Kontinuierliche Diagnose und Fehlerbehebung

Um ein angemessenes Niveau an Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten, müssen öffentliche IT-Organisationen eine steigende Anzahl von Gesetzen, Regulierungen und Standards einhalten. Oberstes Ziel ist es, illegales Eindringen (Vertraulichkeit) zu stoppen, sensible Daten zu schützen (Integrität) und die Risiken von Denial-of-Service-Angriffe (Verfügbarkeit) zu minimie.

Das CDM-Programm für kontinuierliche Diagnose und Fehlerbehebung ist eine dynamische Herangehensweise zur Stärkung der Cyber-Sicherheit der Netzwerke und Systeme öffentlicher Institutionen. Mit CDM verfügen Ministerien und Regierungsbehörden über Funktionen und Tools zum kontinuierlichen Identifizieren von Cyber-Sicherheitsrisiken. Dabei können Sie diesen Risiken je nach deren potenziellen Auswirkungen bestimmte Prioritäten zuweisen und Mitarbeiter im Bereich Cyber-Sicherheit so in die Lage versetzen, die wichtigsten Probleme zuerst zu lösen. Der US-Kongress hat das CDM-Programm ins Leben gerufen, um eine angemessene, risikobasierte und kosteneffiziente Cyber-Sicherheit zu gewährleisten und Cyber-Sicherheitsressourcen effizienter einzusetzen.

Die Bedingung der „kontinuierlichen" Diagnose und Fehlerbehebung in CDM bedeutet nicht notwendigerweise, dass dies rund um die Uhr geschehen muss. Vielmehr sind damit je nach Wert der Daten und dem geschätzten Risiko in bestimmten Intervallen wiederkehrende Bewertungen gemeint. Die US-Regierung stellt Richtlinien zur Bestimmung einer solchen Überprüfungsfrequenz auf der Grundlage der Sicherheitskontrollvolatilität, dem Grad der Auswirkungen auf das System in Bezug auf geschützte Funktionen und in Bezug auf sämtliche erkannten Schwachstellen bereit. Im Rahmen dieser Richtlinien wird die Detection Interval Latency (DIL) als Kennziffer definiert, um Reaktionsmaßnahmen in einem CDM-Sicherheitsprogramm zu messen und zu überprüfen.

Herausforderungen bei der Einhaltung von CDM

CDM erfordert proaktive, auf Daten konzentrierte und risikobasierte Aktionen anstelle von passiven Reaktionen und einfacher Dokumentation. In der Regel ist dafür eine erhebliche Umstellung der Sicherheitsinfrastruktur vonnöten, da Prozess- und Datenintegrationen institutionelle, daten- und systembezogene Grenzen überschreiten müssen. Im Rahmen von CDM werden zur gleichen Zeit, und nicht periodisch, Daten gesammelt, Assets verwaltet und Risiko-Managementprozesse in der gesamten Umgebung durchgeführt. Die größten technischen Herausforderungen für IT-Organisationen bestehen im Zusammenhang mit der Integration und Korrelation der kontinuierlich fließenden Daten.

Sobald neue Daten über die IT-Umgebung verfügbar werden, muss das CDM-System die Daten aufnehmen und reagieren, indem Schwellwerte angehoben und Netzwerkrichtlinien sowie Kontrollmaßnahmen in einer ununterbrochenen Feedback-Schleife angepasst werden. Zudem müssen bei CDM auch teure Sicherheitsvorgänge optimiert werden, um leitenden Beamten einen besseren Überblick über den Sicherheitsstatus und die Risiko-Managementdaten ihrer Organisation zu bieten. Eine effiziente Implementierung sollte Daten in laufenden Vorgängen sammeln, diese mit verschiedenen Kontextfaktoren korrelieren, wann immer angemessen automatische Maßnahmen ergreifen und die verbleibenden Probleme nach deren Priorität anzeigen.

