FROST & SULLIVAN

Kontinuierliches Monitoring und Bedrohungsabwehr mit Next-Generation NAC

Ein Frost & Sullivan Whitepaper

HÄUFIGE LÜCKEN IN DEN NETZWERKSICHERHEITSSTRATEGIEN

Die herkömmlichen Sicherheitspraktiken verlieren zunehmend an Wirkung. Sicherheitslösungen wie Antivirus (AV), Verschlüsselung, Data Leakage Prevention (DLP), Patch-Management und Schwachstellenanalysen (Vulnerability Assessment, VA) gehen in der Regel davon aus, dass alle Endpunkte in einem Netzwerk ordnungsgemäß verwaltet werden, mit Sicherheitsagenten ausgestattet sind und statisch im Netzwerk verbleiben (also nicht nur gelegentlich verbunden sind) – problematische Annahmen angesichts der heutigen Realitäten wie Bring-Your-Own-Device (BYOD), Unternehmens-IoT (Internet der Dinge) und mobile Computernutzung.

Hinzu kommt, dass die meisten konventionellen Sicherheitstools als Insellösungen bereitgestellt werden und nicht darauf ausgelegt sind, mit anderen Produkten zusammenzuarbeiten. Herkömmliche Sicherheitstools wie VA- und Intrusion-Detection-/Intrusion-Prevention-Systeme (IDS/IPS) dienen sehr spezifischen Zwecken. VA-Tools scannen Endgeräte auf Fehlkonfigurationen und Anfälligkeiten für bekannte Sicherheitslücken. IDS/IPS-Systeme geben Warnungen aus, wenn eine potenzielle Sicherheitsverletzung am Perimeter entdeckt wird. Die Lösungen zum Schutz des Netzwerkperimeters erfüllen ihre individuellen Aufgaben gut. Doch vielfach tauschen sie keine kontextbezogenen Informationen mit anderen Sicherheitstools aus und bieten keine nativen Kontrollen zur Entschärfung von Bedrohungen. Dieser isolierte Ansatz lässt Blind Spots entstehen und stellt eine enorme Belastung für die Sicherheitsmitarbeiter dar, die manuell auf Sicherheitswarnungen reagieren müssen.

Network Access Control (NAC) ist eine Technologie, die bereits seit fast zwei Jahrzehnten existiert. Sie ist also gut etabliert, erlebt derzeit aber einen enormen Aufschwung: Frost & Sullivan prognostiziert für den Zeitraum von 2013 bis 2018 eine Expansion des weltweiten NAC-Markts mit einer jährlichen Wachstumsrate (CAGR) von 30 Prozent.1 NAC-Engines erkennen und erstellen ein Profil sämtlicher Endpunkte, die sich mit dem Unternehmensnetz verbinden. NAC-Lösungen erfreuen sich aktuell großer Beliebtheit, da sie BYOD-, mobile und IoT-Geräte gleichermaßen sichtbar und transparent machen können. Hier haben konventionelle Plattformen für Unternehmenssicherheit ihre Probleme. Sobald ein Endpunkt erkannt wird, kann die NAC-Lösung ihn überprüfen und dann Richtlinien auf ihn anwenden. So kann sie zum Beispiel Geräte in ein kleineres Netzwerksegment verschieben, in dem die Endnutzer nur wenige Berechtigungen haben. Die NAC-Hersteller machen sich diesen Vorteil zunutze, um einen Gesamtüberblick über die Sicherheitsaufstellung der Endpunkte sowie Netzwerk-Mapping zu bieten. NAC ist zudem in der Lage, Endpunkte durchgehend zu verwalten und Richtlinien für Endpunkte rollenbasiert durchzusetzen. Bi-direktionale Integrationen mit anderen Sicherheitslösungen erlauben es, den Perimeterschutz zusätzlich zu verstärken. NAC-Tools sehen oft Dinge, die der Perimeter-Abwehr entgehen.

Dieses Whitepaper beschreibt NAC-Technologie und zeigt insbesondere, wie NAC kontinuierliches Monitoring und die Entschärfung von Bedrohungen ermöglicht. Zudem erläutertes, was die Plattform ForeScout CounterACT™ von anderen NAC-Produkten auf dem Markt unterscheidet: Sie benötigt keine Agenten und funktioniert sowohl mit als auch ohne 802.1 X.

UMFRAGE ZUR SICHTBARKEIT UND TRANSPARENZ VON NETZWERKEN

Im Auftrag von ForeScout führte Frost & Sullivan im Zeitraum von August bis September 2015 eine Umfrage unter IT- und Sicherheitsfachleuten durch. Die Umfrage sollte in Erfahrung bringen, wie diese Fachkräfte über die Sichtbarkeit und Transparenz von Netzwerken, Tools, Bedrohungserkennung und Incident-Response denken.

Aus der Frost & Sullivan Studie, Analysis of the Global Network Access Control (NAC) Market, Dezember 2014

Um eine globale Perspektive zu erhalten, wurden IT- und Sicherheitsfachleute aus den USA, Großbritannien und Deutschland befragt, die in großen Unternehmen tätig sind. Die Teilnehmerzahlen und Kriterien für die Unternehmensgröße sahen wie folgt aus:

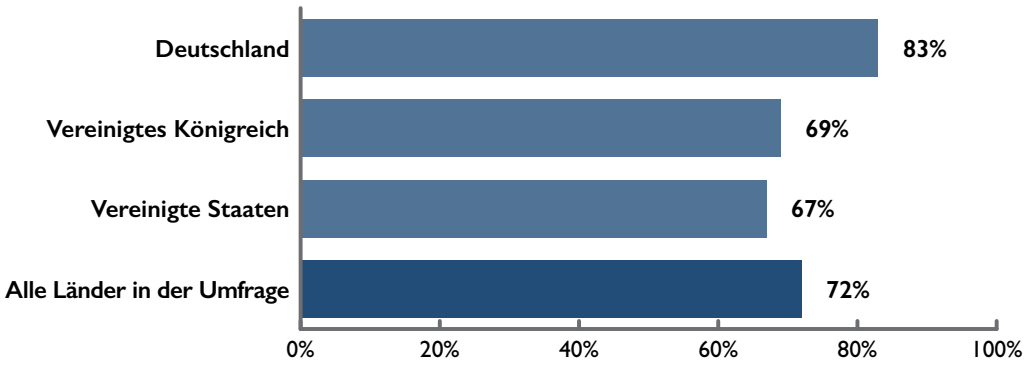
- **Deutschland (100 Antworten).** In Deutschland kamen die Teilnehmer aus Unternehmen, die mindestens 4.000 Mitarbeiter beschäftigen oder zu den Global 2000 gehören.
- **UK (100 Antworten).** Im UK kamen die Teilnehmer aus Unternehmen, die mindestens 4.000 Mitarbeiter beschäftigen oder zu den Global 2000 gehören.
- **US (201 Antworten).** In den USA kamen die Teilnehmer aus Unternehmen, die mindestens 10.000 Mitarbeiter beschäftigen oder zu den Global 2000 gehören.

