FORESCOUT
Active Defense for the Enterprise of Things™

Approche moderne du contrôle d'accès au réseau

Pourquoi la visibilité et le contrôle sur les appareils sont-ils essentiels à une cybersécurité efficace ?

Visibilité et contrôle sur les appareils : 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 bénéficier d'une **sécurité Zero Trust**. 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 le niveau de sécurité des appareils, ainsi que d'une correction et d'un contrôle d'accès automatisés, basés sur des politiques. Ces éléments sont indispensables pour une protection fiable des systèmes et des données ainsi qu'une intervention sur incident à la fois rapide et précise.

100%
VISIBILITÉ EN TEMPS RÉEL

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 zones d'ombre. La visibilité et le contrôle sans agent sont les pierres angulaires de la sécurité et de la conformité. Ils jouent également un rôle important dans la résolution de nombreux défis opérationnels. Ainsi, grâce à une visibilité continue en profondeur sur les appareils, il est possible de réaliser un **inventaire précis des actifs en temps réel** qui permet aux équipes informatiques et de sécurité de réduire les coûts opérationnels tout en facilitant la mise en conformité réglementaire et la réussite des audits.

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'appareils et la virtualisation ont fortement compliqué la visibilité et le contrôle contextualisés.

La multiplication et la diversification des équipements ont bouleversé le paysage des appareils. Les systèmes cyberphysiques, tels que les appareils de l'Internet des objets (IoT) et les systèmes des technologies d'exploitation (OT) se connectent désormais au réseau d'entreprise. De nombreux employés travaillent depuis leur domicile, et certains se connectent au cloud. L'entreprise moderne s'est rapidement transformée en **environnement EoT**, et la plupart de ces objets ne prennent pas en charge les agents de gestion. Même pour ceux qui en sont capables, une approche de gestion par agent est problématique :

- Les systèmes avec agent ne fonctionnent pas si des agents sont désactivés, défectueux ou manquants.
- Les méthodes basées sur les agents et l'authentification 802.1X génèrent des zones d'ombre sur le réseau et compliquent les opérations, ce qui se traduit souvent par des déploiements incomplets.
- Les outils de gestion de la conformité des appareils sont généralement isolés et ne proposent pas de vue unifiée de l'environnement, ce qui perpétue la présence de zones d'ombre.
- Sur de nombreux réseaux, les appareils non gérés sont plus nombreux que les appareils gérés, et ils ne permettent pas une authentification au moyen des méthodes traditionnelles.
- Lorsque les employés utilisent des appareils mobiles, BOYD, invités ou de télétravail, la sécurité avec agent devient fastidieuse et inefficace.
- Les réseaux multifournisseurs sont monnaie courante et nécessitent des alternatives à la norme 802.1X qui n'exigent pas de mises à niveau logicielles ou matérielles.

> **Les outils NAC d'aujourd'hui sont conçus pour repérer les appareils et les entités non approuvés (utilisateurs, segments, périphériques, etc.), et les empêcher d'entrer en contact avec le réseau.**
> **Grâce à ces toutes nouvelles technologies, proposées par des fournisseurs tels que Forescout, vous pouvez interdire aux éléments inconnus et probablement non corrigés d'accéder à vos réseaux de type Zero Trust [1].**
>
> **DR. CHASE CUNNINGHAM**
> **ANALYSTE EN CHEF, FORRESTER RESEARCH**

La solution NAC moderne de Forescout

Forescout Technologies a mis au point une approche sans agent du contrôle d'accès au réseau (NAC) pour résoudre les problèmes liés aux environnements actuels, à la fois hétéroclites et dynamiques.