CounterACT-Sicherheitsplattform

Die ForeScout CounterACT-Sicherheitsplattform bietet Monitoring- und Verwaltungsfunktionen sowie richtlinienbasierte Fehlerbehebung von verwalteten, nicht verwalteten und unkonventionellen Geräten, um als Eckpfeiler für Ihren CDM zu dienen. Und so funktioniert es:

See

- Geräte erkennen, sobald sich die mit Ihrem Netzwerk verbinden – auch ohne Agenten
- Profile zu Geräten, Benutzern, Anwendungen und Betriebssystemen erstellen und diese klassifizieren
- Verwaltete Geräte, BYOD- und IoT-Endpunkte kontinuierlich überwachen

Control

- Netzwerkzugang basierend auf Gerätestatus und Sicherheitsrichtlinien zulassen, verweigern oder einschränken
- Schädliche oder risikoreiche Endpunkte bewerten und reparieren
- Die Einhaltung von Branchenstandards und gesetzlichen Vorgaben verbessern

Orchestrate

- Kontextbezogene Information mit IT-Sicherheits- und Managementsystemen teilen
- Alltägliche Arbeitsabläufe, IT-Aufgaben und Sicherheitsvorgänge in mehreren Systemen automatisieren
- Reaktionszeiten im gesamten System verkürzen, um Risiken und Datenverletzungen schnell zu beheben

Highlights

Sichtbarkeit in Echtzeit. Erhalten Sie automatisierte Sichtbarkeit in Echtzeit von Endpunkten, sobald diese sich mit Ihrem Netzwerk verbinden. Entdecken Sie sogar heimliche Ausspähgeräte, die keine IP-Adresse verwenden.

Acitve Asset Management. Erstellen Sie ein Echtzeit-Inventar Ihres Netzwerks: Geräte, Hardware, Betriebssysteme, Anwendungen, Patch-Status, Prozesse, offene Ports, dezentrale Geräte, Benutzer und vieles mehr.

Richtlinienbasierte Zugangskontrolle. Begrenzen Sie den Netzwerkzugang von nicht autorisierten Benutzern und Geräten mit oder ohne 802.1X für Switch-Port-Sicherheit.

Kontinuierliches Monitoring. Bewerten Sie den Sicherheits- und Compliance-Status von Endpunkten in Echtzeit, bevor und nachdem diese sich mit Ihrem Netzwerk verbinden. Erkennen Sie Verletzungen von Endpunkt-Konfigurationen, schädliches Verhalten und passen Sie die jeweilige Reaktion je nach Schwere der Verletzung an.

Automatische Korrektur. Automatisieren Sie die Korrektur von nicht regelkonformen Endpunkten, indem Sie die Endpunkt-Konfiguration und die Schutzsysteme, Patches und Updates automatisch aktualisieren und Anwendungen und dezentrale Geräte installieren, aktivieren oder deaktivieren.

HBSS-Integration. Verbessern Sie Ihre situative Kenntnis und Ihre Reaktionen auf Vorfälle, indem Sie Endpunkte mit fehlenden oder nicht funktionsfähigen HBSS-Agents (Host Based Security System) automatisch erkennen und korrigieren. Lassen Sie den Netzwerkzugang basierend auf vom HBSS bewerteten Compliance-Standards zu, verweigern Sie ihn oder schränken Sie ihn ein.

Compliance-Berichte. Erstellen Sie Echtzeit-Berichte über den Status Ihrer Richtlinien-Compliance. Verkürzen Sie die Erkennungsintervall-Latenz (Detection Interval Latency, DIL), indem Sie Compliance-Scans starten, sobald sich Hosts mit dem Netzwerk verbinden, anstatt auf zeitbasierte Scans warten.

Implementationsanforderungen

Um CDM gerecht zu werden, müssen Organisationen in Echtzeit-Asset-Discovery und Schwachstellen-Management, automatisierte und datenbasierte Reaktionsmechanismen sowie kontinuierliches Feedback zu Daten in einem Unternehmens-Managementsystem investieren. Zudem muss das System leicht in Ihrem vorhandenen IT-Framework zu implementieren sein.