DIE WICHTIGSTEN ERGEBNISSE DER UMFRAGE ZUR SICHTBARKEIT UND TRANSPARENZ VON NETZWERKEN

Ein Teil der Fragen in der Untersuchung bezog sich auf Sicherheitsverletzungen und die Wirksamkeit bestimmter Tools für Netzwerksicherheit. So wurden die IT-Fachleute gefragt, wie viele Sicherheitsvorfälle sich in den vergangenen zwölf Monaten in ihrem Unternehmen ereignet hatten, aufgegliedert nach spezifischen Netzwerkkomponenten. Diese Netzwerkkomponenten waren: verwaltete Computer von Endnutzern, verwaltete Server, unverwaltete BYOD-Geräte, Smartphones/Tablets, Nicht-Computer (IoT), physisches Eindringen sowie Netzwerkeinbruch.

Die Ergebnisse gaben Anlass zur Besorgnis. Rechnet man alle Netzwerkkomponenten zusammen, ereigneten sich in den letzten zwölf Monaten in 72 Prozent aller Netzwerke fünf oder mehr Sicherheitsvorfälle.

Abb. 1. Prozentsatz der Netzwerke, in denen sich in den letzten zwölf Monaten mindestens fünf Sicherheitsvorfälle ereigneten



Source: Network Visibility Study, Frost & Sullivan, October 2015

Ein näherer Blick auf die Daten macht deutlich, dass keine Netzwerkkomponente wirklich sicher ist. Angesichts des Prozentsatzes von Unternehmen, die für die einzelnen Kategorien von Netzwerkkomponenten mindestens fünf Sicherheitsereignisse melden, wird eine Botschaft mehr als deutlich: Sowohl verwaltete als auch unverwaltete (BYOD) Netzwerkkomponenten bieten ausnutzbare Einfallstore zu den Netzen.

Abb. 2. Gemeldete Sicherheitsvorfälle in den letzten zwölf Monaten

Netzwerkkomponente	Deutschland	UK	USA	Total
Verwaltete Computer von Endnutzern	50%	19%	31%	31%
Verwaltete Server	36%	19%	27%	27%
Unverwaltete BYOD-Geräte/Computer von Partnern	36%	17%	21%	21%
Smartphones oder Tablets	42%	17%	23%	23%
Nicht-Computer (Drucker, IoT etc.)	34%	19%	24%	24%
Physisches Eindringen (z.B. gestohlene Medien)	16%	12%	18%	18%
Netzwerkeinbruch (z.B. Wi-Fi-Angriff)	21%	12%	19%	19%
Q. Wie viele Sicherheitsvorfälle ereigneten sich in Ihrem Unternehmen im letzten Jahr bei (Netzwerkkomponente)? Antworten mit mindestens fünf Vorfällen im letzten Jahr.				

Source: Network Visibility Study, Frost & Sullivan, October 2015

Es sei noch einmal betont, dass in den hier dargestellten Resultaten nur Meldungen von fünf oder mehr Sicherheitsereignissen berücksichtigt sind. Bei verwalteten Endnutzer-Computern war die Zahl der verzeichneten Sicherheitsereignisse durch die Bank hoch, und in Deutschland erklärten sogar sage und schreibe 50 Prozent der Befragten, dass es in ihrem Unternehmen fünf oder mehr Sicherheitsereignisse gegeben habe. Das sind alarmierende Resultate, doch es gibt eben auch zahllose Faktoren, die zu Sicherheitsverstößen führen können. Netzwerksicherheitsumgebungen basieren auf der Annahme, dass Server und Endgeräte-Agenten richtig konfiguriert sind. Treten aber doch Fehler in der Konfiguration auf, können Endpunkte im Netzwerk verlorengehen, ohne dass das Sicherheitsteam dies bemerkt (die Umfrage-Ergebnisse zum Thema Endpunkt-Agenten werden etwas weiter unten beschrieben).

Die Zahlen erscheinen durchwegs hoch – fünf Sicherheitsvorfälle bei einer einzigen Kategorie von Netzwerkkomponenten in einem Jahr ist eine Menge. Da Netzwerksicherheitstechnologien häufig als isolierte Insellösungen arbeiten, lässt sich keine Art von Rechner leicht absichern. Und angesichts der Evolution der Netzwerkarchitekturen ist dieses Resultat verständlich. Noch vor sieben, acht Jahren waren Netzwerkarchitekturen darauf ausgelegt, PCs zu unterstützen, die über Ethernet an ein lokales Netz angeschlossen waren. Heute sind Laptops und Tablets nahezu ausschließlich transiente Geräte. Und private, öffentliche und hybride Cloud-Infrastrukturen erhöhen die Komplexität der Netzwerke noch zusätzlich.

Die Teilnehmer wurden gefragt, ob es in ihren Netzen einen „signifikanten“ Blind Spot gibt, der durch bestimmte Technologieplattformen verursacht wird. Die Antworten zeichnen ein ziemlich klares Bild. Unabhängig von der Region oder Technologie gaben die IT- und Sicherheitsadministratoren an, dass es in ihren Netzwerken signifikante Blind Spots gibt (s. Abb. 2). Somit lässt sich aus der Umfrage schließen, dass bessere Sichtbarkeit und Transparenz erforderlich ist und dass die Technologien miteinander kommunizieren müssen, um die Blind Spots auszuräumen.

Viele Fragen in der Untersuchung waren nicht quantitativ, sondern qualitativ ausgerichtet. Dabei wurde eine Skala von 1 bis 7 verwendet, bei der „1“ nicht signifikant bedeutete und „7“ sehr signifikant (zudem konnte auch die Antwort „Ich weiß nicht“ gegeben werden).

Abb. 3. In den Netzwerken gibt es im Hinblick auf die Sicherheit eine Reihe von Blind Spots

Netzwerksicherheitstechnologie	Deutschland	UK	USA
Schwachstellenanalyse	38%	32%	44%
Firewall	45%	38%	44%
Network Intrusion Prevention	38%	29%	37%
Advanced Threat Detection	46%	35%	36%
SIEM	39%	31%	38%
Mobile Device Management (MDM)	37%	30%	39%
Endgeräteschutz (Antivirus)	37%	33%	35%
Patch- und Konfigurationsmanagement	41%	29%	34%

Gibt es in Ihrem Netzwerk einen signifikanten Blind Spot aufgrund (Netzwerksicherheitstechnologie)? Zusammengefasste Prozentsätze der Antworten mit „6“ und „7“ auf einer siebenstufigen Skala.

Source: Network Visibility Study, Frost & Sullivan, October 2015

Die zunehmende Komplexität der Netzwerk- und Informationssicherheit belastet die ohnehin überforderten Sicherheitsteams noch zusätzlich. Die meisten Unternehmen geben an, dass sie zu wenige IT-Sicherheitsmitarbeiter haben. Es scheint daher sinnvoll zu sein, die manuellen Aufgaben durch Automatisierung zu reduzieren, doch stellt sich die Frage, inwieweit das Sicherheitspersonal willens ist, Möglichkeiten der Automatisierung auch zu nutzen. Deshalb wurden die Umfrageteilnehmer gefragt: „Wie sehr würde Ihr Netzwerk profitieren, wenn eine Reihe vorgegebener Sicherheitskontrollen (Netzwerksicherheitstechnologien) automatisch aufgerufen werden könnten?“ Die Antworten auf diese Frage sind eine klare Ansage an die Anbieter von Sicherheitslösungen, ihre Produkte stärker zu automatisieren (s. Abb. 4 .) Idealerweise möchten die IT- und Sicherheitsteams die Einstellungen anpassen können; jedoch muss ein Sicherheitstool out-of-the-box effektiv arbeiten und auch dann noch effektiv bleiben, wenn es in einer mehrschichtigen Cyber-Abwehrarchitektur mit anderen Tools integriert wird.