La plateforme Forescout offre une vue unifiée et continue sur l'ensemble des appareils connectés à vos réseaux de campus, de centre de données, cloud et OT. Elle vous donne une visibilité granulaire sur :

- 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 autres 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-feux, VPN, points d'accès sans fil et contrôleurs

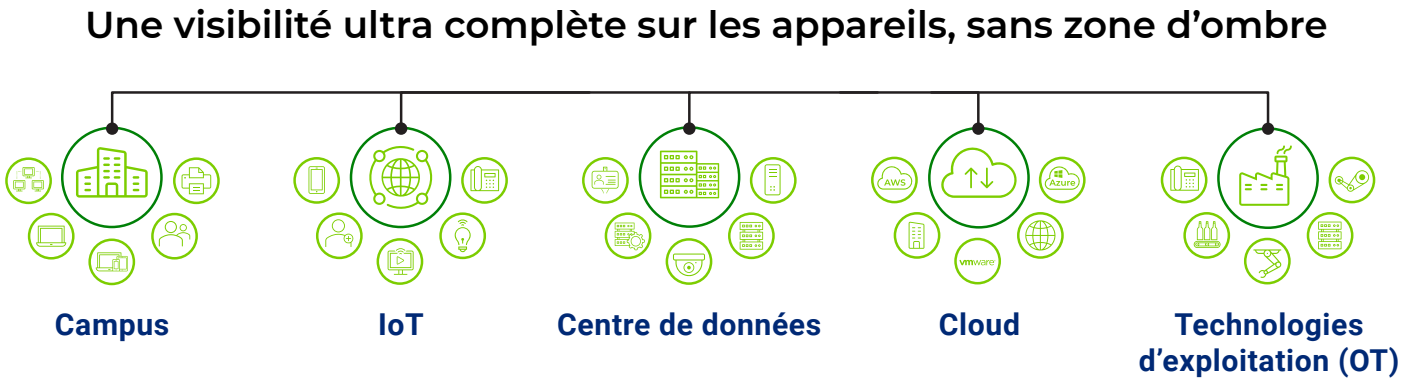


Figure 1. Forescout offre une visibilité sur les appareils à l'échelle de l'entreprise étendue qui permet de réaliser un inventaire des actifs détaillé et en temps réel de tous les objets qui se connectent à votre réseau.

