

**BRANCHE**

Wasserversorgung

UMGEBUNG

240 Mitarbeiter and 500 Endpunkte an 12 Standorten

DIE HERAUSFORDERUNG

- Steigerung der internen Sicherheits-Compliance durch mehr Sichtbarkeit und bessere Verwaltungsmöglichkeiten von privaten und firmeneigenen Devices, sowie von Software im Netzwerk des Unternehmens

DIE LÖSUNG

- Eine leicht zu bedienende agentenlose Lösung, die geringstmöglichen manuellen Aufwand erfordert
- Installation und Betrieb ohne direkten Eingriff für eine unkomplizierte Integration in das vorhandene Cisco-Netzwerk von SESW
- Out-of-Box-Funktionalität für die automatische Erkennung von Geräten, Benutzern und Software, flexible Richtlinienmaßnahmen sowie Warnungen und Berichte

DIE ERGEBNISSE

- Umfassende Sichtbarkeit in Echtzeit des internen Netzwerks
- Ein übersichtliches Dashboard, auf dem der Compliance-Status der Endpunkte im IT-Bestand von SESW angezeigt wird
- Schnellere interne Bedrohungserkennung und Fehlerbehebung
- Integration in McAfee-Software, um eine angemessene Konfiguration der Antivirensoftware auf allen Endpunkten sicherzustellen

Sutton and East Surrey Water

Sutton and East Surrey Water hat sich für ForeScout CounterACT® aufgrund der Netzwerksichtbarkeit in Echtzeit, der internen Sicherheits-Compliance und der Automatisierung von Verwaltungsaufgaben entschieden.

Überblick

Sutton and East Surrey Water (SESW) stellt Trinkwasser für etwa 670.000 Personen in 284.000 Haushalten in East Surrey und in Teilen von West Sussex, West Kent und South London bereit. Auf einer Fläche von 835 Quadratkilometern liefert SESW durchschnittlich 160 Millionen Liter Wasser pro Tag. An heißen Sommertagen kann die Menge sogar auf 220 Millionen Liter steigen.

Die Herausforderung für das Unternehmen

Sutton and East Surrey Water benötigte eine Lösung für umfassendere Netzwerksichtbarkeit und Network Access Control (NAC) für seine 240 Mitarbeiter und 500 Endpunkte an 12 Standorten.

Die internen Anforderungen von SESW an die Lösung waren die folgenden:

- dynamische Netzwerksichtbarkeit von privaten und unternehmenseigenen Geräten und Software
- kontinuierliche Endpunkt-Schwachstellenanalyse und Fehlerbehebung
- Identifizierung und Kontrolle von WLAN-Zugriffen ohne entsprechende Freigabe
- richtlinienbasierte Einschränkung von Netzwerkports, -protokollen und -diensten durch Kontrollen, die sich leicht in die vorhandene Netzwerkinfrastruktur von SESW integrieren lassen
- Interoperabilität mit McAfee, um einen besseren Endpunkt-Schutz, wie etwa Antiviren-Konfiguration, im gesamten internen Bestand zu gewährleisten
- ein Roadmap- und Monitoring-Tool für interne Sicherheits-Compliance
- ein zentrales Archiv für Daten von IT-Assets

Warum ForeScout?

Als SESW sich auf die Suche nach einer Lösung begab, die seine Netzwerksichtbarkeit und Sicherheitskontrolle verbessern sollte, ging das Unternehmen auf BlueFort Security zu, seinen langjährigen Partner im Bereich IT-Integration. BlueFort empfahl ForeScout CounterACT® und bot einen Proof of Concept (PoC) vor Ort für das IT-Sicherheitsteam von SESW an. Das Wasserunternehmen bewertete die Tauglichkeit von CounterACT und kam zu dem Schluss, dass die Lösung weitaus mehr Funktionen bot, als es für SESW als Minimum erforderlich gewesen wäre.