Abb. 4. Netzwerke würden von automatisierten Sicherheitskontrollen profitieren

Netzwerksicherheitstechnologie	Deutschland	UK	USA
Schwachstellenanalyse	53%	58%	67%
Firewall	65%	65%	69%
Network Intrusion Prevention	56%	62%	70%
Advanced Threat Detection	62%	56%	67%
SIEM	57%	50%	66%
Mobile Device Management (MDM)	54%	48%	68%
Endgeräteschutz (Antivirus)	50%	58%	73%
Patch- und Konfigurationsmanagement	59%	52%	65%

Wie sehr würde Ihr Netzwerk profitieren, wenn eine Reihe vorgegebener Sicherheitskontrollen (Netzwerksicherheitstechnologien) automatisch aufgerufen werden könnten? Zusammengefasste Prozentsätze der Antworten mit „6“ und „7“.

Source: Network Visibility Study, Frost & Sullivan, October 2015

Viele Sicherheitsadministratoren nutzen Sicherheits- und Management-Agenten, um die Endpunkte in ihren Netzwerken zu verfolgen. Ein Agent ist eine kleine Applikation, das auf einem Endpunkt installiert wird und diesen mit dem Unternehmensnetz assoziiert. Der Einsatz von Agenten hat den Vorteil, dass ein Endpunkt vom Netzwerk leichter erkannt wird und die Kommunikation zwischen dem Endpunkt und dem Netzwerk vereinfacht wird, zum Beispiel bei Software-Updates.

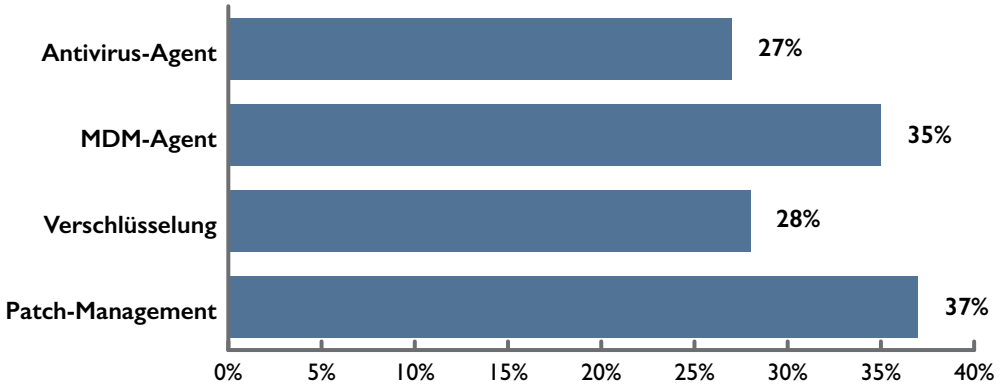
Allerdings werfen Agenten drei erhebliche Probleme auf. Das erste Problem ist, dass die meisten Cyber-Sicherheitstools eine auf „Polling" basierende Scantechnologie anwenden. Üblicherweise führen Schwachstellenmanagement-Lösungen, SIEM-Systeme (Security Information and Event Management) und andere Cyber-Technologien semi-permanente Scans durch. Für statische Geräte, die via Ethernet mit einem Netzwerk verbunden sind, eignet sich dieses Verfahren gut. Wenn sich aber zunehmend mobile Geräte mit den Netzen verbinden, kann zwischen den einzelnen Abrufen viel geschehen. Geräte, die nur ab und an im Netz sind, werden leicht übersehen. Außerdem können Agenten falsch konfiguriert oder deaktiviert sein. Unternehmensnetze sind oftmals dynamische Umgebungen. Endpunkte werden häufig neu konfiguriert, Standorte werden aufgegeben oder hinzugefügt. Wenn ein Agent nicht richtig funktioniert, geht dem Netzwerk die Sichtbarkeit und Transparenz über das Endgerät verloren, und die Sicherheit steht auf dem Spiel.

Das zweite Problem bei der Nutzung von Sicherheitsagenten besteht darin, dass die von den IT-Teams benötigten Agenten auf einer wachsenden Anzahl von persönlichen (BYOD) und IoT-Geräten im Unternehmensnetz gar nicht erst installiert werden können. Abhängigkeit von Agenten bedeutet somit, dass das Netzwerk genau das Segment von Endpunkten im Unternehmensnetz nicht erkennt, das am schnellsten wächst, und sich folglich das Sicherheitsniveau verschlechtert.

Das dritte Problem schließlich ist, dass ein falsches Gefühl von Sicherheit entstehen kann, wenn man sich auf Sicherheitsagenten verlässt. In der Frost & Sullivan-Umfrage zur Sicherheit und Transparenz von Netzwerken wurden die teilnehmenden Sicherheitsfachleute gefragt, wie sehr sie den installierten Agenten für Virenschutz, MDM (Mobile Device Management), Verschlüsselung und Patch-Management in ihren Netzwerken vertrauen.

Gemäß der Skala bedeuten „6" und „7" großes beziehungsweise äußerstes Vertrauen in die installierten Agenten. Nachfolgend sind jedoch diejenigen Antworten dargestellt, in denen Werte von 1 bis 5 ausgewählt wurden, die also besagen, dass das Vertrauen nicht optimal ist.

Abb. 5. Geringes Vertrauen, dass die Sicherheitsagenten korrekt installiert sind und richtig arbeiten



Source: Network Visibility Study, Frost & Sullivan, October 2015

Zu wissen, was sich im Netzwerk befindet und wie die Beziehungen zwischen allen Infrastrukturgeräten und Endpunkten aussehen, ist ein Grundpfeiler der Netzwerksicherheit. Die Daten aus der Umfrage zeigen jedoch, dass es Unternehmen an echter Sichtbarkeit und Transparenz der Geräte fehlt, die sich mit ihren Netzen verbinden. Geräte, die nur zeitweilig verbunden sind, haben die Spielregeln im Hinblick auf die Verwundbarkeit von Netzwerken grundlegend verändert. NAC bietet Sichtbarkeit und Transparenz von Endpunkten, Netzwerksegmentierung und Zugangskontrolle – die grundlegenden Sicherheitseigenschaften, die für eine erfolgreiche Cyber-Abwehr in der heutigen vernetzten Realität erforderlich sind.

NEXT-GENERATION NAC LÖST DAS PROBLEM DER BLIND SPOTS IM NETZWERK

Next-Generation NAC erkennt, überprüft und verwaltet dynamisch alle Geräte, die sich mit dem Netzwerk verbinden – egal, ob kabelgebunden oder drahtlos – und stellt sicher, dass die verwalteten Endpunkte die Sicherheitsrichtlinien einhalten. Der Nutzen von Next-Generation NAC geht also weit über die einfache Zugangskontrolle hinaus, die frühere NAC-Lösungen boten. Heute minimiert NAC die Angriffsfläche, die unsichere, kompromittierte oder schädliche Geräte, unbefugte Nutzer und unerwünschte Anwendungen darstellen, und verringert auf diese Weise die Risiken für das Unternehmen.

