FORESCOUT

Vollständige Transparenz: Der Königsweg zu Zero Trust

Forescout's Device-Visibility-Plattform für Zero-Trust-Sicherheit

> "Transparenz ist der Schlüssel zum Schutz aller Assets. Du kannst nicht schützen, was Du nicht siehst. Je größer die Transparenz im gesamten Business-Netzwerk ist, desto schneller lassen sich verräterische Anzeichen eines Angriffs erkennen und stoppen."[3]

Traue niemandem

Das Zero-Trust-Modell der IT-Sicherheit ist aus gutem Grund sowohl in den Strategien der Sicherheitsteams als auch in den Roadmaps der Entwickler von Sicherheitslösungen fest verankert. Perimeter-Sicherheitsarchitekturen, die auf großes Vertrauen der Geräte untereinander im Netzwerk bauen, können zu teuren Katastrophen führen. Eine neue Analyse der Online Trust Alliance ergab, dass sich Business-Sicherheitsvorfälle in 2017 fast verdoppelt haben. In den ersten 9 Monaten des Jahres 2017 wurden mehr als 7 Mrd. Datenschutzverletzungen registriert – eine Vervierfachung gegenüber 2016.[1] Die Kosten für diesen massenhaften Datenmissbrauch belaufen sich laut des Ponemon Institute pro gestohlenem Datensatz auf 117 Euro und pro Fall auf durchschnittlich 3,02 Mio. Euro.[2]

Die Mehrfachversagen der Perimeter-Sicherheit

Heutige Unternehmen sind stark auf Cloud-Dienste und -Infrastrukturen angewiesen, die harte Netzwerkgrenzen komplett aufweichen. Workloads, Daten und die Belegschaft selbst sind inzwischen mobil und brauchen flexible Sicherheit. Benutzer benötigen mehr Zugriffsmöglichkeiten auf mehr Konten, Daten und Ressourcen. Gleichzeitig überfordern Anzahl und Vielfalt der Geräte im Netzwerk das traditionelle Endpoint-Management. Da auf vielen dieser Geräte keine Netzwerk-Management-Software läuft (Besuchergeräte, BYOD-Systeme, IoT-Geräte und Steuerungen), sind die Sicherheitsteams bei vielen Geräten blind was angemeldete Benutzer, der Sicherheitsstatus und Aktivitäten der Geräte angeht.

Diese systemischen Mängel der Perimeter-orientierten Sicherheit veranlassten Analysten von Forrester Research im Jahr 2010, Zero Trust als Alternative zu entwickeln. Zero Trust ist ein konzeptionelles Modell, wie Sicherheitsteams

- Netzwerke in sichere Mikro-Perimeter umbauen,
- die Datensicherheit durch Verschleierungstechniken stärken,
- die mit zu großen Benutzerrechten verbundenen Zugriffsrisiken begrenzen
- und sowohl die Analyse als auch die Reaktion auf Sicherheitsprobleme mit Analytik und Automatisierung drastisch verbessern können.

Zero Trust: Vom Konzept zum umfassenden Framework

Die ersten Zero-Trust-Modelle konzentrierten sich auf Konzepte zur Schutz-Segmentierung und des Zugangs mit geringsten Privilegien. Sie ließen aber meist offen, wie bestehende Sicherheitskontrollen in der Praxis besser genutzt werden können. Im Laufe der Zeit ist das Basismodell zu etwas gereift, was Forrester das Zero Trust eXtended (ZTX) Ecosystem nennt. Dieses umfassende Framework bildet alle relevanten Sicherheitstechnologien auf sieben Schlüsselaspekte einer typischen Unternehmensinfrastruktur mit Zero-Trust-Prinzipien ab: Netzwerke, Daten, Personen, Workloads, Geräte, Sichtbarkeit und Analyse sowie Automatisierung und Orchestrierung.

