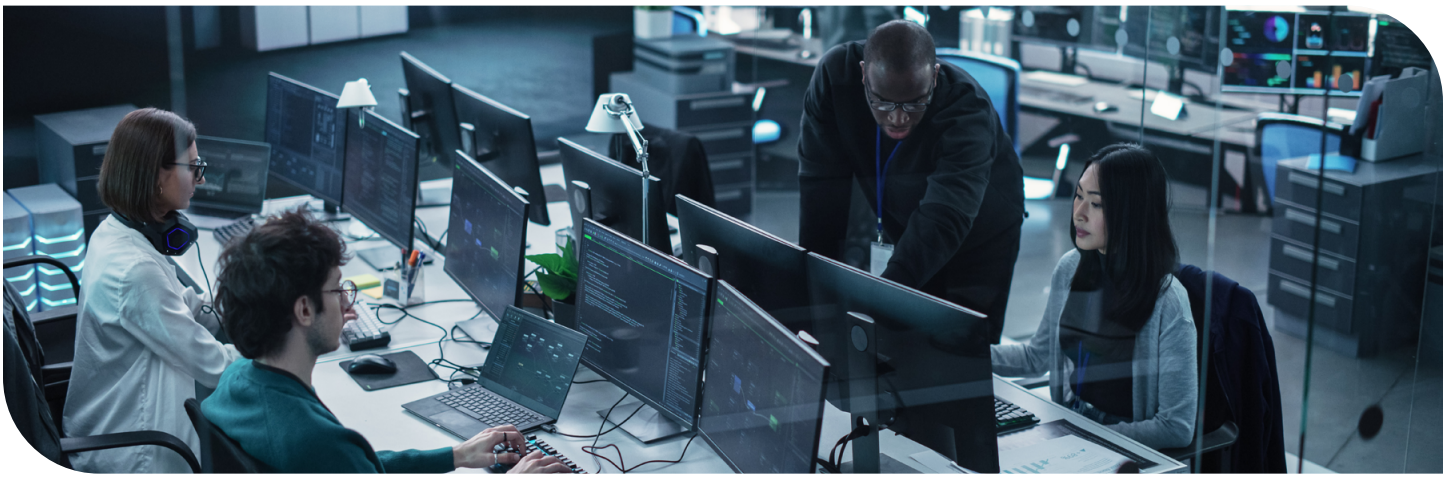
Gestion des risques et de l'exposition

Identifiez, quantifiez et priorisez les risques et la conformité



« Les intrusions sont rarement le fait d'attaques sophistiquées impliquant des États nations ou des modes d'action complexes. Elles sont le plus souvent un enchaînement de procédures simples que l'on peut prévenir en appliquant des fondamentaux de sécurité tels que la gestion des risques de vulnérabilité. »

Forrester Research, *The State of Vulnerability Risk Management, mars 2023*

L'essor du Shadow IT, les environnements de travail hybrides et l'adoption du cloud ne cessent d'accroître la surface d'attaque, à un rythme tel que les équipes réseau et de sécurité, censées protéger les entreprises et leurs précieux actifs numériques, ont du mal à suivre. Des technologies obsolètes, des vulnérabilités sans correctif et autres actifs informatiques de « moindre valeur » sont souvent oubliés, mais n'en constituent pas moins des cibles faciles. Les malfaiteurs profitent de ces points faibles pour s'infiltrer sur le réseau et se frayer un chemin vers des actifs plus importants. Une dépendance excessive à l'égard d'outils de sécurité réactifs, qui alertent lorsque des menaces ou des infractions sont déjà survenues, peut entraîner des temps d'arrêt qui auraient pu être évités avec des contrôles de sécurité proactifs.

Les entreprises ont besoin d'un meilleur moyen de comprendre l'état de leur surface d'attaque et de concevoir des processus de sécurité sans impact sur l'activité ni frictions du côté des utilisateurs. Il leur faut des outils permettant de prioriser la gestion des actifs et des risques de manière proactive, tout en fournissant le contexte nécessaire à la résolution d'incidents.