NAC ermöglicht Sichtbarkeit und Transparenz und kann die Problembehebung für Endpunkte auch da einleiten, wo agentenbasierte Lösungen dies nicht können, zum Beispiel bei mitarbeitereigenen und IoT-Geräten. Zur letzteren Kategorie gehören beispielsweise Drucker, Industrieausrüstung, Überwachungssysteme und medizinische Geräte – kurz, alles in einem Unternehmensnetz, was sich nicht mit einem Agenten verwalten lässt. NAC-Lösungen kategorisieren diese Geräte und platzieren sie in Netzwerksegmenten mit unterschiedlichen Zugangsrichtlinien. Diese Segmentierung und Abriegelung von Netzwerkbereichen reduziert die Sicherheitsrisiken, die kompromittierte Geräte für den Rest des Netzes darstellen. Wenn ein Gerät kompromittiert ist, kann ein Angreifer Authentifizierungsverfahren untergraben, um auf sensible Daten zuzugreifen oder Angriffe zu starten. Einige Next-Generation NAC-Systeme bieten auch Funktionen zum Monitoring des Datenverkehrs. Sie können verdächtige Aktivitäten von unverwalteten und IoT-Geräten erkennen und diese in Quarantäne verlegen, damit sich Bedrohungen nicht im Netz ausbreiten können.

Auch Bring-Your-Own-Device (BYOD) ist ein wichtiges Anliegen für viele Unternehmen, die die Mobilität ihrer Mitarbeiter gewährleisten müssen, gleichzeitig aber maximale Flexibilität bei der Gerätewahl ermöglichen und die Sicherheitsrisiken minimieren wollen. MDM-Systeme (Mobile Device Management) erfordern die Installation von Software auf jedem mobilen Gerät, was für die Endnutzer und das IT-Personal mehr Komplexität und Aufwand bedeutet. Eine Kombination aus NAC und MDM ermöglicht Sichtbarkeit und Transparenz, Verwaltung und detaillierte Kontrolle für alle Geräte, die Verbindung zum Netzwerk aufnehmen wollen, und sichert damit BYOD-Strategien ab.

In der von Frost & Sullivan durchgeführten *2015 ISC² Global Information Security Workforce Study*, für die 13.930 Sicherheitsfachleute befragt wurden, wurden zwei Fragen gestellt, die die Herausforderungen bei der Integration neuer Technologien in das Framework der Netzwerksicherheit beleuchten:

1. Verursacht die Absicherung neuer Technologien, die Ihr Unternehmen einführt (zum Beispiel BYOD, soziale Medien), erheblichen Zeitaufwand? **50 Prozent der Teilnehmer antworteten mit Ja.**

2. In welchen Bereichen der Informationssicherheit sehen Sie in den nächsten drei Jahren einen wachsenden Schulungs- und Weiterbildungsbedarf? **47 Prozent der Teilnehmer antworteten, dass BYOD zusätzliche Schulungsmaßnahmen erforderlich machen wird.**

Das offensichtlichste Werteversprechen von Next-Generation NAC mögen zwar Zugangskontrollen, Sichtbarkeit und Transparenz der Netzwerke, kontinuierliches Monitoring und die Überprüfung des Sicherheitsniveaus von

Endpunkten sein, doch es mag noch mehr in ihnen stecken, als es auf den ersten Blick den Anschein hat. Eine gute Plattform mit intuitiven Dashboards kann dazu beitragen, künftige Kosten für die Schulung und Fortbildung der Mitarbeiter sowie für Wartung und Monitoring zu reduzieren.

NEXT-GENERATION NAC LÖST DAS PROBLEM DER ZEITWEILIG VERBUNDENEN GERÄTE

Wie bereits ausgeführt, sind die meisten bestehenden IT-Sicherheits- und IT-Management-Systeme für statische Endpunkte optimiert. Da konventionelle Netzwerksicherheitssysteme davon ausgehen, dass die Endpunkte im Netzwerk statisch sind, scheint semi-permanentes Scannen/Monitoring eine vernünftige Option zu sein. So werden beispielsweise Schwachstellenanalysen meist periodisch durchgeführt, zum Beispiel einmal monatlich oder einmal wöchentlich. In der heutigen Welt entsteht bei periodischen Scans jedoch das Problem, dass in den Intervallen zwischen den einzelnen Scans leicht ein Laptop übersehen werden kann, das sich immer nur kurzzeitig im Netzwerk befindet.

NAC-Lösungen ermöglichen Ein- und Übersicht über die Endpunkte in Echtzeit, und diese Fähigkeit können IT-Teams nutzen, um alle Geräte, die Verbindung aufnehmen, kontinuierlich zu überwachen. So ist gewährleistet, dass die Geräte von Mitarbeitern und autorisierten Gästen stets den Sicherheitsrichtlinien entsprechen. Monitoring und Überprüfung der Geräte sorgt dafür, dass die erforderlichen Sicherheitsprogramme, Patches und Konfigurationssoftware vorhanden, aktiv und auf dem neuesten Stand sind.

NAC-Richtlinien sind flexibel und können so gesetzt werden, dass der Nutzer, der Helpdesk oder das Sicherheitsteam sofort über bekannte Probleme und Sicherheitsverletzungen informiert werden; dass nicht konforme Endpunkte in Quarantäne gestellt werden; oder dass die Problembehebung direkt auf dem Endpunkt in Gang gesetzt wird. Diese Fähigkeit zur unverzüglichen Reaktion und richtlinienbasierten Korrektur ist eine entscheidende Voraussetzung, um Anfälligkeiten zu minimieren und ein breites Spektrum an Sicherheitsproblemen rasch zu entschärfen. Next-Generation NAC bietet flexible, richtlinien- und netzwerkbasierte Mechanismen zur Überprüfung und Kontrolle von Endpunkten, um Sicherheitsrichtlinien bei der Verbindungsaufnahme und danach durchzusetzen. Diese fortschrittlichen Technologien schützen Unternehmensnetze auf folgende Weise:

- **Identifikation von Endpunkten ohne Einsatz von Agenten.** Next-Generation NAC kann ohne Agenten alle mit dem Netzwerk verbundenen Geräte in Echtzeit identifizieren, Profile erstellen und die Geräte überwachen. Das gilt auch für Geräte von Mitarbeitern und Gästen sowie IP-fähige Geräte, die keine Software-Agenten unterstützen, zum Beispiel Drucker und Überwachungssysteme.
- **Erkennung.** Next-Generation NAC erkennt unautorisierte Geräte, unautorisierte Wireless Access Points und unverwaltete Legacy-Systeme und kann sie entfernen.
- **Zugangskontrolle.** Mithilfe von Richtlinien für die Zugangskontrolle kann das IT-Team unternehmenseigene mobile Geräte verwalten und mobile Geräte von Mitarbeitern in Gast-VLANs verlegen.
- **Netzwerk-Awareness.** Da Next-Generation NAC-Lösungen umfassende Sichtbarkeit und Transparenz des Netzwerks ermöglichen, können sie Geräte und Systeme in Echtzeit inventarisieren. Sie sind nicht nur anwendungsbewusst, sondern können unerwünschte oder unautorisierte Anwendungen auch deaktivieren, zum Beispiel Instant Messaging und Peer-to-Peer (P2P) Filesharing-Programme, die auf einem System laufen.