Das ZTX-Framework hilft Sicherheitsteams zu verstehen, was die jeweilige Technologie bewirkt:

- Es führt die Prinzipien der Netzwerkisolierung, Segmentierung und Sicherheit ein
- Ermöglicht die Kategorisierung, Isolierung, Verschlüsselung und Kontrolle von Daten
- Schützt die Nutzer der Netzwerk- und Infrastrukturressourcen, indem es die Anwender von den Ressourcen abschottet
- Schützt Anwendungs-Suiten in Public und Private Clouds
- Automatisiert und orchestriert Zero-Trust-Kontrollen und -Prozesse in heterogenen Umgebungen
- Beleuchtet und sichert mit Transparenz und Analyse jeden Winkel der ausgedehnten Unternehmensinfrastruktur

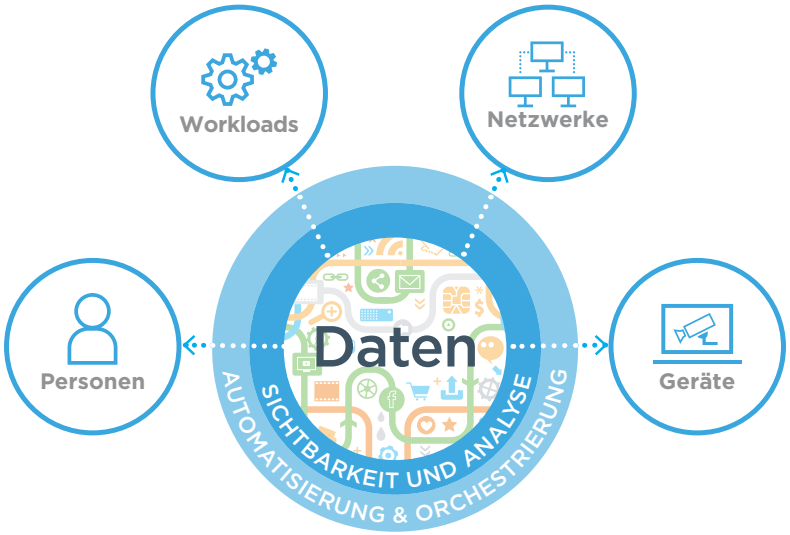

Bild 1: Die sieben Dimensionen des Forrester Researchs Zero Trust eXtended Ecosystem Frameworks

Wenn Transparenz die Strategie ist, ist Forescout die Plattform

Ein Beispiel für eine Zero-Trust-Strategie ist das Ziel, ausnahmlos alle Geräte , die mit dem Netzwerk verbunden sind – auch solche ohne spezielle, vorher installierte Software – zu ermitteln und zu klassifizierenund Zugriffsrichtlinien mit geringsten Rechten strikt durchzusetzen. Diese basieren auf einer gründlichen Analyse des Geräts, der Benutzerberechtigungen, des Software-Stacks, der einzuhaltenden Konfiguration und des Sicherheitsstatus. Um strenge Richtlinien durchzusetzen, muss man alles im Netzwerk sehen, bewerten und kontrollieren können.

Forrester betont das Thema Sichtbarkeit in Zero-Trust-Strategien. Laut Forrester-Analyst Chase Cunningham gilt: "Transparenz ist der Schlüssel zum Schutz aller Assets. Du kannst nicht schützen, was Du nicht siehst. Je größer die Transparenz im gesamten Business-Netzwerk ist, desto schneller lassen sich verräterische Anzeichen eines Angriffs erkennen und stoppen."[3]

Um diese Strategie zu realisieren, bedarf es einer umfassenden Lösung, die auch Geräte erkennt und kontrolliert, welche von herkömmlichen Netzwerk-Managementsysteme meistens übersehen werden: Besucher- und BYOD-Geräte, Devices ohne aktive Agenten, Spionage- und IoT-Geräte, Netzwerk-Switches und -Router, Industrie- und Produktionssysteme sowie virtuelle Maschinen in Public Clouds.