Ein System für Echtzeit-Asset-Discovery und Schwachstellen-Management sollte eine Kombination aus passiven und aktiven Erkennungs- und Überwachungstechniken verwenden, um Systeme im Netzwerk unabhängig von Betriebssystem oder Form zu erkennen und Profile zu diesen zu erstellen. Passive Erkennungstechniken überwachen den Datenverkehr, um zu sehen, welche Geräte aktiv sind. Aktive Erkennungstechniken überprüfen das Netzwerk, um inaktive Geräte zu erkennen. In Verbindung wird eine vollständige und konstante Sichtbarkeit der IT-Assets erreicht. Sobald jemand ein Gerät im Netzwerk installiert oder neu konfiguriert, wird diese Änderung erkannt und das Gerät überprüft. Zu guter Letzt sollte das Asset-Management-System Funktionen zum Überprüfen des Sicherheitsstatus und der Schwachstellen der Endpunkte im Netzwerk beinhalten.

Die automatisierten Reaktionsmechanismen sollten in der Lage sein, Daten vom Asset-Discovery- und Schwachstellen-Managementsystem aufzunehmen und auf Grundlage dieser Informationen und zusammen mit den Daten zum Endpunkt-Verhalten eine Reihe von raffinierten Maßnahmen ergreifen, um die Unternehmensrisiken zu verringern. Die Maßnahmen sollten je nach Schwere des Richtlinienverstoßes und/oder dem Verhalten des Endpunkts angemessen sein. Beispielsweise sollte das Reaktionssystem in der Lage sein, folgende Maßnahmen zu ergreifen:

- eine Warnung an die Person oder das entsprechende IT-Managementteam senden
- den Endpunkt automatisch reparieren oder ein Drittanbieter-System veranlassen, den Endpunkt zu reparieren
- den Netzwerkzugang einschränken
- den Netzwerkzugang blockieren

Asset-Daten und automatisierte Verwaltungsaktionen sollten an andere Komponenten des CDM-Systems weitergegeben werden, um die Effizienz des gesamten Systems zu verbessern (siehe Abb. 1). Zum Beispiel kann mithilfe von Verbindungen zwischen dem CDM-System und den SIEM-Systemen (Security Information and Event Management) des Unternehmens sichergestellt werden, dass die vom SIEM-System erstellten Compliance-Berichte genau sind.

Darüber hinaus sollte das CDM-System Informationen an agentenbasierte Systeme wie Antiviren-, Patch-Management- und MDM-Systeme (Mobile Device Management) weiterleiten, um sicherzustellen, dass diese Systeme über nicht verwaltete Endpunkte im Netzwerk informiert sind.

Zu guter Letzt sollte das CDM-System schnell und einfach zu implementieren sein. Das System sollte z. B. Folgendes bieten:

- Implementiert wird innerhalb der vorhandenen Netzwerkinfrastruktur, ohne dabei die Netzwerkinfrastruktur neu konfigurieren zu müssen.
- Eine Integration in die vorhandene Netzwerkinfrastruktur wird durchgeführt.
- Das System sollte nicht auf einer linearen Implementierung oder anderen Single Points of Failure (SPOF) basieren.
- Es ist keine Installation von zusätzlichen Endpunkt-Agenten notwendig.

Highlights (Fortsetzung)

Mobile und kabellose Verwaltung. Erkennen Sie Sicherheitsrisiken auf Mobilgeräten wie Smartphones und Tablets und setzen Sie diese durch. Setzen Sie Compliance in kabelosen Netzwerken um, indem Sie ihre Netzwerkinfrastrukur entsprechend anpassen.

Störungsfreie Bereitstellung. CounterACT kann stufenweise implementiert werden, um Störungen zu minimieren und Ergebnisse zu verbessern.

IT-Interoperabilität. Nutzen Sie die Integration in die vorhandene IT-Infrastruktur wie Verzeichnisdienste, Patch-Management-, Endpunkt-Schutz-, Schwachstellenanalyse-, SIEM- und MDM-Systeme.