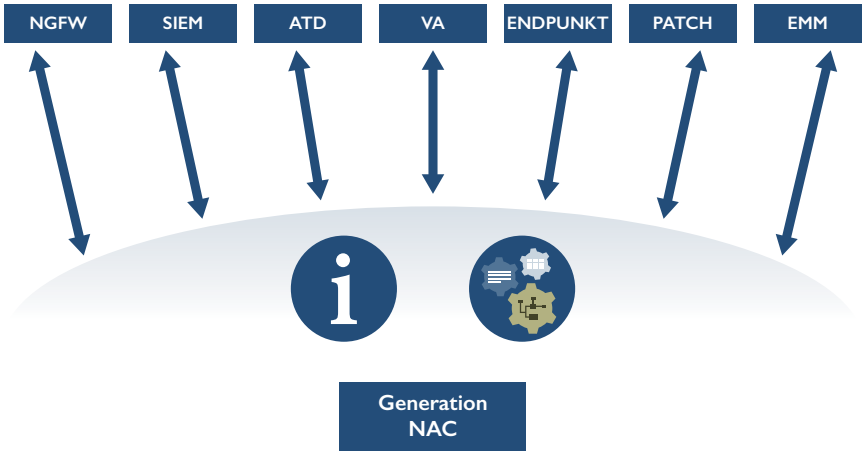
- **Validierung von Sicherheitsagenten.** Next-Generation NAC-Lösungen dienen der doppelten Kontrolle, indem sie gewährleisten, dass Sicherheitslösungen wie Virenschutz, Patch-Management, Verschlüsselung und Tools zur Systemaktualisierung installiert, aktiviert und aktuell sind.
- **Kontinuierliches Monitoring auf Sicherheit und Compliance.** Einer der Hauptvorteile von Next-Generation NAC ist das kontinuierliche Monitoring von Endpunkten, das es erlaubt, Anzeichen für eine Kompromittierung oder Nichteinhaltung von Richtlinien zu erkennen.
- **Alarme und Warnmeldungen.** Next-Generation NAC ist ein ausgesprochen proaktives Tool. Das Sicherheitsteam kann auf Verletzungen der Richtlinien reagieren: durch Protokollierung, Alarme, Zugangsbeschränkungen, Blockaden und Quarantänemaßnahmen. Danach kann die NAC-Lösung genutzt werden, um die Probleme auf den Endgeräten zu beheben.
- **Plattform-Integrationen.** Next-Generation NAC-Tools arbeiten mit Virenschutz-, MDM-, SIEM- (Security Information and Event Management) und ATD- (Advanced Threat Detection) Systemen sowie sonstigen Tools zusammen, die das Gesamt-Sicherheitsniveau eines Unternehmens verbessern.

NEXT-GENERATION NAC LÖST DAS PROBLEM DER SICHERHEITSSILOS

Die Fähigkeit, sich bi-direktional mit verschiedensten Systemen zu integrieren, wie etwa Next-Generation Firewalls (NGFW), Schwachstellenmanagement, Mobile Device Management, Data Leakage Prevention, Virenschutz, Konfigurationsmanagement und Security Information and Event Management (SIEM), ist ein wesentliches Differenzierungsmerkmal von NAC. Wenn eine NAC-Lösung Informationen über die Endgeräte im Netzwerk gesammelt hat, kann sie diese an andere Sicherheitstools übermitteln. Ebenso kann NAC selbst Informationen von diesen Tools empfangen. Die Policy Engine der NAC-Lösung und der anderen Sicherheitstools profitieren erheblich von gemeinsamer Ein- und Übersicht. Zum Beispiel kann das NAC-Tool ermitteln, ob nötige Updates installiert wurden und ein Desktop-Management-System über diese Richtlinienverletzung informieren. Umgekehrt kann ein Schwachstellenscanner oder eine hochentwickelte Lösung zur Bedrohungserkennung anfällige oder kompromittierte Geräte ermitteln und die NAC-Lösung verständigen, damit die betroffenen Geräte repariert oder isoliert werden.

Dank der bi-direktionalen Integration kann NAC zudem die Rolle des vertrauenswürdigen Dritten übernehmen, der die Sicherheit der Systeme überwacht und verifiziert und dadurch gewährleistet, dass die Kontrollen und gewünschten Veränderungen umgesetzt werden. IT-Teams berichten, dass eine NAC-Management-Konsole weitaus genauere und umfassendere Daten liefert als die Management-Konsolen von Plattformen für Netzwerksicherheit und Konfigurationsmanagement-Systemen. Besonders wichtig ist, dass die Integration mit Verzeichnisdiensten, Wireless- und MDM-Systemen die NAC-Plattform in die Lage versetzt, die Identifizierung, Registrierung und Problembeseitigung für persönliche und mobile Geräte zu automatisieren. Die bi-direktionalen Integrationsmechanismen befähigen Next-Generation NAC-Lösungen also, eine symbiotische Beziehung mit den vorhandenen Sicherheitstools des Kunden einzugehen, um ein breites Spektrum an Aufgaben für Monitoring und Risikominimierung durchzuführen.

Abb. 6. Integrationen von Next-Generation NAC mit anderen Sicherheitstechnologien



Source: ForeScout, Frost & Sullivan

NEXT-GENERATION NAC PASST SICH AN IT-GRC-FRAMEWORKS AN

Die leistungsstarken und flexiblen Kontrollen, die eine Next-Generation NAC-Plattform bietet, verstärken nicht nur den dynamischen Schutz, sondern lassen sich auch nutzen, um Compliance-Vorgaben zu erfüllen. Kontinuierliche Ein- und Übersicht sowie Problembehebung für Endpunkte sind notwendig, um ein breites Spektrum von IT-Governance-, Risikomanagement- und Compliance- (GRC) Anforderungen einzuhalten und die Einhaltung nachzuweisen. Dazu zählen gesetzliche Vorschriften und Branchenstandards wie der Federal Information Security Management Act (FISMA), Continuous Diagnostics and Mitigation (CDM), der Payment Card Industry Data Security Standard (PCI DSS), die NERC-Standards (North American Electric Reliability Corporation), der Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act (HITECH) sowie der Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG). All diese Bestimmungen definieren erforderliche Sicherheitspraktiken wie Vergabe von Zugangsberechtigungen und Netzwerkisolierung, Monitoring der Integrität und Konformität von Endpunkt-Konfigurationen, Beseitigung von Bedrohungen und Ereignisprotokollierung. IT-Teams in Unternehmen können einer Reihe verschiedener IT-GRC-Rahmenwerke und Regulierungsanforderungen gerecht werden, indem sie die folgenden Fähigkeiten von Next-Generation NAC nutzen:

- **Hostbasierte Systemsicherheit (HBSS).** Mit Funktionen für Ein- und Übersicht für Endgeräte sowie der Integration mit Lösungen für Schwachstellenanalyse und HBSS-Suites adressiert NAC Vorgaben, wonach Geräte richtig konfiguriert, gescannt und vor Schwachstellen geschützt werden müssen. Dabei werden aktive HBSS-Suites eingesetzt, wie in PCI DSS, HIPAA und DISA STIG beschrieben.

