ForeScout CounterACT®

Monitoring, Management und richtlinienbasierte Fehlerbehebung von verwalteten, nicht verwalteten und unkonventionellen Geräten in Echtzeit.

ForeScout CounterACT® ist eine agentenlose Security-Appliance, die Netzwerkendpunkte und Anwendungen dynamisch identifiziert und bewertet, sobald diese eine Verbindung zu Ihrem Netzwerk herstellen. CounterACT identifiziert rasch den zugehörigen Benutzer, Eigentümer, das jeweilige Betriebssystem, die Geräteeinstellungen, Software, Dienste sowie den Patch-Status und es wird ermittelt, ob ein Sicherheits-Agent vorhanden ist. Darüber hinaus bietet das Produkt Funktionen zur Fehlerbehebung, Verwaltung und zum kontinuierlichen Monitoring dieser Geräte.

CounterACT führt diese Aktionen bei Geräten des jeweiligen Unternehmens, persönlichen BYOD-Endpunkten und unkonventionellen Geräten durch – ohne, dass dabei Softwareagenten oder vorherige Gerätekenntnisse erforderlich sind. Es lässt sich problemlos in Ihre vorhandene Umgebung integrieren und im Regelfall sind keinerlei Veränderungen der Infrastruktur, Upgrades oder eine erneute Konfiguration von Endpunkten erforderlich.

Darum entscheiden sich unsere Kunden für CounterACT

Heterogener Support. Funktioniert mit bekannten Netzwerkinfrastrukturen, Betriebssystemen, Endpunkt-Software und Sicherheitslösungen von Drittanbietern.

Agentenlos. Für die Authentifizierung und die Netzwerkzugangskontrolle sind keine Endpunkt-Agenten erforderlich.

Herausragende Sichtbarkeit. Sie sehen Geräte, die andere Lösungen nicht sehen können:

- Desktop-PCs, Laptops, Server, Router, Smartphones und Tablets
- kabelgebundene/kabellose LANs und Drucker
- IoT-Geräte (Projektoren, Maschinensteuerungen, IoT im Gesundheitswesen, Produktion, POS-Geräte und vieles mehr)

Automatisierte Verwaltung. Automatisieren Sie ein breites Spektrum an Aktionen:

- Netzwerkzugang basierend auf Gerätestandort und Sicherheitsrichtlinien zulassen, verweigern oder einschränken
- schädliche/gefährdete Endpunkte unter Quarantäne stellen und Fehler beheben

Schnelles Return of Investment. Implementieren Sie das System im Handumdrehen für Netzwerksichtbarkeit binnen Stunden.

Durchsetzung von Richtlinien. Sie können Netzwerkzugangskontrolle, Endpunkt-Compliance und Mobilgerätesicherheit durchsetzen.

Produktivität. Gewähren Sie jeder Person und jedem Gerät den passenden Netzwerkzugriff, ohne das dies Produktivität der Angestellten beeinträchtigt.

Zuverlässigkeit. Verbessern Sie die Netzwerkstabilität, indem Sie unbekannte Infrastruktur identifizieren und entfernen.

Kosteneinsparung. Beseitigen Sie manuelle Aufgaben, die mit dem Öffnen oder Schließen von Netzwerkports für den Gästezugang verbunden sind.

Compliance. Identifizieren Sie automatisch Richtlinienverstöße, korrigieren Sie Endpunkt-Mängel und prüfen Sie die Einhaltung von Compliance-Regeln.