Die Forescout-Plattform: Transparenz gewinnen und Risiken senken

Forescout zeigt beispielhaft die Weiterentwicklung führender Netzwerktechnologien zu Zero-Trust-Plattformen. Die Forescout-Plattform ist eine agentenlose Sicherheitslösung, die Netzwerkgeräte dynamisch identifiziert und bewertet, sobald sie sich mit Ihrem ausgedehnten, heterogenen, Multicloud-Netzwerk verbinden. Es erkennt sofort Benutzer, Besitzer, Betriebssystem, Gerätekonfiguration, Software, Dienste, Patch-Level und die Existenz von Sicherheitssoftware. Daraufhin übernimmt es die kontinuierliche Überwachung, Kontrolle und Wiederherstellung dieser Geräte.

Forescout setzt diese Funktionen auf administrierten Unternehmensgeräten, nicht kontrollierten Besuchergeräten, physischen und virtuellen Servern, der Netzwerkinfrastruktur, industriellen Steuerungssystemen und IoT-Geräten ein – ohne dass Software auf den Geräten oder Vorkenntnisse erforderlich sind. Es integriert sich schnell in bestehende Umgebungen und erfordert selten Anpassungen oder Upgrades der Infrastruktur oder Endgeräte. Wesentlich dabei ist, dass es in physischen, virtuellen und hybriden Cloud-Umgebungen problemlos funktioniert.

Die Forescout-Plattform erkennt und klassifiziert 100 Prozent aller IP-Geräte im Netzwerk und ermöglicht eine kontinuierliche, agentenlose Risiko- und Lagebewertung, um in Echtzeit für jedes Gerät die aktuelle Situation zu ermitteln. Es nutzt diese Informationen, um auf Geräten regelbasierte Kontrollen zu automatisieren und Aktionen zu koordinieren. Diese Fähigkeiten bilden die Grundlage einer effektiven Zero-Trust-Sicherheit.

Transparenz, Analyse und Kontrolle von Zero-Trust-Geräten

Agentenloses Erkennen jedes Geräts - Die Forescout-Plattform nutzt aktive und passive Methoden ohne Agenten, um alle Geräte in großen heterogenen Unternehmensnetzwerken zu identifizieren – vom Campus und Rechenzentrum bis hin zu Cloud- und Industrie-Netzwerken. Es erkennt PCs und Notebooks, physische und virtuelle Server, mobile und IoT-Geräte, Cloud-Instanzen und OT-Netze ohne herstellerspezifische Netzwerkausrüstung, Upgrades der bestehenden Infrastruktur oder Rekonfiguration von Switches und Ports, mit oder ohne 802.1X-Authentifizierung.infrastructure or reconfiguration of switches and switch ports, with or without 802.1X authentication.

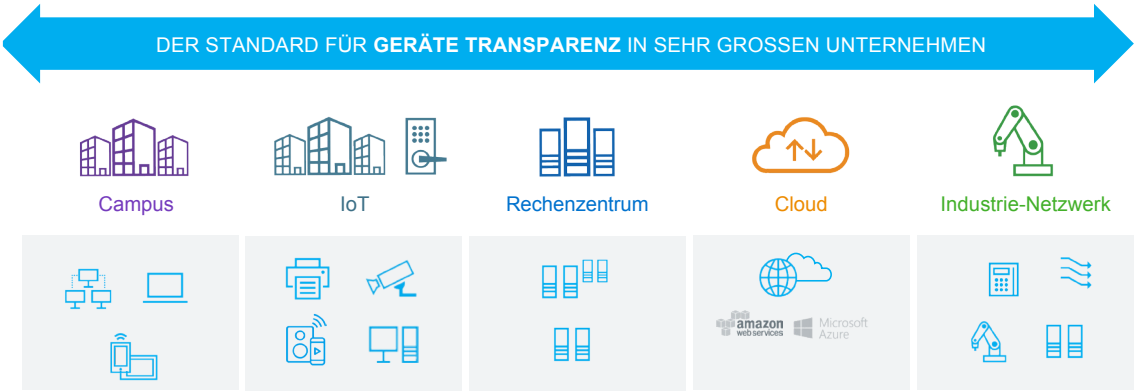

Bild 2: Forescout bietet eine Device Visibility and Control-Plattform für die Gerätetransparenz und -kontrolle großer Unternehmen.