- **Problembehebung bei Endgeräten.** Die automatisierte Behebung von Problemen bei Endgeräten entspricht den Anforderungen an Problembehebung und Endpunkt-Sicherheit gemäß PCI DSS, National Institute of Standards and Technologies (NIST) und Gramm-Leach-Bliley Act (GLBA).

- **Zugangskontrollen.** Die in PCI DSS, DISA STIG, GLBA und NERC beschriebenen Anforderungen hinsichtlich einer portbasierten Zugangskontrolle erfüllt NAC durch die Unterstützung für 802.1X-Authentifizierung sowie zusätzliche Authentifizierungsmechanismen in Netzwerk-Umgebungen, die 802.1X nicht unterstützen.

- **Unterstützung für Prüfpfade.** Die Integration mit SIEM- und Log-Management-Tools trägt dazu bei, die Forderungen von PCI DSS, GLBA und NERC nach soliden Prüfpfaden sowie Monitoring der Benutzerzugriffe auf sensible Daten und Systeme zu erfüllen.
- **Systemkontrollen für Daten und Geräte.** NAC befähigt die IT-Teams, noch weitere Anforderungen zahlreicher Regulierungsstandards zu erfüllen, wie zum Beispiel Kontrolle mobiler Geräte, Entfernung nicht autorisierter Zugangspunkte sowie Einführung von Programmen, die eine Preisgabe von Daten verhindern.

Next-Generation NAC unterstützt auch Kontrollen für ein breites Spektrum anderer IT-GRC-Frameworks und sicherheitsrelevanter Best-Practices. So können NAC-Funktionalitäten zum Beispiel auf die Critical Security Controls (CSCs) angewandt werden, die das Council on CyberSecurity pflegt. Die CSCs sollen Hilfestellungen bei der Implementierung einer effektiven Architektur für Netzwerksicherheit bieten. Sie beschreiben sicherheitsrelevante Best-Practices wie die Inventarisierung autorisierter und unautorisierter Geräte und Software, sichere Konfigurationen für Hardware und Software, laufende Beseitigung von Schwachstellen, Kontrolle drahtloser Geräte, Malware-Abwehr, Perimeter-Abwehr und Pflege und Überwachung von Audit-Logs.

Unternehmen, die die Vorschriften nicht einhalten, müssen mit empfindlichen Geldbußen und sonstigen Sanktionen rechnen. Daher ist es von großem Wert, Auditoren demonstrieren zu können, dass die Regelkonformität laufend geprüft werden kann. NAC überwacht diese Kontrollen und Geräte kontinuierlich in Echtzeit und dient damit als externes Verifizierungssystem: ein ergänzender Kontrollmechanismus, der Audit- und Bewertungsprozesse unterstützt.

SO UNTERSTÜTZT FORESCOUT COUNTERACT™ DYNAMISCHE EIN- UND ÜBERSICHT UND PROBLEMBEHEBUNG BEI ENDPUNKTEN

ForeScout ist ein führender, innovativer Anbieter auf dem NAC-Markt. ForeScout CounterACT™ ist eine Next-Generation NAC-Plattform für Großunternehmen und adressiert zahlreiche Sicherheitsrisiken, mit denen die Kunden konfrontiert sind. Sie bietet Zugangskontrolle für Mitarbeiter und Gäste, Sichtbarkeit und Transparenz von Netzwerken in Echtzeit, Sicherheit für mobile Geräte sowie Compliance und Problembehebung für Endgeräte.

Die Plattform CounterACT kann in kleinen und mittelgroßen Unternehmen eingesetzt werden, ist jedoch für Großunternehmen optimiert. Große Unternehmen und Behörden haben spezielle Erfordernisse in Hinblick auf zusätzliche Funktionalitäten und Verwaltung. ForeScout arbeitet mit zahlreichen bedeutenden Integrationspartnern zusammen und kann in vielen Fällen eine Plug-and-Play-Lösung bieten, die im Rahmen eines bestehenden Cyber-Abwehr-Programms unverzüglich nutzbar ist. CounterACT lässt sich schnell vor Ort implementieren, und seine Dashboards sind einfach zu handhaben. ForeScout unterstützt seine Sicherheitsprodukte mit häufigen Software-Upgrades und einem engagierten Kundendienst.

AGENTENLOSER BETRIEB SCHÜTZT DURCHGEHEND SÄMTLICHE GERÄTE

ForeScout CounterACT arbeitet ohne Agenten und erfasst wichtige Sicherheitsdaten zu sämtlichen Geräten, die mit dem Netzwerk verbunden sind. Dadurch kann CounterACT Richtlinien auch auf diejenigen Geräte anwenden, die keinen installierten Agenten unterstützen oder vom IT-Team nicht verwaltet werden. Dazu zählen beispielsweise mitarbeitereigene Geräte und IoT-Geräte des Unternehmens.

ECHTZEIT-FUNKTIONALITÄTEN UND BRANCHENFÜHRENDE AUTOMATISIERUNG

ForeScout CounterACT macht sich schnell bezahlt, da die IT-Administratoren ein umfassendes Echtzeit-Inventar aller mit dem Netz verbundenen Geräte und ihrer wichtigen Eigenschaften erhalten. Dann kann CounterACT genutzt werden, um Sicherheitsrichtlinien für nicht-konforme Geräte zu erstellen und durchzusetzen. Mithilfe der automatisierten Reaktionen, die CounterACT ermöglicht, lassen sich hochgradig sichere Richtlinien durchsetzen oder die Arbeitsabläufe des IT-Helpdesks vereinfachen.

FORESCOUT CONTROLFABRIC™

Über ForeScout ControlFabric kann sich ForeScout CounterACT mit anderen IT-Lösungen integrieren, um Informationen auszutauschen und Sicherheitsrisiken effizienter zu entschärfen. Diese Integrationen tragen dazu bei, das zuvor geschilderte Problem der Sicherheitssilos zu lösen.

ForeScout ControlFabric bietet offene Schnittstellen wie SYSLOG, SQL, Lightweight Directory Access Protocol (LDAP) und Web Services API, die eine sichere, bi-direktionale Kommunikation ermöglichen. Diese Schnittstellen, mit deren Hilfe Hersteller und Kunden ihre eigenen Integrationen entwickeln können, ergänzen weitere Integrationen, die ForeScout für gängige Infrastruktur-Komponenten entwickelt hat – so etwa Verzeichnisse, Virtual Private Networks (VPN), Next-Generation Firewalls, Virenschutz- und Patchmanagement-Systeme –, sowie Integrationen mit IT-Sicherheitstechnologien wie VA-, MDM-, ATD- und SIEM-Systemen. Zum Zeitpunkt der Abfassung dieses Papers integriert sich ForeScout mit mehr als 70 verschiedenen IT-Sicherheitsprodukten und Diensten.

Die folgende Fallstudie illustriert, wie ForeScout großen IT-Abteilungen hilft, ihre Programme für Sicherheitsmonitoring und Risikomanagement zu verbessern und zu erweitern.