Netzwerksicherheitsrisiken und Blind Spots

Der Schwerpunkt der traditionellen Netzwerksicherheit liegt auf der Abwehr externer Angriffe durch Firewalls und Intrusion-Prevention-Systeme. Diese Sicherheitstools unternehmen jedoch nichts, um Ihr Netzwerk vor der Vielzahl an inneren Bedrohungen zu schützen, die zunehmend mehr Sicherheitsvorfälle und -verletzungen verursachen. Zu den möglichen Bedrohungen gehören:

- **Besucher:** Gäste und Dienstleister bringen Ihre Computer in Ihre Firma mit. Alle benötigen einen Internetzugang. Für Serviceprovider sind unter Umständen noch zusätzliche Ressourcen erforderlich. Wenn Sie diesen Besuchern unbegrenzten Zugriff gewähren, riskieren Sie Angriffe auf Ihr Netzwerk.
- **WLAN- und mobile (BYOD) Benutzer:** Ihre Mitarbeiter wollen ihre eigenen Smartphones, Tablets und Notebook in Ihrem Netzwerk verwenden. Wenn Sie das nicht ausreichend kontrollieren, können diese Geräte Ihr Netzwerk infizieren oder zu Datenverlust führen.
- **IoT-Geräte (Internet der Dinge):** Unkonventionelle Geräte vergrößern Ihre Angriffsfläche, wenn z. B. nicht verwaltete Geräte wie IP-Projektoren, Thermostate, Beleuchtungsschalter, Sicherheitskameras und vieles mehr hinzugefügt werden.
- **Bösartige Geräte:** Mitarbeiter können Ihr Netzwerk in guter Absicht durch billige Hubs, Abteilungs-Server, Router und Wireless Access Points erweitern, die unter Umständen zur Instabilität und zu Schwachstellen in Ihrem Netzwerk führen können.
- **Malware und Botnetze:** Sobald Ihr Netzwerk infiziert ist, können verbundene Geräte für sogenannte Pivot-Angriffe verwendet werden, bei denen Außenstehende Ihr Netzwerk durchsuchen und Ihre Daten stehlen.
- **Compliance:** Falsch konfigurierte Endpunkte und virtuelle Maschinen können unangemessene Einstellungen oder Software enthalten. Darüber hinaus kann es sein, dass diese absichtlich vom Benutzer oder durch Malware deaktiviert werden, wodurch dann auch die Sicherheitskontrollen deaktiviert werden.

Sicherheit durch Sichtbarkeit

Eingeschränkte Sichtbarkeit führt zu Blind Spots in Ihrer IT. Für die Mehrheit der Endpunkt-Sicherheitssysteme müssen Sie über aktualisierte Agenten auf jedem Ihrer Geräte verfügen, um diese zu sehen und verwalten zu können. IT-Sicherheitsverantwortliche können in der Regel keine nicht verwalteten BYOD-Endpunkte erkennen und haben auch keinen Einblick in die steigende Anzahl von IoT-Geräten, die täglich mit Netzwerken verbunden werden.

So funktioniert ForeScout CounterACT®

ForeScout CounterACT bietet Ihnen die einzigartige Möglichkeit, IP-Netzwerkgeräte zu sehen, diese zu verwalten und den Austausch von Informationen und die Vorgänge unter verschiedenen Sicherheitstools zu koordinieren. Und so funktioniert es:

See. Die CounterACT-Appliance lässt sich im Handumdrehen in Ihrem Netzwerk implementieren. Danach überwacht es kontinuierlich den Netzwerkdatenverkehr und kann in Ihre vorhandene Netzwerkinfrastruktur integriert werden, um Geräte zu identifizieren, sobald sich diese mit dem Netzwerk verbinden. CounterACT verfügt über die einzigartige Fähigkeit, ein breites Spektrum an IP-Endpunkten, Benutzern und Anwendungen zu sehen. So erkennen die raffinierten Technologien von CounterACT Geräte, die für Konkurrenzprodukte unsichtbar sind.

Und CounterACT kann noch viel mehr. So klassifiziert es über passive und aktive Abfragetechnologien detailgenau Endpunkte in Ihrem Netzwerk. CounterACT ist in der Lage, den Gerätetyp, Standort und Benutzer zu identifizieren und erkennt, ob das Gerät Mitglied Ihrer Domäne ist. Zudem sammelt es zusätzliche Informationen. Darüber hinaus erhält es detaillierte Daten über den Sicherheitsstatus eines Geräts, indem es Administratorkennungen verwendet, um unternehmenseigene Geräte abzufragen.