Réduction prouvée du niveau de risque

- Gestion rationalisée des actifs de cybersécurité
- Renseignements exhaustifs sur les risques des actifs
- Évaluation claire et concise de l'exposition des actifs
- Intervention sur incident plus rapide
- Conception de politiques de sécurité proactives
- Meilleure protection des appareils IoT et médicaux

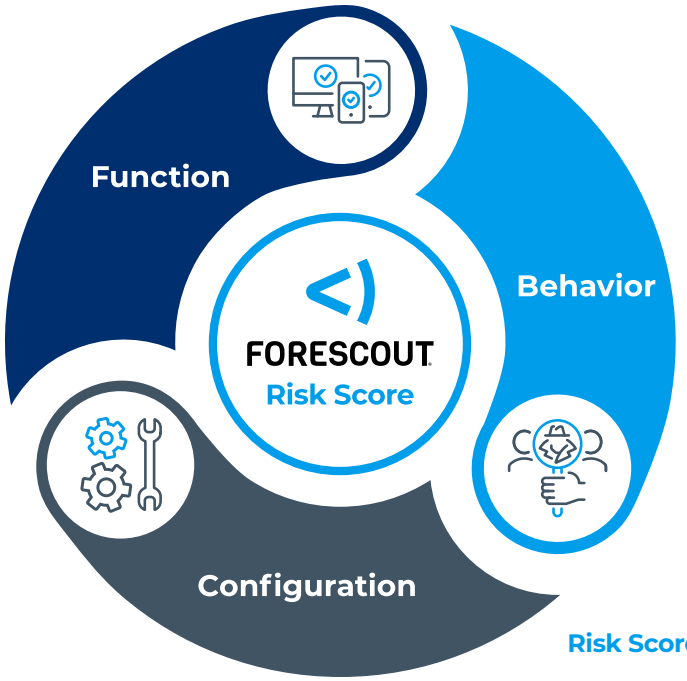
Améliorez le niveau de sécurité de votre réseau grâce à la priorisation basée sur les risques

Pour les équipes de cybersécurité dépassées par l'expansion de leur surface d'attaque et qui peinent à contextualiser les informations provenant d'outils de sécurité cloisonnés, Risk and Exposure Management de Forescout est un outil complet de renseignement sur les actifs, qui permet de bien comprendre le niveau de sécurité. La solution contrôle l'efficacité des mesures d'intervention prises dans l'ensemble de l'écosystème de sécurité afin de réduire les risques et l'exposition. Pour ce faire, elle s'appuie sur une approche automatisée basée sur le risque qui permet d'éliminer les vulnérabilités.

Au-delà de la simple visibilité, la solution Forescout® Risk & Exposure Management permet aux entreprises de comprendre les risques et ainsi de :

- réduire la charge opérationnelle liée à la gestion des actifs de cybersécurité ;
- atteindre un niveau d'intégrité inédit en matière de cybersécurité en identifiant l'exposition de la surface d'attaque ;
- évaluer, classer et quantifier avec précision la gravité des risques et l'exploitabilité de chaque appareil connecté d'après sa configuration et son état ;
- justifier les investissements existants en matière de sécurité et suivre l'efficacité des actions de contrôle afin de réduire les risques au fil du temps ;
- accélérer l'examen des incidents et concevoir des politiques d'intervention proactives pour prévenir les incidents futurs.

- **Configuration:**
  - Vulnerabilities (CVE's)
  - Exploitability (EPSS)
  - Exposed Services
- **Function:**
  - Device Criticality
- **Behavior:**
  - Internet Exposure



$$\text{Risk Score} = f\left(\text{Detected Risk Indicators}, \text{Device Criticality}\right)$$

Données persistantes sur les actifs et priorisation des risques de cybersécurité

Forescout Risk & Exposure Management vous aide à identifier, quantifier et prioriser les risques en fonction des vulnérabilités et des mauvaises configurations. Un score de risque multifacteur unique met ainsi en corrélation les facteurs relatifs à la configuration, à la fonction et au comportement de chaque actif.