Von der Geräteerfassung zur Asset-Analyse – Forescouts vielfältige Erkennungs- und Analysemethoden ermitteln und aktualisieren in kürzester Zeit diverse Informationen zu Geräteidentität, -status und -verhalten. Die adaptive Abstraktionsschicht untersucht Milliarden von Netzwerk-Paketen heterogener Unternehmensnetzwerke. Es verknüpft und konsolidiert diese Daten und erzeugt eine Übersicht über die gesamte Gerätelandschaft mit vielen Drill-Down-Details der einzelnen Geräte. Die Abstraktionsschicht passt sich der (wachsenden) IT-Umgebung an und erweitert die Geräteübersicht kontinuierlich, wenn neue Datenquellen auftauchen. Die Daten bieten einen detaillierten Überblick über alle Netzwerk-Assets und bilden damit die Grundlage für viele Entscheidungen, Maßnahmen und risikomindernde Aktionen.

Zusätzlich überwacht und visualisiert die Forescout-Plattform die Kommunikation zwischen Geräten, Datenquellen und Systemen. Dies ist besonders für die Segmentierung, Planung und Richtlinienerstellung wichtig.

Die Forescout-Plattform überwacht und visualisiert die Kommunikation zwischen Geräten, Datenquellen und Systemen. Dies ist besonders für die Segmentierung, Planung und Richtlinienerstellung wichtig.

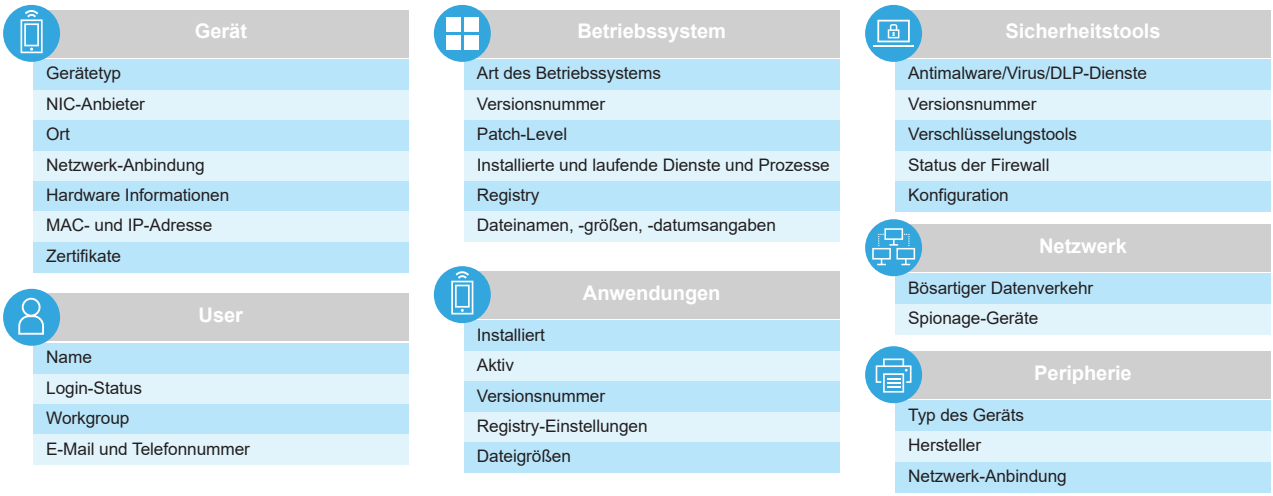

Bild 3: Der Klassifizierungsprozess von Forescout extrahiert detaillierte Daten aller per IP vernetzten Geräte.