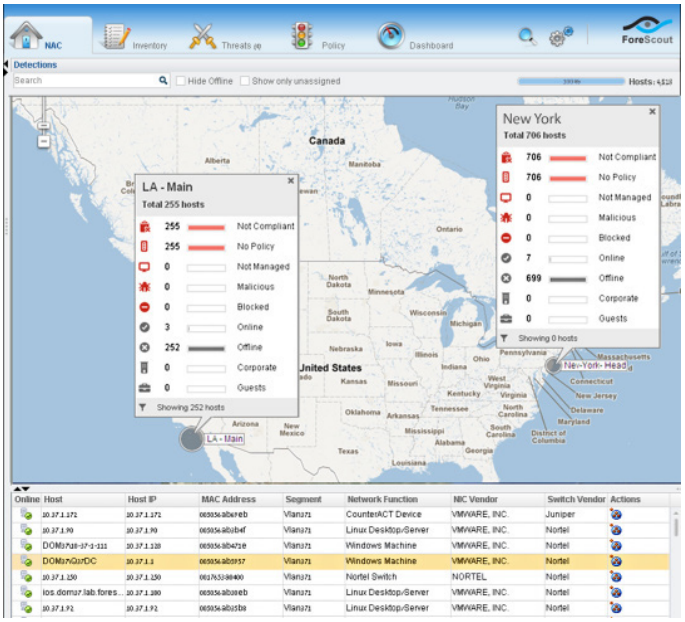

Abbildung 1: ForeScout CounterACT bietet sowohl hochwertige Übersichts- als auch Detaildaten über Geräte in Ihrem Netzwerk.

Control. Sobald CounterACT ein Sicherheitsproblem auf einem Endpunkt erkennt, kann sein raffinierter Compliance-Manager je nach Schwere des Problems automatisch eine Reihe von Maßnahmen durchführen. Bei kleineren Verletzungen wird etwa eine Warnung an den Endbenutzer gesendet. Mitarbeiter und Auftragsnehmer, die ihre eigenen Geräte mitbringen, können an ein automatisiertes Eingliederungsportal weitergeleitet werden. Ernsthafte Verletzungen führen beispielsweise dazu, dass ein Gerät blockiert oder unter Quarantäne gestellt wird, ein Sicherheits-Agent neu installiert, ein Agent oder Vorgang neu gestartet wird, ein Endpunkt veranlasst wird, ein Betriebssystem zu patchen, oder dass andere Aktionen zur Fehlerbehebung durchgeführt werden.

Analysten, Kunden und Partner entscheiden sich für CounterACT

- ForeScout hat die Auszeichnung als Leader im Gartner Network Access Control Magic Quadrant** erhalten für die Durchsetzung vollkommener Sichtbarkeit (vier Berichte in Folge).
- Beste NAC-Lösung vom SC Magazine, Juni 2015
- Beste Kaufentscheidung vom SC Magazine, Oktober 2014

„Wir brauchten eine NAC-Lösung, die wir schnell implementieren können, ohne dabei Geschäftsausfälle zu riskieren. Zudem musste diese unsere gemischte IT-Infrastruktur von Aruba® und Cisco® unterstützen. ForeScout CounterACT bot und all das und noch vieles mehr – einschließlich atemberaubender Integrationsfunktionen mit unseren vorhandenen Sicherheitstools von FireEye® und ArcSight®. Aus diesem Grund nennen wir CounterACT das ‚Schweizer Taschenmesser' unserer Informationssicherheitsabteilung, da es mehrere automatisierte Sicherheitsüberprüfungen und Compliance-Kontrollen äußerst effizient ermöglicht. "

