez notre plateforme :** 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 cinq scénarios d'utilisation.
- **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 (page 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).
- **Faites appel à nos services de conseil (page en anglais) :** Vous êtes en train de concevoir votre environnement selon le modèle Zero Trust ? Les consultants Forescout sont formés, expérimentés et certifiés pour l'implémentation de produits, le développement de processus et l'intégration de systèmes, ainsi que pour l'accès au réseau et la conformité des terminaux.

* Au 31 décembre 2018

*Notes

1. Online Trust Alliance, « Cyber Incident and Breach Trends Report » (Rapport sur les tendances en matière de cyberincidents et de compromissions), janvier 2018
2. Ponemon Institute, « 2017 Cost of Data Breach Study » (Étude 2017 sur le coût des violations de données), juin 2017
3. Forrester Research, « The Zero Trust eXtended (ZTX) Ecosystem » (L'écosystème Zero Trust eXtended), janvier 2018
4. Forrester Research, « The Zero Trust eXtended Ecosystem Road Map: The Zero Trust Security Playbook » (Feuille de route de l'écosystème Zero Trust eXtended : guide de la sécurité Zero Trust), 11 juillet 2019

FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
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