ForeScout CounterACT® als Eckpfeiler für CDM

ForeScout CounterACT® wird allen Anforderungen für CDM-Systeme gerecht und kann als Kernstück Ihrer CDM-Lösung fungieren. CounterACT bietet Sichtbarkeit in Echtzeit und Verwaltung der Endpunkte in Ihrem Netzwerk, einschließlich Smartphones, Tablets, Netbooks und anderen unternehmenseigenen und privaten Mobilgeräten, die mit Ihrem Netzwerk verbunden sind.

CounterACT verwendet eine Kombination aus Erkennungstechnologien, um Endpunkte über passive und aktive Abfragetechniken exakt zu klassifizieren. Da es sich bei CounterACT um eine agentenlose Lösung handelt, funktioniert es mit einer Reihe von Endpunkten – egal, ob Cooperate Device, BYOD oder bekannt oder unbekannt sind.

CounterACT ist in der Lage, den Sicherheitsstatus von Endpunkten in Ihrer LAN-/WAN-Umgebung zu beurteilen. Dies ist von besonderer Bedeutung bei nicht verwalteten BYOD-Endpunkten, da Ihre vorhandenen Endpunkt-Managementsysteme diese Geräte üblicherweise nicht erkennen. CounterACT kann den Sicherheitsstatus von verwalteten Geräten (mit einer Domäne verbundene Computer) beurteilen, ohne dabei einen zusätzlichen Agent auf diesen Geräten zu implementieren. Dies ist ein entscheidender Faktor für die schnelle Implementierung und die einfache Handhabung des CounterACT-Systems. CounterACT kann den Sicherheitsstatus von nicht verwalteten BYOD-Geräten mithilfe der Installation eines leichten, auflösbaren Agents beurteilen. Dieser Agent unterstützt Windows®, MacOS und Linux. Er kann automatisch installiert werden, sobald sich der Benutzer mit dem Netzwerk verbindet und seine Identität auf dem System registriert. Ganz gleich ob, ein Agent verwendet wird oder nicht – CounterACT kann ein breites Spektrum von Compliance-Prüfungen durchführen, einschließlich der Überwachung der erforderlichen Programme, der Softwareversionen und Patch-Versionen, der Gerätekonfiguration sowie der Endpunktschwachstellen, um nur einige zu nennen. Es kann in führende Netzwerk-, Sicherheits- und hostbasierte Sicherheitssysteme integriert werden und Plattformen identifizieren, um Endpunkt-Informationen und Sicherheitsstatus in Echtzeit zu liefern.

ForeScout CounterACT beinhaltet ein breites Spektrum von Endpunkt-Korrekturmaßnahmen, die im Einzelnen vom Sicherheitsstatus des jeweiligen Endpunkts abhängen. CounterACT kann den Antiviren-Server veranlassen, nicht regelkonforme Hosts automatisch zu aktualisieren. Zudem kann es das Patch-Management-System veranlassen, das Betriebssystem des Geräts zu aktualisieren oder nicht autorisierte Software deaktivieren. Darüber hinaus unterstützt CounterACT führende SIEM-Systeme, um so Endpunkt-Konfigurationsdaten bereitzustellen, Zugriffs- und Compliance-Verletzungen miteinander zu korrelieren und die Reaktionen auf Vorfälle zu beschleunigen. CounterACT verfügt über eingebaute Berichte, mit denen Sie die Richtlinienkonformität überwachen, die Einhaltung gesetzlicher Bestimmungen sicherstellen und Inventarberichte in Echtzeit erstellen können.

ForeScout CounterACT ist sowohl als virtuelle als auch als physikalische Appliance erhältlich, die sich nahtlos in Ihr vorhandenes Netzwerk integrieren lässt. Dabei sind in der Regel keine Änderungen der Infrastruktur erforderlich und es ist keine Verschlechterung der Latenzwerte zu erwarten. Die CounterACT-Appliance kann im Handumdrehen installiert werden, was Latenzzeiten oder potenzielle Netzwerkausfälle vermeidet. Zudem kann sie zentral verwaltet werden, um so unzählige Endpunkte von einer Konsole aus zu steuern.