– Ali Kutluhan Aktaş, Head of Information Security/ Risk Management bei KKB

Die Stärke der ControlFabric-Architektur

Die ControlFabric-Architektur verbindet die Funktionen von ForeScout CounterACT mit den Stärken von Netzwerk-, Sicherheits-, Mobilitäts- und IT-Managementprodukten von Drittanbietern. Es verwandelt die Sicherheits-Management-Silos in folgende Vorteile:

- ein einheitliches systemübergreifendes Sicherheitsmanagement
- bessere Effizienz bei sämtlichen Vorgängen
- Verkürzung der Reaktionszeiten bei Bedrohungen
- bessere Ausnutzung Ihrer Sicherheitsinvestitionen
- deutliche Verbesserung Ihrer Netzwerksicherheit und Ihres Compliance-Status

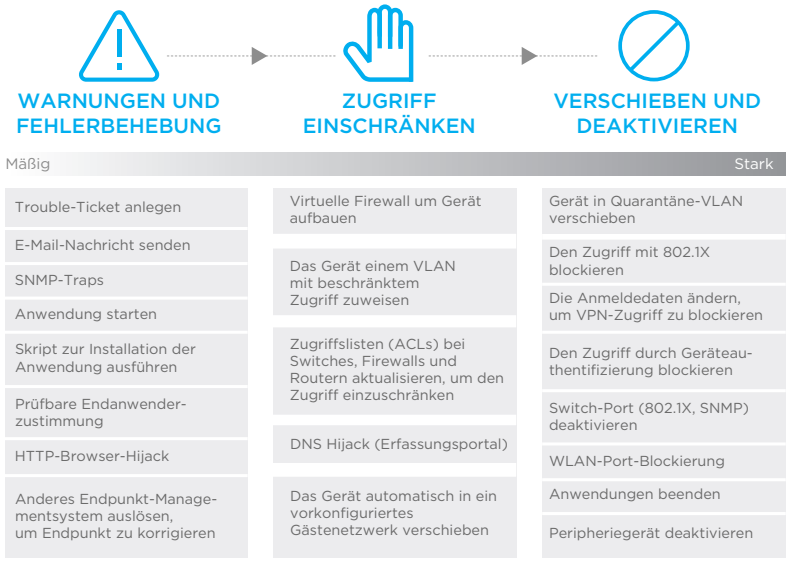

Abbildung 2: ForeScout CounterACT bietet ein volles Spektrum an Kontrollfunktionen.

Orchestrate. CounterACT nutzt die ForeScout ControlFabric®-Architektur, um den Austausch von Informationen und die Vorgänge zwischen Ihren bereits vorhandenen Sicherheits- und System-Management-Tools zu koordinieren. Dank der ControlFabric-Architektur können Sie dies mit individuellen Integrationen oder Plug-and-Play-Softwaremodulen erreichen. Die zusammen mit ForeScout-Technologiepartnern entwickelten Basismodule oder Erweiterungsmodule von ForeScout verleihen mehr als 70 führenden Netzwerk-, Sicherheits-, Mobilitäts- und IT-Management-Produkten* die Stärke von CounterACT, um:

- kontextbezogene Einblicke mit IT-Sicherheits- und Managementsystemen zu teilen,
- alltägliche Arbeitsabläufe, IT-Aufgaben und Sicherheitsvorgänge in mehreren Systemen zu automatisieren,
- Reaktionszeiten im gesamten System zu verkürzen, um Risiken und Datenverletzungen schnell zu beheben.

Merkmale

Allgemein

Spielend leichte Implementierung: CounterACT lässt sich im Handumdrehen in Ihrem Netzwerk implementieren, ohne dabei zu höheren Latenzzeiten oder potenziellen Schwachstellen im Netzwerk zu führen.

Sichtbarkeit: Die Asset-Inventarfunktion bietet eine mehrdimensionale Übersicht Sie ermöglicht die Verwaltung des Netzwerks in Echtzeit und erlaubt es Ihnen, Benutzer, Anwendungen, Prozesse, Ports, externe Geräte und vieles mehr zu verfolgen und zu verwalten (siehe Abb. 1).