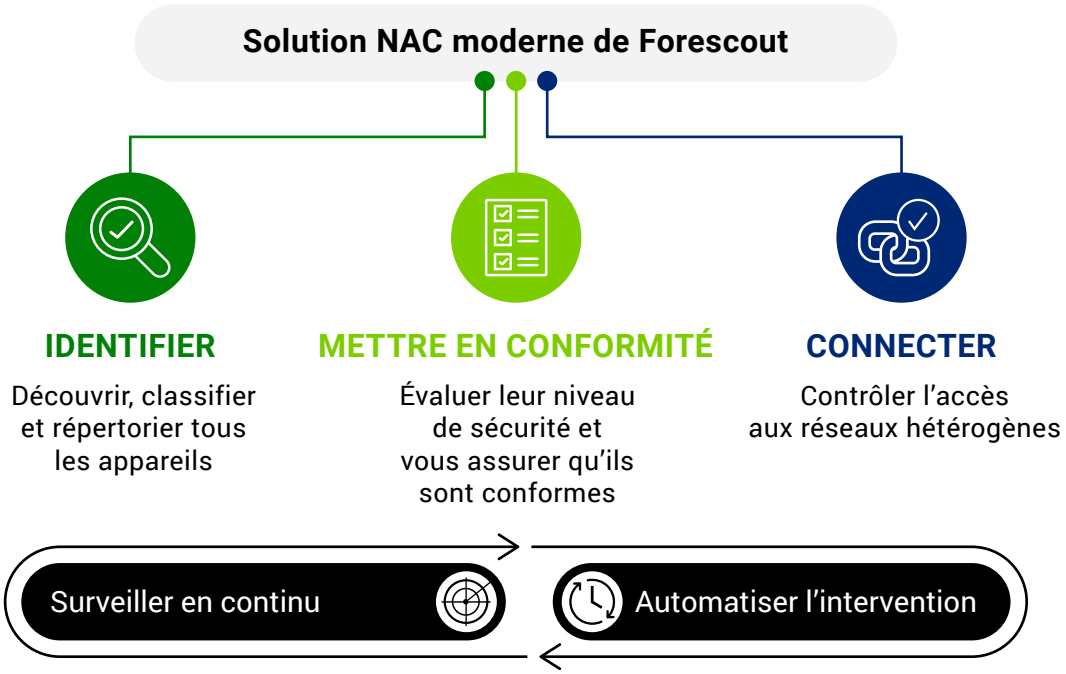


Figure 2. La solution NAC moderne de Forescout offre des fonctionnalités essentielles aux réseaux hétérogènes sans nécessiter l'installation d'agents logiciels ni l'authentification 802.1X.

Ses atouts

La solution NAC moderne de Forescout offre de multiples possibilités aux services informatiques :

- Sélection possible de quelque 20 techniques actives et passives pour découvrir, sans agent, tous les types d'appareils sur l'ensemble des sites et des réseaux — sans laisser aucune zone d'ombre
- Autoclassification précise des appareils sur la base de leur fonction, du système d'exploitation et de la version, ainsi que du fabricant et du modèle
- Création et gestion automatiques d'un inventaire des actifs en temps réel de tous les appareils à connexion IP de votre réseau étendu
- Évaluation et surveillance ininterrompue du niveau de sécurité de tous les équipements — sans agent
- Conformité aux politiques de sécurité et aux réglementations sectorielles grâce à une correction automatisée des terminaux
- Mise en œuvre de contrôles réseau flexibles basés sur l'authentification, le rôle utilisateur, le type d'appareil et le niveau de sécurité — sur n'importe quel réseau VPN, sans fil ou filaire hétérogène
- Contrôle d'accès basé sur le principe du moindre privilège pour une sécurité Zero Trust

Méthodes proposées pour identifier tous les équipements d'un réseau

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-feux 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 **passives sur le réseau et l'équipement.** 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 permet l'inspection approfondie des paquets de plus de 150 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 surveille également les requêtes RADIUS à l'aide d'un serveur externe ou intégré.
- Méthodes de découverte **actives 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 **actives portant sur l'équipement.** À titre d'exemple, citons l'analyse des segments réseau à l'aide de Nmap en vue d'identifier les appareils connectés, l'inspection à distance des appareils Windows avec WMI ou des appareils Mac et Linux avec SSH, et le profilage des terminaux au moyen de requêtes SNMP.

Techniques de visibilité sur les équipements

DÉCOUVERTE PASSIVE	DÉCOUVERTE ACTIVE D'INFRASTRUCTURES	DÉCOUVERTE ACTIVE D'ÉQUIPEMENTS
Traps SNMP	Interrogation de l'infrastructure réseau physique	Inspection sans agent pour Windows (WMI, RPC, SMB)
Trafic SPAN • Requêtes DHCP • Agent utilisateur HTTP • Empreintes TCP • Analyse de protocoles médicaux (20 protocoles) • Analyse de protocoles ICS/OT (plus de 70 protocoles)	Intégration de l'infrastructure réseau basée sur le contrôleur • Juniper Mist • Cisco ACI, Cisco Meraki	Inspection sans agent pour macOS, Linux (SSH)
Analyse des flux • NetFlow • Flexible NetFlow • IPFIX • sFlow	Intégration (de l'infrastructure virtuelle) de cloud privé • VMware	Nmap
Requêtes DHCP (via l'IP helper)	Intégration de cloud public • AWS • Azure	Requêtes SNMP sur les terminaux
Agent utilisateur HTTP (via redirection d'URL)	Services d'annuaires de requêtes (LDAP)	Inspection avec agent (SecureConnector)
Requêtes RADIUS	Applications web de requêtes (REST)	
Identificateur OUI de l'adresse MAC	Interrogation de bases de données externes (SQL)	
	Orchestrations (ITSM, UEM, EPP, EDR, VA)	

Figure 3. Méthodes Forescout de visibilité sur les appareils

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.

