

# Test en conditions réelles Forescout : expérience Test Drive



## Découvrez les avantages de la plateforme Device Visibility and Control, sans agent

Voici une occasion unique de mettre à l'épreuve la plateforme Forescout. Durant ce test de trois heures, l'équipe Forescout fera tourner des sessions virtuelles de la solution Forescout et vous guidera tout au long de six cas d'utilisation tirés de situations réelles. Vous aurez ainsi l'occasion de constater par vous-même les avantages du produit.

### Organisation du cours

Cet essai en conditions réelles va aborder bien des situations.

Voici comment les trois heures se déroulent :

#### <) Arrivée des participants et accueil

(premières 15 minutes)

#### <) Présentation du cours

(45 minutes) Boissons et en-cas inclus

#### <) Expérience Test Drive

(2 heures)

 <b>1re partie : Visibilité</b>	Découvrez comment détecter tous les appareils physiques et virtuels connectés à votre réseau, les classer et évaluer leur niveau de sécurité.
 <b>2e partie : Gestion des actifs</b>	La visibilité sans agent et la surveillance continue alimentent chaque aspect de la cybersécurité. Accédez à un inventaire des actifs matériels et logiciels en temps réel (dont vous ignorez peut-être l'existence !) afin de réaliser un audit logiciel annuel, sans qu'il soit nécessaire de détourner votre équipe d'autres tâches critiques.
 <b>3e partie : Conformité des appareils</b>	Optimisez votre audit de sécurité et déterminez rapidement l'état de mise à jour des logiciels de protection exécutés sur les appareils en réseau. Créez et appliquez des politiques qui entraînent l'envoi d'une notification aux employés lorsqu'ils utilisent un appareil non conforme, et d'une confirmation lorsque les exigences de sécurité sont à nouveau respectées.
 <b>4e partie : Intervention sur incident</b>	Intervenez lors d'une attaque WannaCry en exploitant le moteur de politiques Forescout au maximum de son potentiel. Appliquez une politique automatisée permettant de repérer rapidement les systèmes vulnérables et de déterminer lesquels sont déjà infectés ou nécessitent l'application de correctifs. Plus besoin de passer par un processus complexe comme la plupart des autres entreprises.

 <b>5e partie :</b> <b>Contrôle d'accès au réseau</b>	<p>Modifiez la politique antivirus de l'entreprise. En cas d'attaque WannaCry, sortez rapidement de votre réseau les appareils qui n'exécutent pas d'antivirus à jour. Expérimentez un niveau de contrôle inédit : évaluez rapidement les appareils, puis restreignez, bloquez ou placez en quarantaine les systèmes non conformes.</p>
 <b>6e partie :</b> <b>Segmentation du réseau</b>	<p>Évaluez les appareils présents sur votre réseau, et veillez à ce qu'ils ne puissent accéder qu'aux seules ressources dont ils ont besoin. Afin de réduire les risques que représentent les appareils non approuvés et non conformes, segmentez l'accès en fonction du type des appareils et de leur niveau de sécurité.</p>



### Affinez votre rentabilité

Vous souhaitez voir l'impact de Forescout sur vos résultats ? En 10 minutes, l'outil de ROI/valeur métier de Forescout (basé sur la méthodologie IDC d'évaluation des retours financiers) vous permet de traiter les données de votre entreprise et de les partager avec votre équipe sous la forme d'un rapport personnalisé. Contactez [info-france@forescout.com](mailto:info-france@forescout.com) pour obtenir votre rapport de rentabilité personnalisé.

### Vérifiez les angles morts de votre réseau

Sur votre réseau, les appareils inconnus vous attendent au tournant. La solution Forescout fournit une évaluation détaillée des terminaux de votre réseau (systèmes d'infrastructure et non approuvés ; appareils BYOD, IoT et OT) et signale les appareils cachés.

Vous disposez ainsi d'une connaissance situationnelle complète, vous exercez un contrôle strict sur les appareils et vous pouvez orchestrer les actions permettant de réduire les cyberrisques et les risques opérationnels, sans agent et sans interrompre les services stratégiques.

La première étape de notre processus est l'évaluation gratuite de la visibilité et des risques.

Inscrivez-vous dès aujourd'hui sur [www.forescout.fr](http://www.forescout.fr)

### Public visé :

Ingénieurs bureautiques

Responsables de centre d'assistance ou bureautiques

Analystes informatiques

Responsables informatiques

Architectes réseau

Ingénieurs réseau

Ingénieurs système

Responsables de l'équipe d'ingénieurs système

Analystes des opérations de sécurité

Responsables des opérations de sécurité



### Crédits de formation continue disponibles

Les membres du programme (ISC)<sup>2</sup> qui participent au test en conditions réelles Forescout Test Drive Experience pourront gagner jusqu'à trois crédits de formation continue. Merci de nous communiquer votre numéro de membre lors de votre inscription.

**Remarque :** ce document décrit une session technique au cours de laquelle vous allez vous exercer à utiliser la plateforme Forescout. Un expert vous guidera tout au long de la création et du déploiement de politiques basées sur les bonnes pratiques. Vous devez apporter votre propre ordinateur portable Windows®, Linux® ou Mac doté de Google Chrome™ ou de Mozilla Firefox® (navigateurs recommandés).

Découvrez tous les avantages par vous-même dès aujourd'hui

Consultez la page [https://resources.forescout.com/test\\_drives\\_french.html](https://resources.forescout.com/test_drives_french.html) pour découvrir les sites de test et vous inscrire.

Pour en savoir plus, consultez le site [forescout.fr](http://forescout.fr)



© 2019 Forescout Technologies, Inc. Tous droits réservés. Forescout Technologies, Inc. est une société ayant son siège dans l'État du Delaware. Les logos et marques commerciales de Forescout sont disponibles à l'adresse suivante : [www.forescout.com/company/legal/intellectual-property-patents-trademarks](http://www.forescout.com/company/legal/intellectual-property-patents-trademarks). Les autres marques, produits ou noms de services mentionnés dans ce document peuvent être des marques commerciales de leurs propriétaires respectifs. Version 06\_19