FINANZINSTITUT WÄHLT FORESCOUT COUNTERACT, UM SEINE SICHERHEITSVERFAHREN ZU VERBESSERN

Ein Dienstleister aus dem Finanzsektor arbeitet seit rund vier Jahren mit ForeScout und seiner Plattform CounterACT. Es handelt sich dabei um ein großes, international agierendes Unternehmen mit Sitz in den USA.

CounterACT kann zur Umsetzung zahlreicher unterschiedlicher Ziele eingesetzt werden, doch für dieses Finanzinstitut lag der Hauptfokus auf der Verbesserung des Sicherheitsniveaus. Das Unternehmen integriert NAC mit Sicherheitslösungen verschiedener Art. Zu Sicherheitszwecken hat es eine Next-Generation Firewall (NGFW), SIEM sowie ein fortschrittliches System zur Erkennung von Bedrohungen im Einsatz. Zur Verbesserung der Sichtbarkeit, Transparenz und Anwendungskontrolle hat das Finanzinstitut CounterACT über ForeScout ControlFabric mit McAfee ePolicy Orchestrator (ePO) integriert.

Große Unternehmen haben den Vorteil, über separate Response Teams zu verfügen. Wenn eine NAC-Lösung beispielsweise mit einem SIEM-System integriert wird, kann sie mithilfe von Basisberechnungen feststellen, ob es auf einem Endpunkt Veränderungen gegeben hat. Weichen diese Veränderungen von den üblichen Mustern im Datenverkehr ab, kann ein Alarm ausgelöst werden. Wenn ein verifizierter Alarm eingeht, kann das Desktop-Response-Team den Vorfall isolieren und das betroffene Gerät und die Ports innerhalb von 5-10 Minuten in Quarantäne setzen. (Übrigens: Wenngleich das Cyber-Abwehr-Netz des Finanzinstituts zahlreiche verschiedene Technologien und Dashboards umfasst, stellte der IT-Verwantwortliche fest, dass die Risikomanagement-Analysen in CounterACT zusätzlichen Nutzen erbrachten.)

COUNTERACT ERMÖGLICHT SICHTBARKEIT UND TRANSPARENZ DER ENDPUNKTE UND DIE BEWERTUNG DER SICHERHEITSAUFSTELLUNG

Ein Unterschied zwischen ForeScout und anderen NAC-Lösungen ist, dass ForeScout ohne 802.1X-Protokolle auskommt – wenngleich 802.1X ein häufig verwendetes Protokoll ist und ForeScout auch dieses hervorragend unterstützt. Für das Finanzinstitut beschränkt sich die Sichtbarkeit und Transparenz der Endpunkte nicht nur auf den Endpunkt selbst; auch die Switches und Router, mit denen die Geräte im Netzwerk verbunden sind, müssen sichtbar und transparent sein. Das Finanzinstitut hat ein hybrides Netzwerk, in dem mehrere verschiedene Protokolle verwendet werden. CounterACT hat in diesem heterogenen Netzwerk keine Probleme, da die Lösung neben 802.1X unter anderem auch Erkennung ohne Agenten, MAC-Adressen-Routing sowie das Simple Network Management Protocol (SNMP) unterstützt.

Zu den Aspekten der Sichtbarkeit und Transparenz von Endpunkten zählen kontinuierliches Monitoring und die Isolierung von Endpunkten in verschiedenen Server- und Betriebssystem-Umgebungen. Das Finanzinstitut verfügt über Sicherheitsteams, die für die Einhaltung der Compliance-Vorgaben und den Sicherheitsstatus der Endgeräte verantwortlich sind. So werden zum Beispiel in UNIX- und Windows-Umgebungen unterschiedliche Sicherheitserwägungen angewandt. Die NAC-Lösung ist in der Lage, Endpunkte sofort zu erkennen und die Konfigurationsdetails zu bewerten: Beispielsweise werden die Windows-Registrierungseinstellungen überprüft, um dafür zu sorgen, dass die Endgeräte den Vorschriften entsprechen.

Um zu gewährleisten, dass der Sicherheitsstatus der Endpunkte in dieser Installation gewahrt bleibt (oder um Alarm zu schlagen, falls er kompromittiert ist oder sich zu verschlechtern beginnt), kann CounterACT™ Folgendes leisten:

- Jeden Endpunkt alle paar Stunden neu überprüfen.
- Redundanz im Hinblick auf das Patch-Management und die Konfiguration bieten. In einem Fall wurde ein Patch auf den Endgeräten verteilt, jedoch unvollständig installiert, da beim MAC-Routing die Switches und Umgebungen nicht richtig zugeordnet wurden. Während das Patch-Management-System anzeigte, dass die Patches eingespielt waren, ergab eine kurze Überprüfung der Endpunkte durch die NAC-Lösung, dass die Patches nie auf diesen angelangt waren.
- Wenn ein neues Gerät ins Netz kommt, verständigt CounterACT ein Schwachstellenanalyse-Tool, um einen Scan zu veranlassen.
- CounterACT stellt die Geräte in unterschiedlichen Teilen des Netzwerks bereit. Laptops, die an die Mitarbeiter ausgegeben werden, sind mit voreingestellten Sicherheitseinstellungen versehen und entsprechen dem festgelegten Sicherheitsniveau. BYOD-Geräte werden in einen anderen Teil des Netzwerks umgelenkt.

> *“Manche NAC-Lösungen liefern bei der Überprüfung der Endgeräte Erkenntnisse über Betriebssystem- und Software-Updates, Patches und Schwachstellenmanagement. So dienen sie in gewissem Maß als Backup (Redundanz) für das Patchmanagement,VM und SIEM.”*

COUNTERACT™ VERBESSERT COMPLIANCE

Vom Gesundheitssektor vielleicht einmal abgesehen, müssen die Banken und Finanzinstitute in den USA die größte Zahl an Compliance-Auflagen einhalten. Große Finanzinstitute unterliegen einem breiten Spektrum an Vorschriften. Die Konformität muss durch Audits und Berichterstattung nachgewiesen werden. Compliance

erstreckt sich auf gesetzliche Bestimmungen, behördliche Vorschriften und spezifische Branchenstandards. Die Einhaltung der Compliance-Standards kann mühsam sein. So schreibt etwa das National Institute of Standards and Technology (NIST 800 Rev 53.4) vor, dass Regierungsbehörden jeden Monat eine Bestandsaufnahme aller Geräte, Betriebssysteme und Anwendungen in ihren Netzwerken vornehmen müssen.

Das Finanzinstitut übermittelt die Informationen, die die NAC-Plattform liefert, zur Compliance-Berichterstattung und zu forensischen Zwecken an das SIEM-System. Die Sichtbarkeit und Transparenz des Netzwerks ist in diesem Zusammenhang von entscheidender Bedeutung. Die NAC-Lösung kann dem SIEM-System melden, welchen Nutzergruppen ein Endnutzer/Endgerät angehört, auf welche Switches und Ports ein Endpunkt/Gerät zugreifen wollte und welche Anwendungen auf jedem Endpunkt installiert sind. Die Compliance-Berichte werden dann primär von den SIEM- und Log-Management-Tools generiert.

