



eyeExtend Ecosystem

Automatisez les processus et interventions de cybersécurité sur vos solutions tierces

Les intégrations de **Forescout eyeExtend Ecosystem** vous permettent d'automatiser les processus de sécurité entre la plateforme Forescout et d'autres solutions informatiques et de sécurité afin d'améliorer l'efficacité opérationnelle et votre niveau de sécurité global. L'intégration des fonctionnalités de renseignement sur les appareils et d'exécution Forescout à vos produits informatiques et de sécurité actuels offre de nombreux avantages :

- ▶ Élimination des angles morts dans la reconnaissance d'appareils
- ▶ Automatisation des flux de travail entre les produits
- ▶ Réponse plus rapide aux risques, incidents et lacunes de conformité



Grande extensibilité

Vaste écosystème d'intégrations à plus de 70 prestataires technologiques.



Offre préconfigurée

Déploiement rapide d'intégrations conçues, testées et prises en charge par Forescout dans divers grands domaines technologiques.



Retour sur investissement accéléré

Gain de temps et d'argent grâce à des applications et intégrations éprouvées, prêtes à l'emploi.



Partage des données contextuelles des appareils

- ▶ Visibilité optimisée des appareils gérés et non gérés sur vos outils de sécurité
- ▶ Mise à jour de la base de données de gestion des configurations et synchronisation bidirectionnelle des propriétés des appareils
- ▶ Données contextuelles sur les appareils fournies en temps réel au SOC à des fins de corrélation et de priorisation des incidents



Automatisation des flux de travail

- ▶ Numérisation des processus de sécurité et coordination des flux de travail entre les différents outils
- ▶ Déclenchement d'analyses de vulnérabilité en temps réel et lancement de correctifs et de mises à jour de sécurité
- ▶ Vérification du bon fonctionnement et de l'actualité des agents de terminaux, agrégation des informations sur les menaces et chasse aux risques



Intervention accélérée

- ▶ Réduction et correction plus rapides des incidents à l'échelle du système
- ▶ Accès au réseau sur la base de politiques en fonction des utilisateurs, des appareils et du niveau de sécurité
- ▶ Neutralisation, mise en quarantaine ou blocage d'appareils vulnérables, compromis ou à haut risque

eyeExtend Ecosystem résout les problèmes suivants :

- ▶ **Non-respect des politiques de sécurité, réglementations et licences logicielles**
dû aux angles morts des solutions de sécurité existantes.
- ▶ **Coûts opérationnels élevés et baisse de productivité**
dus au cloisonnement des outils de sécurité, nécessitant une coordination manuelle pour résoudre les problèmes.
- ▶ **Risque de propagation des menaces**
dû à la capacité limitée des solutions tierces à réagir de manière rapide et efficace aux menaces de sécurité et aux incidents.

Partage des données contextuelles des appareils

Partagez les informations et les données contextuelles sur les appareils de manière bidirectionnelle avec les solutions tierces pour améliorer les flux de travail des politiques.

- ▶ Exploitez les informations contextuelles fournies par la plateforme ForeScout concernant le type des appareils, leur configuration, leur emplacement, les utilisateurs, les modèles d'authentification, ainsi que l'évaluation sans agent de la sécurité de votre environnement numérique, y compris les appareils IT, IoT et OT.
- ▶ Faites gagner un temps précieux à votre équipe en automatisant la mise à jour des bases de données d'inventaire des appareils.
- ▶ Détectez les anomalies et priorisez les incidents en associant les données de la plateforme Continuum à d'autres sources de cyber-intelligence.

Automatisation des flux de travail

Automatisez les flux de travail entre produits concernant l'évaluation du niveau de sécurité et les mesures correctives afin de garantir une adéquation constante avec les politiques de sécurité internes, les normes externes et les réglementations sectorielles.

- ▶ Déclenchez des analyses en temps réel des vulnérabilités sur les nouveaux appareils et les appareils en transit au moment de la connexion.
- ▶ Lancez les correctifs et les mises à jour de sécurité pour réduire la surface d'attaque.
- ▶ Vérifiez le bon fonctionnement des agents de terminaux et automatisez les mesures de correction en cas de non-conformité.
- ▶ Détectez automatiquement les comptes à privilèges non gérés en temps réel et appliquez la mise en conformité.
- ▶ Étendez la chasse aux menaces aux appareils non gérés grâce aux informations, indicateurs de compromission et violations de politiques fournis par d'autres outils.

Intervention accélérée

Réduisez le délai moyen d'intervention en cas d'incident ou de menace en accélérant la réaction aux alertes de solutions tierces.

- ▶ Lancez des actions de contrôle de l'accès au réseau de manière automatique ou manuelle sur la base de politiques de sécurité.
- ▶ Limitez ou bloquez l'accès au réseau pour les appareils compromis ou malveillants.
- ▶ Mettez en quarantaine ou isolez les appareils non conformes jusqu'à la résolution du problème.



« Nous recherchons un outil qui joue vraiment le jeu. Compatible avec tous les fournisseurs, la solution Forescout est aussi facile que rapide à mettre en œuvre et permet de bénéficier d'excellentes fonctionnalités de visibilité, de conformité et de classification en temps réel. Elle s'intègre aisément à d'autres systèmes de notre environnement, qu'elle rend plus efficaces et efficaces. »

PHIL BATES

RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, ÉTAT D'UTAH

Lisez l'[étude de cas](#)

La plateforme la plus extensible offrant une vaste gamme d'intégrations

Modules d'eyeExtend Ecosystem : conçus et pris en charge par Forescout

Forescout propose des modules eyeExtend Ecosystem couvrant huit catégories de technologies de sécurité, mis à jour et optimisés de manière régulière.

<p>ATD</p>	<p>EMM</p>	<p>SIEM</p>
<p>PAM</p>	<p>VA</p>	<p>ITSM IRM</p>
<p>CONFORMITÉ</p> <p>SCAP</p>	<p>EPP/EDR</p>	<p>NGFW</p>

Inclus dans Forescout eyeExtend Ecosystem

	INCLUS
Module de conformité avancée	✓
eyeExtend pour Carbon Black	✓
eyeExtend pour pare-feu de nouvelle génération Check Point	✓
eyeExtend pour la prévention des menaces Check Point	✓
eyeExtend pour CrowdStrike	✓
eyeExtend pour CyberArk	✓
eyeExtend pour FireEye EX	✓
eyeExtend pour FireEye HX	✓
eyeExtend pour FireEye NX	✓
eyeExtend pour pare-feu de nouvelle génération Fortinet	✓
eyeExtend pour HPE ArcSight	✓
eyeExtend pour IBM BigFix	✓
eyeExtend pour IBM Qradar	✓
eyeExtend pour McAfee ePolicy Orchestrator	✓
eyeExtend pour pare-feu de nouvelle génération Palo Alto Networks	✓
eyeExtend pour Palo Alto Networks WildFire	✓
eyeExtend pour la gestion des vulnérabilités Qualys	✓
eyeExtend pour Rapid7 Nexpose	✓
eyeExtend pour ServiceNow	✓
eyeExtend pour Splunk	✓
eyeExtend pour Symantec Endpoint Protection Manager	✓
eyeExtend pour la gestion des vulnérabilités Tenable	✓