ForeScout CounterACT verwendet eine bewährte IT-Risiko-Management-Strategie. Geräte, die sich mit Ihrem Netzwerk verbinden, werden identifiziert, geprüft, korrigiert (wenn Sie möchten) und kontinuierlich verwaltet, um Compliance und Schutz zu gewährleisten. Die Compliance-Engine erkennt, wenn Geräte oder Benutzer Ihre Sicherheitsrichtlinien nicht einhalten, und spürt Benutzer mit risikoreichem Verhalten auf, etwa Benutzer, die Peer-to-Peer-Anwendungen (P2P), USB-Sticks, Smartphones nutzen und andere nicht autorisierte Aktivitäten aufweisen. Nicht regelkonforme Computer und/oder Benutzer werden in der Hauptkonsole angezeigt, einschließlich des Grunds für die Nichteinhaltung sowie Daten wie beispielsweise der Standort des Geräts.

Zu guter Letzt hilft CounterACT IT-Managern, angemessene DIL-Kennzahlen (Detection Interval Latency) zu erreichen, indem es in Compliance-Scanner integriert werden kann, um so eventbasierte Scan-Funktionen hinzuzufügen. Dank dieser Integration löst CounterACT den Compliance-Scanner aus, sobald sich ein Host mit dem Netzwerk verbindet. Die Ergänzung durch eventbasiertes Scanning wird Ihre DIL-Kennzahlen deutlich verbessern. ForeScout CounterACT kann in eine Vielzahl von führenden Schwachstellenanalyse-Scannern wie Tennable® Nessus, BeyondTrust® Retina und Qualys® integriert werden. An weiteren Integrationsmöglichkeiten wird bereits gearbeitet.

Geringere Komplexität und höhere Effizienz

In der Vergangenheit neigten IT-Sicherheitsmanager dazu, jedes einzelne Risiko mit einer bestimmten technischen Lösung zu behandeln. Gesetzliche Vorgaben wurden mit spezialisierten Kontrollen behandelt. So wurde ein angemessenes Niveau kurzfristiger Sicherheit und Compliance erreicht. Heutzutage wissen wir, dass voneinander unabhängige Sicherheitslösungen die allgemeine Komplexität erhöhen, was die Risiken vergrößert und die Personalkosten für die Verwaltung des Systems erhöht. Der Mangel an Interkonnektivität bei IT-Kontrollen ist eine zentrale Herausforderung, die es IT-Abteilungen schwer macht, Risiken effizient zu verwalten. Darüber hinaus führt dies zu schlechtem situativem Wissen und begrenzt die brauchbaren Daten für eine schnelle Erkennung von Bedrohungen und die Abschwächung von Risiken.

ForeScout CounterACT hilft bei der Lösung dieses Problems. CounterACT kann in vorhandene Systeme integriert werden, um so ein reaktionsschnelles und genaues System zum kontinuierlichen Monitoring aufzubauen, das die Komplexität verringert und mithilfe dessen Sie deutlich effizienter arbeiten können. Im Ergebnis ermöglicht das System Sichtbarkeit in Echtzeit, tiefgreifende Endpunkt-Inspektion, kontinuierliches Monitoring und automatisierte Problembehebung. Darüber hinaus kann das System in andere Sicherheits-Managementsysteme integriert und im Handumdrehen installiert werden, während die Anschaffungskosten überschaubar bleiben.

Abbildung 1: Gewünschter Status – ForeScout CounterACT bietet Sichtbarkeit für das Netzwerk in Echtzeit und teilt diese Informationen bidirektional mit Ihrer vorhandenen Betriebs- und Sicherheitsinfrastruktur.