Kontinuierliche Transparenz und richtlinienbasierte Gerätesteuerung - Die Echtzeit-Richtlinien-Engine von Forescout nutzt diese Asset-Erkenntnisse, um Geräte kontinuierlich zu bewerten und das gewollte Verhalten durchzusetzen. Es triggert Aktionen in Echtzeit, basierend auf den Zugriffsrechten, der Authentifizierung und anderen anpassbaren Attributen eines Geräts. So kann Forescout beispielsweise ein neues IoT-Gerät mit ausgehendem Internetverkehr identifizieren und automatisch einem eingeschränkten Netzwerksegment zuordnen. Es kann Änderungen des Gerätesicherheitsstatus erkennen, wie z.B. die Deaktivierung oder den Ausfall von Antiviren- oder Verschlüsselungssoftware. Die Plattform bewertet Geräte kontinuierlich neu – insbesondere dann, wenn sie dem Netzwerk beitreten oder es verlassen. Es überwacht den Gerätekontext in Echtzeit und leitet automatisch Maßnahmen ein, wie etwa das erneute Scannen von Geräten auf Schwachstellen und Angriffsindikatoren, im Zusammenspiel mit Drittanbietersystemen.

orescout kann Aktionen direkt auf dem Gerät oder über die Netzwerkinfrastruktur durchführen (siehe unten). Hostbasierte Kontrollen umfassen das Starten und Stoppen von Anwendungen, das Aktualisieren von Antivirentools, das Deaktivieren von Peripheriegeräten und Anfordern einer Anwenderfreigabe. Die Richtlinien-Engine wendet diese Vorgaben automatisch an, unabhängig vom Standort eines Geräts. Bei Bedarf kann die Forescout-Plattform Abhilfemaßnahmen wie das Patchen von Geräten oder die Neuinstallation von Schwachstellen-Analysetools, Verschlüsselungs- und Sicherheitssoftware mit Drittanbietertools orchestrieren und automatisieren (weitere Details siehe unten).

Anpassbare Geräteanalyse für Sicherheitsaktionen und Reaktionen auf Angriffe – Sicherheitsteams fehlt oft ein vollständiger Überblick über verbundene Geräte und deren Klassifizierung, Verbindungen und dem Compliance-Kontext. Dies erschwert die passende Reaktion und die vorgeschriebene Berichterstattung. Zusätzlich zur Konsole besitzt die Forescout-Plattform nun auch ein anpassbares Web-Dashboard, das Ihre Gerätelandschaft und den Compliance-Status des gesamten Unternehmensnetzwerks übersichtlich zusammenfasst. Das Dashboard arbeitet mit dem Forescout eyeManage zusammen und gewährt Einblicke in die diversen Geräte ihres vielschichtigen Netzwerks.

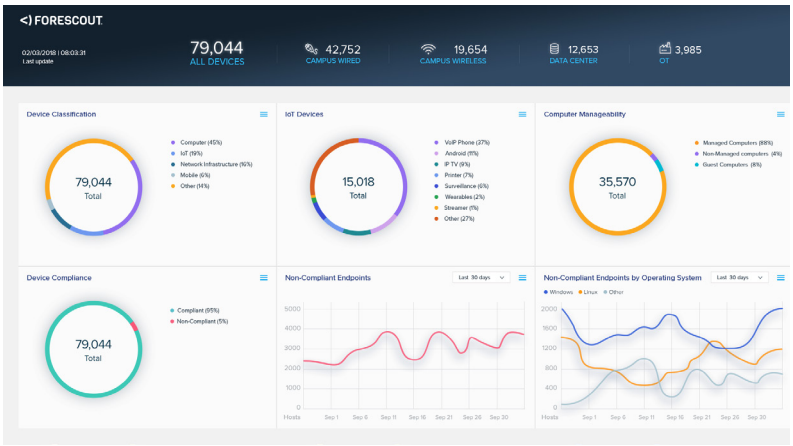

Bild 4: Konsolidierte Ansicht der Gerätelandschaft für Sicherheitszentralen.

Zero-Trust-Netzwerkmöglichkeiten

Zero-Trust-Zugriffs-Broker - Die Forescout-Plattform erzwingt die Gerätekontrolle über die Netzwerkinfrastruktur und implementiert einen zentralen Brokerage-Service und Entscheidungspunkt für die Bereitstellung von Netzwerkzugriffen. Das gelingt durch die ganzheitliche Sicht auf Benutzeridentität, Rolle, Authentifizierung und Gerätestatus. Die Plattform integriert sich nativ in Produkte von mehr als 30 Anbietern von Switches und Wireless-Geräten sowie Routern, die auf Linux laufen. Je nach Anbieter werden dazu verschiedene Techniken eingesetzt, darunter SNMP, CLI und NETCONF. Auf einem Netzwerk-Switch kann sie eine VLAN-Zuordnung ändern, eine ACL hinzufügen oder einen Port deaktivieren. Auf einem Wireless-Gerät kann sie eine MAC-Adresse sperren, die Benutzerrolle ändern oder zusätzlich die Rechte von VPN-Benutzern einschränken.