Die NAC-Lösung liefert den Compliance-Plattformen Informationen, ist selbst jedoch nicht das Hauptinstrument für die Compliance-Berichterstattung. Um Compliance in stark regulierten Branchen zu demonstrieren, werden vorwiegend SIEM-Tools eingesetzt. Wichtig ist jedoch, dass die Abstimmung mit dem SIEM-System für Redundanz sorgt im Hinblick auf die Sichtbarkeit und Transparenz von Geräten, Infrastrukturen, Netzwerk-Mapping, Bewertung der Endpunkt-Aufstellung und Anwendungen auf einem Endpunkt.

MITTELSTÄNDISCHER HERSTELLER NUTZT FORESCOUT COUNTERACT ZUR ZUSAMMENFÜHRUNG DER KOMMUNIKATION

Ein mittelständischer Hersteller ist seit drei Jahren Kunde von ForeScout. Er betreibt einen großen Vertriebskanal. Seine Produkte sind sowohl online als auch in Fachgeschäften erhältlich.

Der Mittelständler stellte spezifische Anforderungen an eine NAC-Lösung. Sie musste genügend Schutzvorteile für seine großen Produktionsstätten, Regionalniederlassungen, die Personalabteilung und Verwaltung sowie 70 Außenstellen bieten. Das Netzwerk weist eine Reihe subtiler Besonderheiten auf. Zum Beispiel nutzen die Mitarbeiter-PCs und die VoIP-Telefone von Cisco denselben Ethernet-Port. Wird der Zugriff auf diesen Port gesperrt, ist der Zugriff für die PCs und Telefone ebenfalls gesperrt. Der Kunde benötigte auch Zugangskontrolllisten (ACL) und VLAN-Kontrollen.

Das Unternehmen wünschte sich eine NAC-Lösung, die sich für VPNs, kabelgebundene und kabellose Systeme eignete. 802.1X war zwar eine Option, die dieser Kunde aber nicht anstrebte, weil eine Implementierung ohne 802.1X Vorteile im Hinblick auf leichte Bereitstellung hatte, bessere Sichtbarkeit und Transparenz bot und eine Lösung ohne Agenten größere Flexibilität und detailliertere Kontrolle ermöglichte.

Ein Problem, das das Wachstum von NAC bislang hemmte, besteht darin, dass eine NAC-Lösung bei schlechter Implementierung versehentlich das Netzwerk lahmlegen kann. Wenn der Zugang zum Netz nicht mehr möglich ist, kann das logischerweise Probleme verursachen, die von einem mittleren Ärgernis bis hin zu einer absoluten Katastrophe reichen. Dieser Kunde deutete an, dass er als Hersteller – wenn er denn zwischen zwei inakzeptablen Ergebnissen wählen müsste – eher einen Einbruch ins Netzwerk riskieren würde als einen Stillstand der Produktion.

DURCHSETZUNG VON RICHTLINIEN MIT COUNTERACT™

Der Hersteller verglich ForeScout CounterACT mit anderen NAC-Systemen und kam er zu dem Schluss, dass die Policy Engine von CounterACT die leistungsfähigste war. Der Netzwerkadministrator konnte Warnmeldungen konfigurieren und hatte mehrere Optionen zur Auswahl, um Geräte in andere VLANs zu

verschieben oder den Zugang zu verweigern. Die IT-Abteilung wollte Richtlinien schreiben, die verschiedene Eventualitäten einbezogen. CounterACT bietet hier die größte Flexibilität.

> *"ForeScout CounterACT war binnen einer Woche in Betrieb und bot uns dabei die Option, je nach Bedarf weitere Abstimmungen vorzunehmen."*

Das Unternehmen stellt ein kommerzielles Produkt her, das sowohl online als offline vertrieben wird. Deshalb muss das Unternehmen unter anderem nachweisen, dass es den PCI-DSS-Standard einhält. Die Compliance-Berichterstattung stellte den Hersteller zunehmend vor Probleme. Die Plattform ForeScout CounterACT übernahm diese Aufgaben.

Sicherheit, Sichtbarkeit und Transparenz der Endgeräte zählen für diesen Hersteller nicht zu den obersten Prioritäten. Dennoch stellte er nach der Installation der NAC-Plattform fest, dass sie im Hinblick auf diese Aspekte einen Zusatznutzen erbrachte. Sie gewährleistet nicht nur Sichtbarkeit und Transparenz aller Endpunkte, sondern auch des Netzwerks, aller Ports, Betriebssysteme und Anwendungen. Der Kunde hatte die umfangreichen Funktionen, die CounterACT zur Überprüfung des Sicherheitsstatus von Endpunkten bietet, zwar nicht erwartet, begrüßte sie aber, weil sie sich auch zur Behebung anderer potenzieller Sicherheitsprobleme nutzen lassen.

Was in der Diskussion über NAC (und andere Sicherheits- und Softwareprodukte für Unternehmen) oft untergeht, ist die Frage, wie lange die physische Implementierung dauern wird. Angebote von Mitbewerbern von ForeScout sahen einen mindestens dreiwöchigen Installationszyklus vor, und die Plattform musste alle sechs Monate neu angepasst werden. Die Lösung von ForeScout war dagegen in weniger als einer Woche betriebsbereit und bot dabei die Option, dass bei Bedarf weitere Abstimmungen vorgenommen werden können.

Auch die Skalierbarkeit war ein wichtiger Aspekt. ForeScout punktete mit seiner Policy Engine, der Compliance-Berichterstattung und den im Vergleich zu anderen Produkten schnellen Installationszeiten. Der Hersteller stellte fest, dass vergleichbare NAC-Systeme diverse Workarounds oder extensive Konfiguration erforderten, um die Sicherheitsrichtlinien korrekt auf VPN-Verbindungen anwenden zu können. CounterACT war ganz einfach die flexiblere Plattform.

FAZIT

Die Fähigkeiten von NAC haben sich in den letzten Jahren in schnellem Tempo weiterentwickelt. Was NAC zu leisten vermag, beschränkt sich längst nicht mehr auf grundlegende Entscheidungen über den Zugang zu Netzwerken, bei denen Blockieren oder Zulassen die beiden einzigen Optionen sind. Next-Generation NAC liefert in Echtzeit umfassende Ein- und Übersicht über sämtliche Geräte, die mit dem Netzwerk verbunden sind. Diese Ein- und Übersicht ist mit herkömmlichen Sicherheits- und Endpunkt-Management-Lösungen nicht erreichbar. Next-Generation NAC wird bereits von großen Unternehmen mit Tausenden oder Hunderttausenden von Geräten und verteilten Netzwerken genutzt, um Sicherheitsrisiken wirksamer zu steuern, BYOD-Strategien zu realisieren und die Spezifikationen von IT-GRC-Frameworks zu unterstützen.

Mit Next-Generation NAC können Unternehmen unterschiedlichste, isolierte Sicherheitstechnologien zu einem einheitlicheren, automatisierten System zusammenführen. Der bi-direktionale Informationsaustausch, den Next-Generation NAC ermöglicht, hilft den einzelnen Sicherheitssystemen, unverwaltete Geräte, kurzzeitig verbundene Geräte, dynamische Risiken und Bedrohungen zu erkennen. Und schließlich bietet Next-Generation NAC auch umfangreiche Automatisierungsmöglichkeiten für die Reaktion auf Bedrohungen und deren Behebung.

FROST & SULLIVAN

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw

SILICON VALLEY
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

SAN ANTONIO
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON
4 Grosvenor Gardens
London SW1W 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?