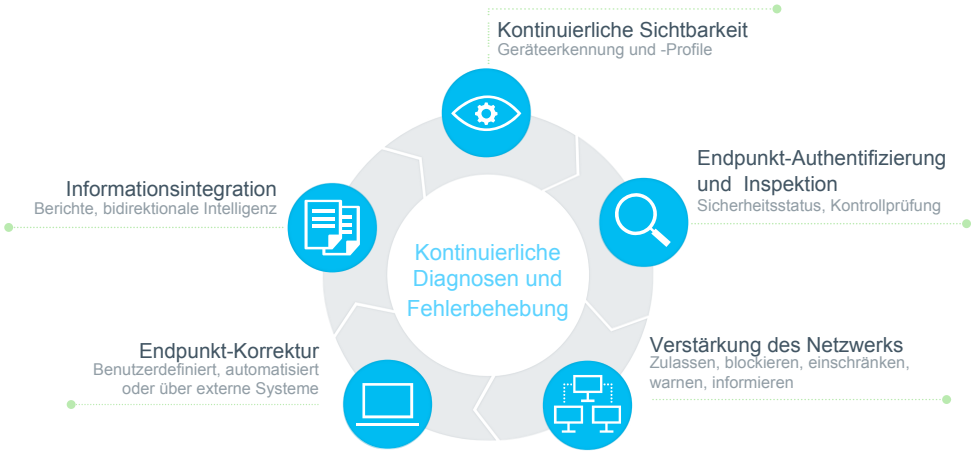

Abbildung 2: Die intelligente Sicherheitsautomatisierungsplattform von ForeScout bietet Sichtbarkeit in Echtzeit sowie automatisierte Kontrollen.

Kontinuierliche Diagnosen und Kriterien zur Fehlerbehebung[1]		ForeScout CounterACT
Erkennung und Klassifizierung von Assets	Erkennen Sie nicht autorisierte oder nicht verwaltete Hardware in einem Netzwerk und nicht autorisierte oder nicht verwaltete Softwarekonfigurationen bei IT-Assets in Ihrem Netzwerk.	CounterACT erkennt Netzwerkgeräte in Echtzeit und pflegt eine umfassende Datenbank aller Hardware- und Softwareassets. Das Inventar kann in Bezug auf mehrere Hardware- und Softwaremerkmale durchsucht und mithilfe dieser organisiert werden. Darüber hinaus können Inventarberichte erstellt werden.
Bewertung	Die Bewertung des Sicherheitsstatus eines Endpunkts für ein genaues und schnell bereitstehendes Softwareinventar ist unerlässlich für die Kenntnis und Kontrolle von Softwareschwachstellen und Sicherheitseinstellungen.	CounterACT ist in der Lage, den Sicherheitsstatus von Endpunkten in Ihrer LAN-/WAN-Umgebung zu beurteilen. Dies ist von besonderer Bedeutung bei nicht verwalteten Geräten (BYOD), da Ihre vorhandenen Managementsysteme diese Geräte üblicherweise nicht erkennen. CounterACT ist in der Lage, ein breites Spektrum an Compliance-Prüfungen durchzuführen, einschließlich des Monitorings der erforderlichen Software, der Softwareversionen und von Patch-Versionen, Gerätekonfigurationen sowie Endpunkt-Schwachstellen. Es kann in andere hostbasierte Agenten/Tools und Schwachstellen-Scannern integriert werden, um zusätzliche Compliance-Informationen zu erhalten.
Authentifizierung und Zugangskontrolle	Sie können nicht autorisierte Netzwerkverbindungen/Netzwerkzugriffe verhindern, entfernen und einschränken. So werden Angreifer davon abgehalten, interne und externe Netzwerkgrenzen auszunutzen, um diese dann zu pivotieren, einen tieferen Netzwerkzugang zu abzutasten. Weiter können sie versuchen, tiefer ins Netzwerk einzudringen und / oder Daten zu erfassen. Verwalten Sie den Zugriff auf Konten, Verhalten, Zugangsdaten und die Authentifizierung.	CounterACT ist in der Lage, den Zugriff von nicht autorisierten Geräten sowie von Geräten, die ihre Regelkonformität verlieren, während sie mit dem Netzwerk verbunden sind, zu blockieren oder einzuschränken. CounterACT ist ereignisgesteuert und bewertet einen Endpunkt neu, sobald eine Konfiguration in dessen Betriebssystem geändert wird.
Automatische Problembehebung und Korrektur	Verhindern Sie Angriffe auf das System, indem Sie es so konfigurieren, dass Schwachstellen kontinuierlich minimiert werden. Angriffsflächen sollten so klein wie möglich gehalten. Es gilt zusätzlich möglichst große Hindernisse für die Angreifer aufzubauen.	Wenn Compliance-Verletzungen erkannt werden, kann CounterACT je nach Schwere der Verletzung einfach eine Warnung senden, das IT-Team benachrichtigen, den Fehler automatisch beheben oder nicht regelkonforme Endpunkte unter Quarantäne stellen bzw. blockieren. Zudem kann es auch mit dem System eines Drittanbieters, wie beispielsweise einem Patch-Management-System, interagieren.
Verhaltensbezogene Erkennung	Der Status eines Endpunkts muss schnell und genau bestimmbar sein, um je nach Situation richtige reagieren zu können. Organisationen müssen die Verwaltung aller Geräte im Netzwerk zu jeder Zeit bewerkstelligen.	CounterACT bietet umfassende kontextbezogene Information, indem Endpunkte im Netzwerk identifiziert werden. Gleichzeitig integriert es sich in Sicherheits- Managementsysteme, wie Endpunkt-Lifecycle- Managementprodukte, Asset-Managementsysteme, Datenbanken, SIEM, VA und Antivirenprodukte, , wodurch Endpunkt-Information in Echtzeit über den jeweiligen Sicherheitsstatus kommuniziert werden können. Zudem unterstützt es SIEM-Systeme, um Daten zu Endpunkt-Konfigurationen zur Verfügung zu stellen sowie Zugriffs- und Compliance-Verletzungen miteinander zu korrelieren.