Un déploiement économique et simplifié dans les environnements de grande taille : la sélection possible de plus de 20 techniques passives et actives offre une grande souplesse pour disposer d'une visibilité complète sur les équipements dans n'importe quel réseau hétérogène, indépendamment de sa complexité, de la taille ou du nombre des sites distants, le tout sans devoir mettre à niveau l'infrastructure (matérielle ou logicielle) ni déployer un boîtier local dans chaque site/bureau.

Aucune zone d'ombre : il n'est pas rare que les entreprises possèdent des sites distants qui ne peuvent pas déployer de boîtiers supplémentaires ni acheminer un trafic SPAN. Notre prise en charge de plusieurs techniques actives et passives permet d'éviter les limitations imposées par le réseau et d'assurer une couverture totale des appareils sans aucune zone d'ombre.

Des méthodes exclusivement passives pour la découverte, la classification et l'évaluation dans les réseaux OT/ICS et du secteur de la santé critiques : ces derniers sont généralement peu adaptés à l'emploi de techniques de sondage et d'analyse actives susceptibles de perturber les systèmes médicaux et de contrôle des processus. La plateforme Forescout offre une visibilité sur les appareils dans tous les réseaux OT et du secteur de la santé au moyen d'une combinaison de techniques exclusivement passives, dont la surveillance du trafic SPAN aux fins d'inspection approfondie des paquets de plus de 150 protocoles IT, OT et médicaux. Ce qui distingue la solution Forescout est qu'au terme de l'identification des appareils, elle peut choisir la méthode à appliquer sur des appareils spécifiques, sans évaluation supplémentaire susceptible de perturber les activités de l'entreprise.

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 de l'adresse IP ou MAC des équipements qui se connectent. Elle met en œuvre deux processus. D'une part, la classification, qui consiste à collecter et à 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 aux politiques de sécurité, afin d'orienter les décisions en matière de contrôle d'accès et de correction. Ces deux méthodes méritent que nous les analysions plus en profondeur.

Autoclassification intelligente

Des données contextuelles exhaustives sur chaque appareil sont essentielles à la création de politiques granulaires. Vous devez connaître 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 575 versions de système d'exploitation ;
- plus de 5 700 produits et modèles de fabricants d'appareils ;
- les équipements médicaux de plus de 400 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'autoclassification de la plateforme bénéficie de cette précieuse source de données contextuelles pour s'adapter à la multiplication et à la diversification des équipements. Device Cloud, le plus grand référentiel au monde de données collaboratives sur les appareils, offre une source unique et multisectorielle d'informations approuvées sur les profils d'empreintes digitales, de comportements et de risques des différentes ressources de votre réseau, cela grâce à l'analyse de plus de 12 millions d'appareils d'entreprises clientes. Forescout Research publie très régulièrement de nouveaux profils pour améliorer l'efficacité de la classification, la couverture et la vitesse d'exécution pour l'ensemble des équipements de votre environnement.

Évaluation du niveau de sécurité et correction automatique sans agent

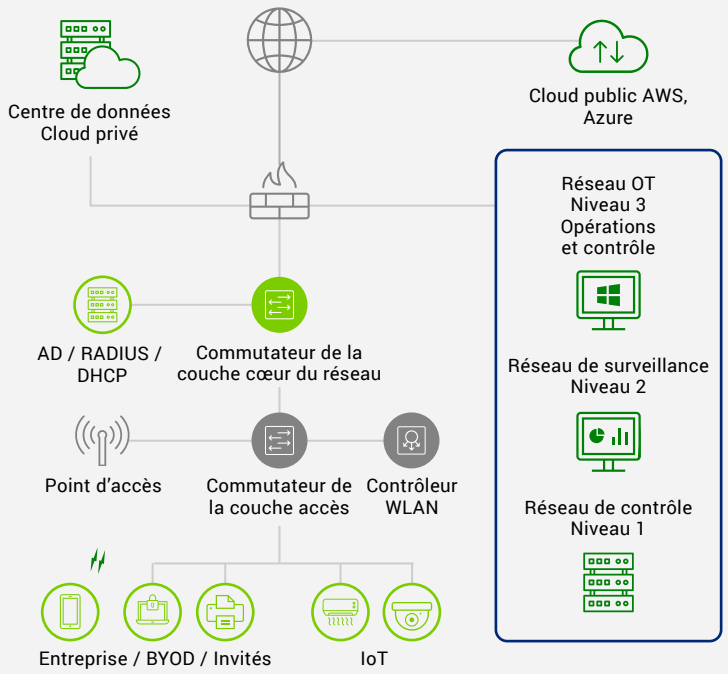
La classification des équipements fournit un contexte opérationnel concernant l'objectif de chacun d'entre eux. Toutefois, pour obtenir des données contextuelles exhaustives, il est nécessaire d'adopter une autre approche afin d'évaluer le niveau de sécurité et d'intégrité de chaque appareil. Forescout 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 ?