Identifier

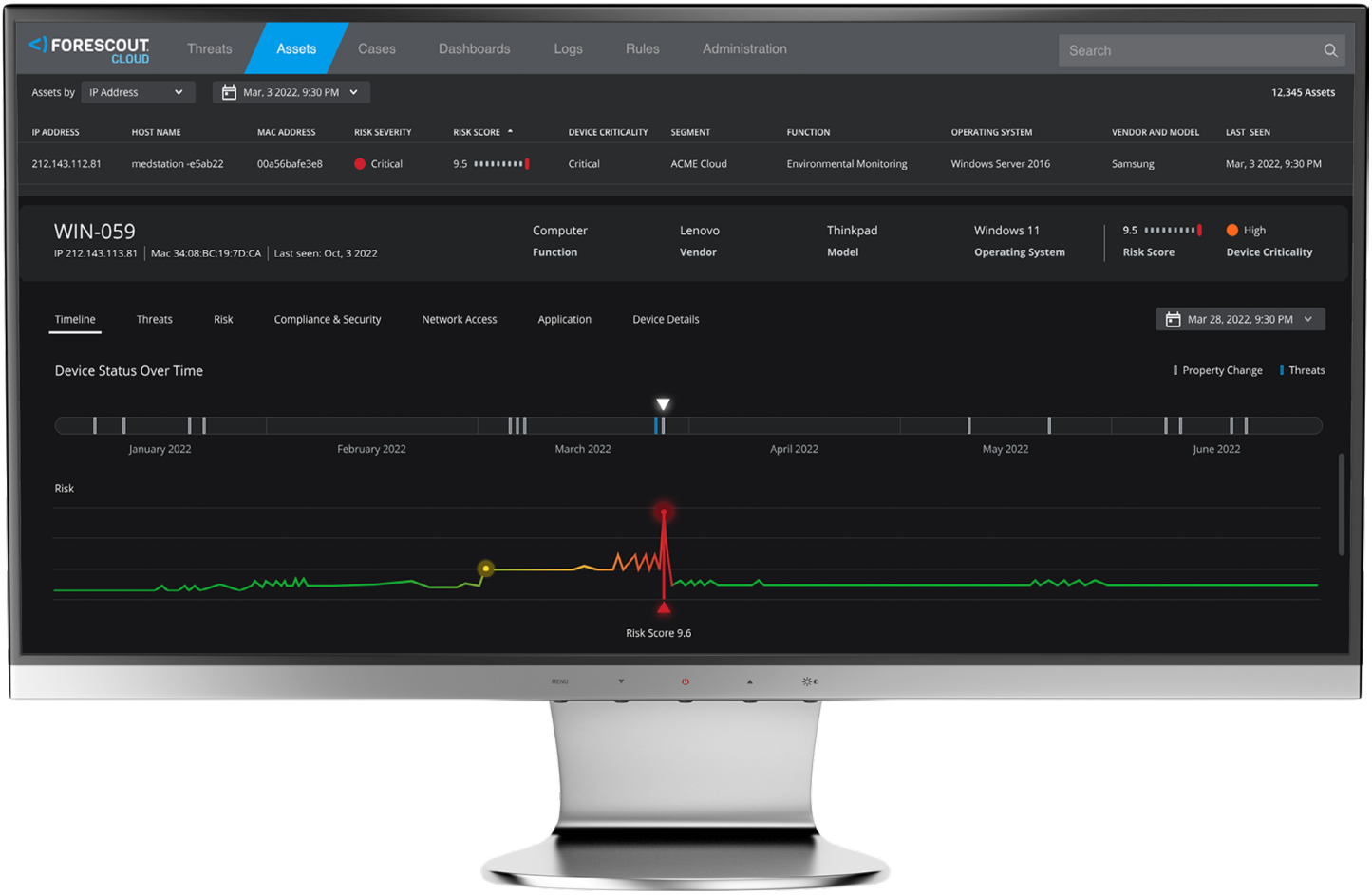
Une gestion des actifs de cybersécurité rationalisée grâce à des renseignements clairs et concis sur chaque appareil connecté

Établissez un inventaire durable et précis de vos actifs avec historique de l'état des appareils et des modifications de la configuration grâce à la classification cloud des appareils gérés et non gérés (IT, IoT, IoMT, OT/ICS).