[1]Vergleichen Sie „Kontinuierliche Diagnosen und Kriterien zur Fehlerbehebung“
https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=f154da08471898c2e7a9ab05595c3df6

ForeScout ControlFabric®-Architektur

Die Verknüpfung von ForeScout CounterACT mit Ihrer CDM-Lösung ist nur eine von zahlreichen IT-Systemintegrationen, die mithilfe der ForeScout ControlFabric-Architektur möglich sind. Bei ControlFabric handelt es sich um eine offene Technologie, die es ForeScout CounterACT und anderen Lösungen ermöglicht, Daten auszutauschen und auf diese Weise ein breites Spektrum an Sicherheitsproblemen effizienter zu beheben. Weitere Informationen finden Sie unter www.forescout.com/controlfabric.

Sehen Sie sich das ForeScout-Angebot an

Sagen Sie uns, welche ForeScout-Lösung Ihren Anforderungen entspricht, und wir arrangieren eine kostenlose Evaluierung vor Ort.

Über ForeScout

ForeScout Technologies Inc. verändert Sicherheit durch Sichtbarkeit. ForeScout bietet den 2.000 weltweit größten Unternehmen und öffentlichen Institutionen die Möglichkeit, einen Überblick über Geräte genau in dem Moment zu gewinnen, in dem diese sich mit dem Netzwerk verbinden. Dies gilt auch für alle unkonventionellen Geräte Geräte. Zudem versetzt ForeScout Sie in die Lage, diese Geräte zu verwalten und die Freigabe von Daten sowie das gemeinsame Bearbeiten von Vorgängen über unterschiedliche Sicherheits-Tools hinweg zu automatisieren, um so schnellere Reaktionszeiten bei IT-Vorfällen zu erreichen. Anders als bei herkömmlichen alternativen Sicherheitslösungen sind bei ForeScout keine Softwareagenten oder Vorwissen erforderlich. Unsere Lösungen lassen sich in alle führenden Netzwerk-, Sicherheits-, Mobilitäts- und IT-Management-Produkte integrieren. So werden Sicherheitssilos überwunden und Arbeitsabläufe automatisiert, was zu erheblichen Kosteneinsparungen führt. Mehr als 2.000 Kunden in mehr als 60 Ländern verbessern ihre Netzwerksicherheit und ihren Compliance-Status mit den Lösungen von ForeScout.*

Weitere Informationen finden Sie unter www.forescout.com.

Weitere Informationen finden Sie unter **www.ForeScout.com**

ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Gebührenfrei (USA) 1-866-377-8771
Tel. (intern) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284

*Stand: Januar 2016