Après quoi, la **plateforme Forescout met en conformité les appareils en automatisant leur correction** à l'aide de contrôles natifs ou tiers. Elle est notamment capable d'exécuter les actions suivantes :

- 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
- Garantir à tout moment que les agents de sécurité fonctionnent correctement (qu'ils sont installés, en cours d'exécution et à jour)
- Désactiver ou bloquer les applications non autorisées qui pourraient engendrer des risques ou solliciter inutilement la bande passante du réseau et 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

Classification et évaluation des équipements



QUI
- Utilisateur
- Nom
- E-mail
- Titre
- Groupe
- Abonnement / Compte
- Rôle / responsable IAM

QUOI
- Fonction
- Système d'exploitation
- Fabricant et modèle
- Adresse IP
- Agent de navigateur
- Ports
- Virtuel ou physique
- Adresse MAC

NIVEAU DE SÉCURITÉ
- Applications
- Services
- Processus
- Versions
- Registre
- Correctifs
- Chiffrement
- Protection antivirus

OÙ
- Commutateur
- Contrôleur
- Port de commutateur / SSID / VLAN
- AWS / Azure
- Région
- VNet / VPC
- Niveau dans le modèle Purdue

Figure 4. 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 état de conformité.

« Les technologies d'appareils IoT et réseau sont source de risques de compromissions des réseaux et des entreprises. Chaque appareil intègre du code et des ressources que les équipes de sécurité doivent surveiller et considérer comme une infrastructure non fiable. Les équipes de sécurité doivent isoler, sécuriser et contrôler en permanence chaque appareil sur le réseau. » [2]

FORRESTER

8 JUIN 2020

La visibilité au service du contrôle

Les réseaux des clients sont tous différents. C'est la raison pour laquelle leurs exigences varient et leurs politiques de sécurité sont uniques. Il est donc crucial de déployer une solution flexible, capable de sécuriser tous les réseaux VPN, filaires et sans fil. Par exemple, les grandes entreprises déploient souvent la **solution non 802.1X** de Forescout **sur leurs réseaux filaires**. Elles choisissent cette option car elle est facile à déployer, ne nécessite pas de mise à niveau de l'infrastructure matérielle/logicielle ni de configuration complexe des commutateurs ou des terminaux, comme c'est le cas avec une solution 802.1X. Qui plus est, elle fonctionne dans une infrastructure réseau mono ou multifournisseur. Une telle pratique est conforme à la recommandation de Gartner qui préconise d'utiliser une solution non 802.1X sur les réseaux filaires pour simplifier le déploiement et réduire les frais d'exploitation. Toutefois, sur les réseaux sans fil, il est d'usage de déployer une solution 802.1X pour authentifier les appareils IT des utilisateurs d'entreprise. Les options de déploiement hybride et flexible de Forescout prennent en charge ces deux bonnes pratiques.