Inventorisation de la surface d'attaque – classification haute fidélité, basée sur le cloud, des appareils gérés et non gérés.

Données contextuelles persistantes sur les actifs – consultables ; conservation pendant 90 jours et suivi de données contextuelles riches sur les actifs, dont l'état et les modifications de configuration.

Filtrage des profils d'exposition – fonctionnalités de filtrage avancées pour faciliter la localisation et le suivi des actifs ayant des caractéristiques de vulnérabilité communes avec les appareils compromis afin de remédier aux problèmes de manière proactive.



Pourquoi Forescout ?

1. Inventaire persistant de tous les types d'appareils sur une interface moderne
2. Score de risque multifacteur unique basé sur la configuration, la fonction et le comportement
3. Classification cloud haute fidélité
4. Technologie brevetée d'inspection approfondie des paquets
5. Corrélation de l'exploitabilité des vulnérabilités et de l'exposition des actifs
6. Intégration aux produits de sécurité leaders et possibilité de contrôler l'efficacité
7. Informations directement exploitables sur les risques et l'exposition
8. Lac de données cloud contenant des informations sur les risques et menaces

Rendez-vous sur www.forescout.fr pour en savoir plus sur l'approche de Forescout en matière de gestion des risques et de l'exposition et demander une démonstration.

Quantifier

Des renseignements exhaustifs sur les risques de cybersécurité

Suivez en continu le niveau de cyberrisque de tous les appareils connectés en calculant un score de risque multifacteur basé sur la configuration, la fonction et le comportement, et protégez ainsi votre réseau de manière proactive.

Configuration – saisissez les exigences de configuration uniques de chaque actif pour identifier son exposition et l'exploitabilité de ses vulnérabilités, notamment :

- les vulnérabilités et expositions courantes, ou CVE, corrélées au catalogue CISA des vulnérabilités exploitées connues (KEV) ;
- le système EPSS (Exploit Prediction Scoring System) ;
- les services exposés et les ports ouverts, ainsi que leur exposition potentielle (contrôle et accès) ;

Fonction – déterminez et évaluez le niveau de criticité des appareils selon leur fonction et leur utilisation.

Comportement – suivez les modifications de la configuration et du comportement de chaque actif afin de déceler des anomalies susceptibles d'augmenter le risque de compromission, notamment depuis Internet.

Prioriser

Examen plus rapide des incidents et conception de politiques de correction proactives

Facilitez l'accès des équipes informatique et de sécurité à des données en temps réel et persistantes sur les actifs pour les aider à examiner les incidents et à remédier aux risques de manière proactive.

Renseignements sur les actifs accessibles partout – le portail Forescout Cloud offre à toutes les équipes informatique et de sécurité une meilleure disponibilité et un accès facilité à des données contextuelles riches sur les actifs.

Priorisation basée sur les risques – associez les caractéristiques de risque et d'exposition aux renseignements sur l'état de configuration et de conformité des appareils pour faciliter l'examen des incidents et la conception de mesures correctives.

Contexte historique des actifs – accélérez l'analyse des risques et l'intervention sur incident afin de limiter l'impact global et de réduire le délai moyen d'intervention (MTTR).

Forescout Technologies, Inc.
Numéro gratuit (US)
1-866-377-8771
Tél. (intl) +1-408-213-3191
Support +1-708-237-6591
Plus d'infos sur Forescout.com