

# Das Forescout-Test Drive-Erlebnis



## Device Visibility and Control:

### Erleben Sie die Vorteile agentenloser Gerätetransparenz und -kontrolle

Nutzen Sie Ihre Chance, die Device Visibility and Control-Plattform von Forescout auf Herz und Nieren zu testen. Während dieses dreistündigen, praktischen Testlaufs startet das Forescout-Team virtuelle Sitzungen der Forescout-Lösung und gibt Ihnen die Möglichkeit, sechs reale Anwendungsszenarien selbst durchzuspielen, damit Sie den Vorher-Nachher-Effekt selbst erleben.

### Der Kursplan



In Ihrem Test Drive werden viele Bereiche vorgestellt.  
Ihr dreistündiges Erlebnis wird aus folgenden Komponenten bestehen:

**<) Ankunft und Begrüßung**  
(erste 15 Minuten)

**<) Einleitung zum Kurs**  
(45 Minuten) einschließlich  
Snacks und Getränken

**<) Test Drive-Erlebnis**  
(2 Stunden)

<b>1. Runde: Transparenz</b>	Erfahren Sie, wie Sie jedes mit Ihrem Netzwerk verbundene physische und virtuelle Gerät erkennen, klassifizieren und dessen Sicherheit bewerten können.
<b>2. Runde: Asset-Verwaltung</b>	Agentenlose Gerätetransparenz und kontinuierliches Monitoring bringen jeden Bereich der Cybersicherheit voran. Verschaffen Sie sich für das jährliche Software-Audit mit einem Echtzeit-Inventar (dessen Existenz Ihnen noch nicht bewusst war) einen vollständigen Überblick über alle Hardware- und Software-Assets – ohne dazu Mitarbeiter von anderen wichtigen Aufgaben abziehen zu müssen.
<b>3. Runde: Geräte-Compliance</b>	Optimieren Sie ein Sicherheits-Audit, um schnell festzustellen, ob vernetzte Geräte die aktuellste Sicherheits-Software verwenden. Erstellen Sie anschließend eine Richtlinie, mit der Mitarbeiter Benachrichtigungen über nicht konforme Endgeräte und Sie Bestätigungen über die Wiederherstellung der Compliance erhalten.
<b>4. Runde: Reaktion auf Vorfälle</b>	Testen Sie das Forescout-Richtlinienmodul bei der Reaktion auf einen WannaCry-Ausbruch. Verwenden Sie eine automatisierte Richtlinie, um gefährdete Hosts schnell zu identifizieren und festzustellen, welche noch gepatcht werden müssen bzw. bereits infiziert sind. Damit gehören die heute in Unternehmen eingesetzten komplexen Prozesse der Vergangenheit an.

 <b>5. Runde:</b> <b>Netzwerkzugriffssteuerung</b>	Setzen Sie Änderungen in der Virenschutzrichtlinie Ihres Unternehmens durch. Bei einem WannaCry-Ausbruch müssen Sie umgehend Endgeräte aus Ihrem Netzwerk entfernen, auf denen keine aktuelle Virenschutzsoftware ausgeführt wird. Erleben Sie völlig neue Kontrollmöglichkeiten, wenn Sie Endgeräte schnell bewerten und nicht konforme Geräte blockieren oder isolieren bzw. deren Zugriffsrechte einschränken.
 <b>6. Runde:</b> <b>Netzwerksegmentierung</b>	Bewerten Sie die Endgeräte in Ihrem Netzwerk, und stellen Sie sicher, dass sie nur auf die erforderlichen Assets zugreifen können. Segmentieren Sie den Zugriff basierend auf Endgerätetyp und Sicherheitsstatus, um die Risiken nicht autorisierter und nicht konformer Systeme zu reduzieren.



### Steigern Sie Ihre Rendite

Sie möchten die Vorteile der Forescout-Lösung für Ihre Rendite sehen? Mit dem Forescout Business Value ROI Tool (basierend auf dem IDC Business Value Model) und den Zahlen Ihres Unternehmens erfahren Sie in nur 10 Minuten, wie sie abschneiden. Und den individuellen Bericht können Sie an Ihr Team weitergeben. Kontaktieren Sie uns noch heute, um Ihren individuellen Forescout-ROI-Bericht zu erhalten.

E-Mail: [info-dach@forescout.com](mailto:info-dach@forescout.com)

### Entdecken Sie die blinden Flecken Ihres Netzwerks

Verborgene Geräte lauern hinter jeder Ecke – und verbergen sich in Ihrem Netzwerk. Forescout macht unbekannte Geräte mit einer detaillierten Bewertung Ihrer Netzwerkendgeräte sichtbar, einschließlich Infrastruktur- und nicht autorisierter Geräte sowie BYOD-, IoT- und OT-Geräte.

So erhalten Sie einen vollständigen Überblick und können Maßnahmen koordinieren, mit denen sich das operative und das Cyberrisiko reduzieren lassen. Dazu sind weder Agenten noch Unterbrechungen geschäftskritischer Dienste erforderlich.

Der erste Schritt besteht aus einer kostenlosen Transparenz- und Risikobewertung.

Vereinbaren Sie noch heute eine Demo unter [www.forescout.de](http://www.forescout.de)

### Die Zielgruppe:

Desktop-Techniker

Desktop- oder Helpdesk-Manager

IT-Analysten

IT-Manager

Netzwerkarchitekten

Netzwerktechniker

Systemtechniker

Systemtechnik-Manager

Sicherheitsablauf-Analysten

Sicherheitsablauf-Manager



### CPE-Credits erhältlich

(ISC)<sup>2</sup>-Mitglieder, die am Forescout Test Drive teilnehmen, qualifizieren sich für bis zu 3 CPE-Weiterbildungs-Credits. Bitte geben Sie daher bei der Registrierung Ihre (ISC)<sup>2</sup>-Mitgliedschaftsnummer an.

**Hinweis:** Hierbei handelt es sich um eine technische, praktische Sitzung, in der Forescout-Experten Ihnen vor Ort an der Forescout-Plattform die Best Practices für Richtlinienerstellung und Bereitstellung nahebringen. Sie müssen Ihren eigenen Windows<sup>®</sup>-, Linux<sup>®</sup>- oder Mac-Laptop mitbringen. Als Webbrowser sind Google Chrome<sup>™</sup> oder Mozilla Firefox<sup>®</sup> empfohlen.

### Erleben Sie den Unterschied!

Informationen zu Veranstaltungsorten und zur Registrierung finden Sie unter [resources.forescout.com/test\\_drives\\_germany.html](http://resources.forescout.com/test_drives_germany.html)

Weitere Informationen finden Sie unter [forescout.de](http://forescout.de)



© 2019 Forescout Technologies, Inc. Alle Rechte vorbehalten. Forescout Technologies, Inc. ist ein Unternehmen aus Delaware. Eine Liste unserer Marken und Patente finden Sie unter [www.forescout.com/company/legal/intellectual-property-patents-trademarks](http://www.forescout.com/company/legal/intellectual-property-patents-trademarks). Andere genannte Marken, Produkte oder Servicennamen können Marken oder Servicemarken ihrer jeweiligen Eigentümer sein. Version 06\_19