Ein wichtiger Unterschied zu anderen realen Zero-Trust-Implementierung ist, dass die agentenlose Forescout-Plattform den Zugriff auch auf alle älteren IP-Geräte entdecken, bewerten und bereitstellen kann. Forescout sieht und steuert jedes IP-Gerät und integriert sich zu 100 Prozent in die gesamte IT- und OT-Netzwerkinfrastruktur.

Ein wichtiger Unterschied zu anderen realen Zero-Trust-Implementierung ist, dass die agentenlose Forescout-Plattform den Zugriff auf alle älteren IP-Geräte entdecken, bewerten und bereitstellen kann.

Mit der Übernahme von SecurityMatters erweitert Forescout auch seine situative Netzwerküberwachung über die IT hinaus auf OT- und ICS-Umgebungen (Industrie-Netzwerke). Zu den vereinten Funktionen gehören jetzt Deep Packet Capture/Inspektion von mehr als 100 IT/OT-Protokollen, Netzwerk-Maps, Datenflussanalyse, Richtlinien- und Verhaltensüberwachung, Netzwerk-Forensik, Bedrohungsanalyse und Risikobewertung.

Dynamische Netzwerk-Segmentierung – Forescout arbeitet auch mit NG-Firewalls zusammen und liefert die Entscheidungen und Angriffspunkte für eine dynamische, richtlinienbasierte Segmentierung. Neue Firewalls können Netzwerke basierend auf Benutzer-, Geräte-, Anwendungs- und Verkehrsklassifizierung steuern. Sie nutzen den Benutzer- und Gerätekontext vieler Quellen, einschließlich der Forescout-Plattform, um detaillierte Zugriffsvorgaben auf Ressourcen präzise und flexibel durchzusetzen. Das erlaubt IT-Organisationen eine dynamische Netzwerksegmentierung zu implementieren und kontextabhängige Sicherheitsrichtlinien in ihren NG-Firewalls zu erstellen, die auf Geräte-Kontextinformationen von Forescout basieren.

Zero Trust Automations- und Orchestrierungsfähigkeiten

Die Forescout-Plattform koordiniert das infrastrukturweite Sicherheitsmanagement, damit ehemals solitäre Sicherheitsprodukte als Einheit funktionieren. Seine einzigartige Reihe von verknüpften Netzwerk-, Sicherheits- und Management-Technologien wird durch API-Integration über Forescout's eyeExtend-Produkte auf mehr als 70 Sicherheits- und IT-Managementprodukte* von Drittanbietern erweitert. Das so verknüpfte System beschleunigt die Reaktion, verbessert die Effizienz deutlich und gewährleistet eine außergewöhnlich hohe Sicherheit.

Forescout ermöglicht die Sicherheitsautomatisierung und -orchestrierung auf drei Arten:

- **Teilen von Kontext-Erkenntnissen in Echtzeit -** Forescout überwacht und teilt die Identitäts-, Konfigurations- und Sicherheitsdaten von Endgeräten kontinuierlich mit Ihren anderen Sicherheits- und Managementsystemen. Dieser bidirektionale Datenaustausch ergänzt die Möglichkeiten anderer regelbasierter Tools und verbessert Richtlinien und Aktionen.
- **Workflows automatisieren -** Forescout erlaubt über mehrere Systeme hinweg richtlinienbasierte Entscheidungen auszutauschen, was bisher eine manuelle Analyse erforderte. Die Automatisierung dieser Workflows und Prozesse führt zu einer koordinierten, sofortigen Reaktion.
- **Reaktionen automatisieren –** Viele Sicherheitstools wie hochentwickelte Bedrohungserkennungssysteme, Sicherheitsinformations-, Ereignisverwaltungs- und Schwachstellenanalysetools können das IT-Personal über Sicherheitsprobleme informieren. Forescout wendet diese Sicherheitsinformationen sofort an, um eine automatisierte Reaktion auszulösen und sein breites Spektrum an richtlinienbasierten Aktionen umzusetzen, wie zum Beispiel die Isolierung des Geräts und das Beseitigen des Problems, um den Angriff abzuwehren.