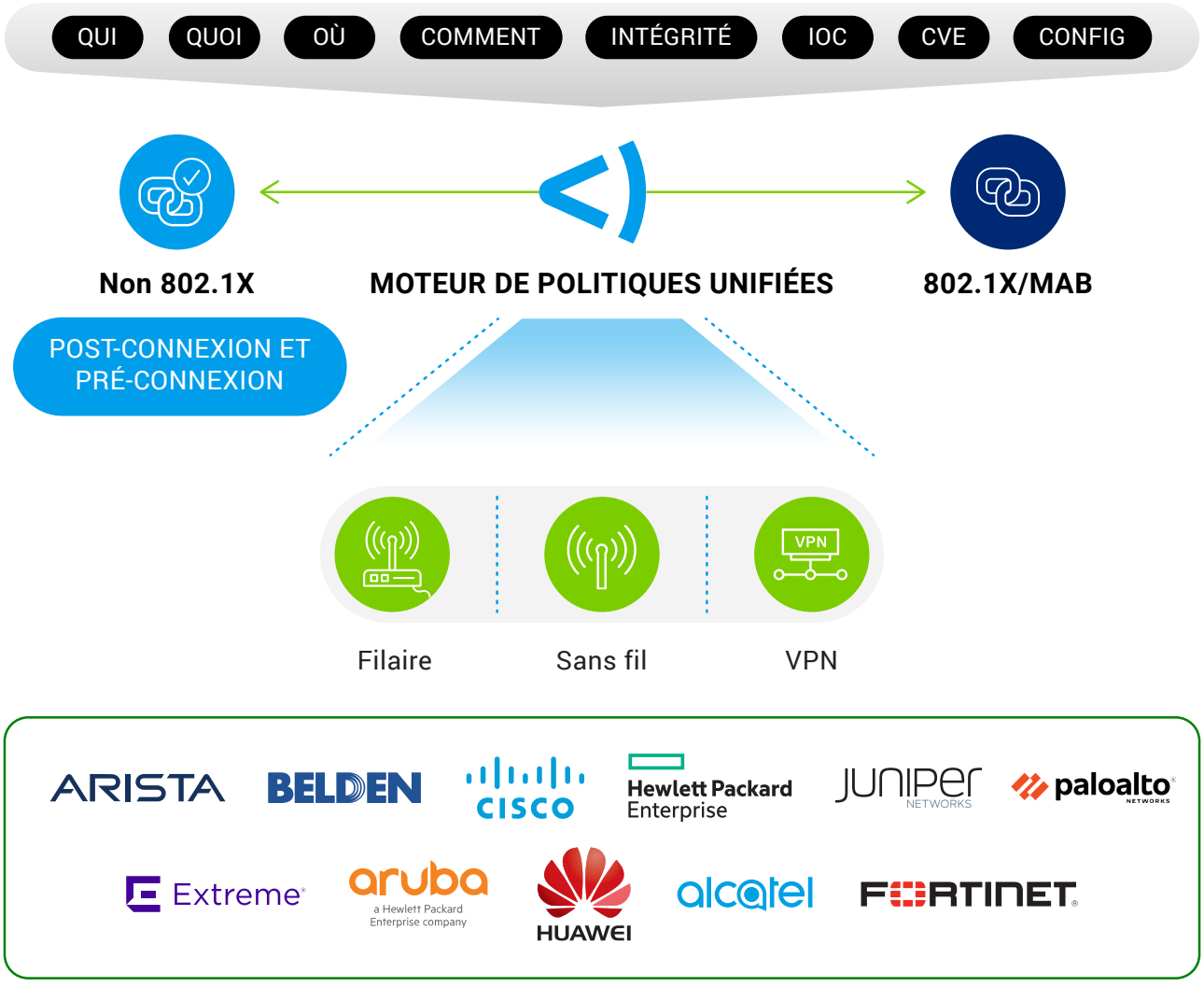


Figure 5. Forescout propose des options avec ou sans authentification 802.1X pour sécuriser les terminaux sur les réseaux VPN, filaires et sans fil multifournisseurs.