Offene Interoperabilität: CounterACT funktioniert mit den bekanntesten Switches, Routern, VPNs, Firewalls, Endpunkten, Betriebssystemen (Windows®, Linux, iOS, OS X und Android), Patch-Managementsystemen, Antivirensystemen, Verzeichnissen und Ticketsystemen – ohne dass Änderungen an der Infrastruktur oder Upgrades erforderlich sind.

Audits: ForeScout CounterACT verfügt über eine voll integrierte Bericht-Engine, mit der Sie Ihr Niveau an Richtlinienkonformität überwachen, die Einhaltung gesetzlicher Bestimmungen sicherstellen und Inventarberichte in Echtzeit erstellen können.

Skalierbarkeit: ForeScout kann auf herausragende Erfolge bei Kundennetzwerken mit mehr als 1.000.000 Endpunkten verweisen. Die CounterACT-Appliances sind in einer Vielzahl von Größen erhältlich.

Zertifizierungen: CounterACT ist mit den folgenden Zertifizierungen klassifiziert:

- USMC Authority to Operate (ATO)
- U.S. Army CoN (Certificate of Networthiness)
- UC APL (Unified Capabilities Approved Product List)
- Common Criteria Evaluation Assurance Level (EAL) L4+

Ohne Betriebsstörungen: Das Implementieren ist ohne negative Auswirkungen für Benutzer oder Geräte möglich. Wenn Sie eine automatisierte Kontrolle einsetzen wollen, können Sie das stufenweise tun, wobei Sie mit den größten Problembereichen beginnen und passende Durchsetzungsmaßnahmen wählen.

Verwaltung von Richtlinien: Erstellen Sie für Ihr Unternehmen passende Sicherheitsrichtlinien. Konfiguration und Verwaltung können dank der integrierten Richtlinienvorlagen, Regeln und Berichte schnell und einfach durchgeführt werden.

ControlFabric-Architektur: Die ControlFabric®-Architektur bietet umfangreiche Interoperabilität mit Drittanbieterprodukten und eine offene Integrationsarchitektur.

Endpunkt

Agentenlos: Identifizieren, klassifizieren, authentifizieren und verwalten Sie den Netzwerkzugriff ohne Agenten. Außerdem kann eine umfassende Endpunkt-Inspektion ohne Agenten durchgeführt werden, solange CounterACT Administratorzugriff auf den Endpunkt hat. In Situationen, in denen CounterACT nicht über Administratorzugriff verfügt (wie bei BYOD), kann eine umfassende Inspektion mithilfe unseres optionalen SecureConnector-Agents durchgeführt werden, der ohne Aufpreis in CounterACT enthalten ist.

Endpunkt-Compliance: Stellen Sie sicher, dass Endpunkte in Ihrem Netzwerk konform mit Ihrer Virenschutzrichtlinie sind, die neuesten Patches besitzen und keine unerlaubte Software aufweisen. CounterACT Identifiziert automatisch Richtlinienverstöße, korrigiert Endpunkt-Sicherheitsmängel und prüft die Einhaltung von Compliance-Regeln.

Erkennung von Bedrohungen: Dank dem kontinuierlichen Monitoring erhalten Sie schnellere und exaktere Einblicke als bei Point-in-Time-Schwachstellenscans, da manche Geräte sich nicht konstant im Netzwerk befinden.

Erkennung von Schadgeräten: Entdecken Sie schädliche Infrastruktur wie nicht autorisierte Switches und Wireless Acccess Points. CounterACT kann sogar Geräte ohne IP-Adressen erkennen wie beispielsweise getarnte Paketerfassungsgeräte, die vertrauliche Daten stehlen können.