Zero Trust Workload-Fähigkeiten

Da die Forescout-Plattform physische und virtuelle Server überall in großen Netzwerken entdeckt, klassifiziert und profiliert, kann sie Workloads überwachen, die zwischen Private- und Public-Cloud-Umgebungen verschoben werden. Forescout kann alle Anwendungen jedes Servers identifizieren und sicherstellen, dass nur autorisierte Benutzer und Geräte Zugriff erhalten.

Zero Trust IAM-Fähigkeiten

Die Forescout-Plattform lässt sich in führende Verzeichnis- und IAM-Systeme integrieren, um verfügbare Benutzerdaten inklusive Rollen- und Rechtedaten zu erfassen. Es verknüpft diese Informationen mit den erfassten Daten über Gerätekonfiguration, Sicherheitsstatus und Compliance und ermöglicht Zugriffsentscheidungen, die auf Geräte- und Benutzerinformationen basieren. Das Benutzerverhalten wird kontinuierlich überwacht, und die Integration mit privilegierten Zugriffsmanagementsystemen erkennt Benutzerkonten mit nicht konformen Berechtigungen.

Zero Trust Daten-Fähigkeiten

Forescout unterstützt die Datensicherheit auf allen IP-Geräten im Netzwerk, indem es vorgeschriebene Software zur Verschlüsselung, Verschleierung und Informationssicherheit überwacht. Wenn solche Anwendungen fehlen oder inaktiv sind, kann Forescout richtlinienbasierte Maßnahmen ergreifen, wie die Benachrichtigung eines Anwenders oder Administrators sowie die Isolation des Geräts, bis es wieder instandgesetzt wird.

Starten Sie Ihren Zero-Trust-Erfolg mit umfassender Gerätetransparenz

Forescout bietet Ihnen viele Möglichkeiten, die Forescout-Plattform im Detail besser kennenzulernen:

- **Probieren Sie es aus:** Erleben Sie den Vorher-Nachher-Unterschied der Forescout-Plattform bei einem Test Drive, einem Hands-on-Probelauf, der Sie durch fünf praxisnahe Anwendungsfälle führt.
- **Buchen Sie eine Demo:** Besuchen Sie die Forescout-Webseite, um eine persönliche Demo anzufordern und weitere Informationen zu erhalten.
- **Verwenden Sie das Forescout Business Value ROI-Tool (in englisch):** Ermitteln Sie den wirtschaftlichen Gewinn, den die Forescout-Plattform Ihrem Unternehmen (berechnet nach dem Business Value Model von IDC) in nur 10 Minuten bieten kann.
- **Kontaktieren Sie uns:** Gestalten Sie Ihre Architektur gerade nach dem Zero-Trust-Modell um? Die Berater von Forescout sind gründlich geschult, erfahren und zertifiziert in den Bereichen Produktimplementierung, Prozessentwicklung und Systemintegration sowie Netzwerkzugang und Compliance-Beispielimplementierungen für Endgeräte.

*Stand: 31. Dezember 2018

*** Quellen**

1 Online Trust Alliance, Cyber Incident and Breach Trends Report, Januar 2018

2 Ponemon Institute 2017 Cost of Data Breach Study, Juni 2017, Währungsangaben umgerechnet zu einem Kurs von 1,2 U$ = 1 Euro

3 The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Januar 2018

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

E-Mail: info-dach@forescout.com
Tel (Intl): +1-408-213-3191
Support: +1-708-237-6591

Erfahren Sie mehr unter www.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-propertypatents-trademarks. Andere genannte Marken, Produkte oder Servicenamen können. Marken oder Servicemarken ihrer jeweiligen Eigentümer sein.. Version 04_19