L'utilisation de la plateforme Forescout pour sécuriser l'accès au réseau présente de nombreux avantages, dont les suivants :

Flexibilité accrue

- Large choix de méthodes de contrôle d'accès — avec ou sans 802.1X
- Architecture filaire non 802.1X robuste — sans interruption des activités, déploiement simple, exigences de configuration minimales, sans mise à niveau de l'infrastructure, options de post-connexion et pré-connexion, rentabilité et retour sur investissement accélérés
- Moteur de politiques unifiées pour implémenter un accès sécurisé Zero Trust et différencié (accès entreprise, invité, BYOD, IoT)

Sans mise à niveau

- Intégration avec l'infrastructure existante sans mise à niveau logicielle/matérielle
- Compatible avec les composants d'infrastructure réseau de n'importe quel fournisseur (par ex. commutateur, contrôleur sans fil, IaaS), ce qui permet d'éviter l'enfermement propriétaire
- Rentabilité et retour sur investissement accélérés

Prise en charge d'outils hétérogènes

- Intégration directe (via SNMP, SSH, Telnet, RADIUS) avec des centaines de commutateurs et contrôleurs sans fil (quelle que soit la version de système d'exploitation) de plus de 30 fournisseurs d'infrastructure réseau, ce qui permet la mise en œuvre des accès réseau dans n'importe quel réseau multifournisseur
- Solution flexible qui garantit la continuité des activités et limite les coûts opérationnels, de déploiement et de maintenance
- Prise en charge d'outils hétérogènes permettant à un acquéreur de bénéficier rapidement de la visibilité et du contrôle requis sur les ressources après une fusion-acquisition

Segmentation à l'échelle de l'entreprise

- Tirez parti des données de visibilité de la plateforme Forescout pour déterminer l'état de segmentation en temps réel pour n'importe quel appareil, où qu'il soit.
- Concevez des politiques de segmentation logique et procédez à des simulations pour évaluer leur impact avant leur mise en œuvre.
- Surveillez en temps réel l'intégrité de la segmentation et réagissez aux violations des politiques dans l'entreprise étendue.

Pour en savoir plus sur la solution de segmentation à l'échelle de l'entreprise de Forescout, cliquez ici.

BONNES PRATIQUES DE DÉPLOIEMENT D'UNE SOLUTION NAC

Forescout recommande les bonnes pratiques suivantes pour le déploiement d'une solution NAC :

Réseau sans fil : 802.1X est couramment utilisé pour authentifier les appareils IT des utilisateurs d'entreprise sur les réseaux sans fil. Une fois ces derniers authentifiés, Forescout identifie et évalue sans agent la conformité des appareils pour les ordinateurs Windows, macOS et Linux.

Grâce au moteur de politiques de Forescout, les clients peuvent opter pour la correction automatique et mettre en œuvre les contrôles réseau appropriés afin de respecter les politiques de sécurité (par ex. envoi de notifications à l'utilisateur, correction, blocage et/ou partage du contexte avec des outils tiers).

Réseau filaire : sur les réseaux filaires, Forescout recommande une architecture non 802.1X. Compte tenu de la complexité du déploiement et de la gestion de l'authentification 802.1X et MAB sur les réseaux filaires, les clients optent généralement pour une option sans 802.1X. Ils commencent par la découverte des appareils, leur identification et une évaluation du niveau de sécurité/conformité, avant de mettre en œuvre les niveaux d'accès réseau appropriés à l'aide de contrôles non 802.1X dans n'importe quel réseau hétérogène. Remarque : Forescout assure aussi une prise en charge complète de l'authentification 802.1X sur les réseaux filaires.

Orchestration avec les produits IT et de sécurité

Tout au long du processus de contrôle d'accès au réseau, Forescout peut communiquer avec vos outils existants pour échanger des données contextuelles en temps réel sur les appareils et automatiser les flux de travail d'intervention. En plus d'accélérer la réduction des risques, vous pouvez maximiser le retour sur investissement des outils de gestion IT et de sécurité existants. Grâce à nos intégrations eyeExtend prêtes à l'emploi et à l'application eyeExtend Connect, nous aidons les clients à transformer rapidement leur mosaïque d'outils de gestion de la sécurité en un système d'intervention automatisé à l'échelle de l'entreprise, capable de défendre activement votre environnement EoT.