Zugriff

Gästeregistrierung: Erlauben Sie Ihren Gästen, auf Ihr Netzwerk zuzugreifen, ohne dass dadurch die interne Netzwerksicherheit gefährdet wird. Dank mehrerer Gastregistrierungsoptionen können Sie den Zulassungsprozess für den Gästezugriff ganz an die Bedürfnisse Ihres Unternehmens anpassen.

Rollenbasierter Zugriff: CounterACT stellt sicher, dass nur die richtigen Personen mit den richtigen Geräten Zugriff auf die richtigen Netzwerkressourcen erhalten. Es nutzt Ihr vorhandenes Verzeichnis, in dem Sie Rollen den Benutzeridentitäten zuweisen.

Flexible Verwaltung: Im Gegensatz zu altmodischen NAC-Produkten, die schwerfällige Kontrollfunktionen verwenden und Benutzer behindern, bietet CounterACT ein volles Spektrum an Durchsetzungsoptionen, mit denen Sie Ihre Reaktion an die jeweilige Situation anpassen können. Als Reaktion auf Verstöße mit niedrigem Risiko können Sie eine Nachricht an den Endbenutzer senden oder das Sicherheitsproblem automatisch beheben. So kann der Benutzer produktiv bleiben, während das Problem gelöst wird (siehe Abb. 2).

802.1X-Authentifizierung – mit oder ohne: Sie haben die Wahl zwischen der 802.1X-Authentifierung und anderen Authentifizierungstechnologien wie LDAP, Active Directory®, RADIUS®, Oracle® und Sun. Der Hybridmodus ermöglicht die gleichzeitige Verwendung mehrerer Technologien, was die NAC-Implementierung in umfangreichen, vielfältigen Umgebungen beschleunigt.

Eingebauter RADIUS: Ein integrierter RADIUS-Server erleichtert die Einführung von 802.1X. Sie können auch bestehende RADIUS-Server nutzen, indem Sie CounterACT als RADIUS-Proxy konfigurieren.

Skalierbare Modelle

CounterACT kann auf herausragende Erfolge bei Kundennetzwerken mit mehr als 1.000.000 Endpunkten verweisen. Es ist verfügbar als Palette von physikalischen und virtuellen Appliance-Optionen, um den individuellen Bedürfnissen Ihres Unternehmens gerecht zu werden. Große Netzwerke, die mehrere Appliances erfordern, können über den CounterACT Enterprise Manager zentral verwaltet werden. Jede CounterACT-Appliance enthält eine permanente Lizenz für eine bestimmte Anzahl von Netzwerkgeräten. Weitere Informationen zu unseren Lizenzrichtlinien erhalten Sie unter www.forescout.com/licensing.

Zentrale Verwaltung und Kontrolle

Der CounterACT Enterprise Manager kann für die zentrale Verwaltung und Kontrolle der CounterACT-Implementierungen sowohl als physikalische als auch als virtuelle Appliance bereitgestellt werden. Er überwacht die Aktivitäten und Richtlinien von CounterACT und sammelt Informationen zu schädlichen Aktivitäten in allen Appliances sowie bei von CounterACT durchgeführten Identifikationen, Benachrichtigungen, Einschränkungen und Fehlerbehebungen. Diese Informationen können in der CounterACT-Konsole angezeigt und protokolliert werden.

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

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.
**Gartner, Inc., „Magic Quadrant for Network Access Control", Lawrence Orans und Claudio Neiva, 10. Dezember 2014. Gartner empfiehlt keinen der Anbieter, keins der Produkte oder keine der Dienstleistungen, die in unseren Forschungsberichten erwähnt werden und rät nicht, ausschließlich solche Anbieter zu wählen, die die höchsten Wertungen oder andere Auszeichnungen erhalten haben. Die Forschungsberichte von Gartner stellen die Meinungen der Forschungsabteilung von Gartner dar und sollten nicht als Tatsachenfeststellungen interpretiert werden. Gartner schließt alle ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich dieser Studie inklusive Tauglichkeit oder Eignung für einen bestimmten Zweck aus.