Voici quelques-uns des avantages de l'orchestration avec des outils de sécurité existants au cours du processus de contrôle d'accès au réseau :

Partage des données contextuelles sur les appareils

- Partagez les données contextuelles sur les appareils avec vos outils de gestion des actifs existants pour garantir un inventaire toujours correct et à jour (CMDB).
- Fournissez des données contextuelles en temps réel sur les appareils aux applications et aux équipes chargées des opérations de sécurité aux fins de mise en corrélation et priorisation des incidents.

Exécution des flux de travail à la connexion

- Comme ils procèdent à des analyses ponctuelles, les outils existants peuvent manquer l'évaluation des vulnérabilités des appareils connectés temporairement au réseau. Forescout collabore avec les outils de sécurité pour déclencher des analyses des vulnérabilités en temps réel au moment de la connexion.
- Lancez l'application des correctifs et les mises à jour de sécurité dès la connexion pour réduire la surface d'attaque.

Évaluation du niveau de sécurité

- Vérifiez que les agents de sécurité existants fonctionnent et identifiez les appareils présentant des risques ou des indicateurs de compromission.
- Détectez les comptes à privilèges obsolètes ou non autorisés sur les appareils connectés.

Automatisation des actions d'intervention

- Confinez, mettez en quarantaine ou bloquez les appareils vulnérables, compromis et présentant un risque élevé.
- Initiez des actions de correction et de limitation des risques basées sur des politiques dans le cadre des interventions sur incident.

Forescout domine actuellement le segment des solutions sans agent du marché NAC avec une part de marché de 64,7 %. Qui plus est, selon les estimations, la société compte le plus important pourcentage de déploiements NAC hybrides du secteur. Cette croissance est essentiellement due à l'ensemble très complet de fonctionnalités offertes par Forescout pour répondre aux demandes du segment à forte croissance de ce marché des appareils non gérés et nécessitant une approche sans agent.

IDC

MAI 2020[3]

Détecter, c'est bien. Sécuriser, c'est mieux.

La solution NAC moderne de Forescout propose une approche flexible, sans agent ni interruption des activités, pour mettre en œuvre une sécurité Zero Trust. Consultez ces ressources pour découvrir comment Forescout assure une défense active pour l'environnement EoT :

Lisez le Guide Gartner sur le marché des solutions de contrôle d'accès au réseau (NAC) : découvrez pourquoi Gartner considère Forescout comme « l'une des solutions NAC les plus populaires du marché ».

Visitez le site web de Forescout : apprenez-en davantage sur la solution NAC moderne de Forescout, y compris les cas d'utilisation, les mesures prises pour assurer la conformité des appareils et les témoignages des clients Forescout.

Participez à un atelier 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 une démonstration : rendez-vous sur le site de Forescout pour demander une démonstration personnelle de la plateforme et obtenir plus d'informations.

---

1. *The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook* (L'écosystème Zero Trust eXtended : Plan stratégique des réseaux – Feuille de route de l'architecture de sécurité et des opérations), Forrester Research, 2 janvier 2019
2. *Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles And Techniques* (Réduction des risques liés aux ransomwares grâce au modèle Zero Trust : renforcer votre protection grâce aux techniques et aux principes Zero Trust), Forrester Research, 8 juin 2020
3. *Worldwide NAC Market Shares, 2019: Diverse Market Demands Expand NAC's Addressable Market* (Parts de marché des solutions NAC dans le monde : de nouvelles demandes du marché étendent le marché potentiel des solutions NAC), IDC, mai 2020

Détecter, c'est bien. Sécuriser, c'est mieux.

Contactez-nous dès aujourd'hui pour protéger efficacement votre Internet des objets en entreprise.

forescout.com/solutions/network-access-control info-france@forescout.com Tél. (international) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
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