„Wie alle Unternehmen haben auch wir ein begrenztes IT-Sicherheitsbudget und müssen daher sicherstellen, dass wir das Maximum aus unseren Investitionen in die IT-Sicherheit herausholen“, sagt Michael Cock, Group IT Manager von Sutton and East Surrey Water. „Nachdem wir ForeScout als mögliche Lösung identifiziert hatten, stellten wir fest, dass es sehr wenige direkte Konkurrenten auf dem Markt gibt – sicher gibt es nichts, das dieselbe Bandbreite an Funktionen aufweist. Sowohl Preis als auch Umfang von CounterACT waren deutliche Vorteile gegenüber alternativen Lösungen, die wir in Betracht zogen.“

David Henderson, Chef der Geschäftsentwicklung bei BlueFort Security sagt: „CounterACT ist die ideale Plattform für SESW, von der aus die Datensicherheit und Compliance schnell bewertet werden kann und Kontrollen einfach implementiert werden können. Die PoC-Probe konnte innerhalb von Wochen nahtlos in die Produktion übergehen und ist heute ein Eckpfeiler für das IT-Sicherheitsframework des SESW-Teams.“



„CounterACT erhöht unsere Netzwerksicherheit und erfordert minimale manuelle Eingriffe, wodurch sowohl Risiken als auch Kosten reduziert werden. Zudem erreichen wir dank CounterACT ein hohes Maß an Sicherheitsrichtlinien-Compliance, was für uns essentiell ist.“

- Michael Cock, Group IT Manager, Sutton and East Surrey Water

Was hebt ForeScout von der Konkurrenz ab?

Zentrale Unterschiede, die zum allgemeinen Erfolg von SESW beitragen:

- Netzwerksichtbarkeit privaten und unternehmenseigenen Geräten und Softwares im Netzwerk
- Integration in vorhandene Sicherheitslösungen
- minimaler manueller Aufwand

Weitere Informationen finden Sie unter www.ForeScout.com



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

Die Auswirkungen für das Unternehmen

Sichtbarkeit und Risiko-Management in Echtzeit

SESW benötigte eine Netzwerksicherheitslösung, die eine Bestandsaufnahme der aller Geräte sowie der installierten Software ermöglicht. „Auf der Suche nach einer Lösung, die unsere interne Netzwerksicherheit genauso stark macht wie unsere externe Netzwerksicherheit, war es unser oberstes Ziel, ein überprüfbares und vollständiges IT-Erkennungstool zu finden“, so Michael Cock. „Vor ForeScout nutzten wir eine Reihe von verschiedenen Tools zur Asset-Erkennung und -Prüfung. Zudem war ein erheblicher manueller Aufwand notwendig, um Daten zu sammeln, was natürlich Risiken birgt. Die ForeScout-Lösung löste dieses Problem und die Tatsache, dass sie so viel mehr ist als nur ein Prüfungs- und Erkennungstool, bot uns einen erheblichen Mehrwert.“

Erstellung und Durchsetzung von Richtlinien

SESW erstellte mithilfe von CounterACT eine Reihe von individuellen Sicherheitsrichtlinien, einschließlich der Folgenden:

- Blockieren von nicht autorisierten oder nicht regelkonformen Geräten und Benutzern
- Sicherstellen der Endpunkt-Compliance, z. B. dass die installierte Antivirensoftware funktioniert und auf allen Endpunkten auf dem aktuellsten Stand ist
- Blockieren von Malware-Angriffen im Netzwerk; Threat Prevention
- Blockieren von nicht autorisierten Anwendungen, beispielsweise Instant Messaging und Peer-to-Peer
- Automatisieren von Prüfberichten

Zudem erstellte SESW eine individuelle Richtlinie zum Identifizieren von Dual-Homed-Netzwerkkarten. Michael Cock erklärt: „Die Gefahr ist, dass sich ein

Gerät in unserem internen Netzwerk befindet, das auch kabellos aktiviert ist, sodass unsere interne Sicherheit über ein externes WLAN-Netzwerk beeinträchtigt werden kann. In so einem Fall nutzen wir CounterACT, um die kabellose Verbindung des Geräts zu deaktivieren, um so unser internes Netzwerk zu schützen.“

Geringerer manueller Aufwand

Eines der Auswahlkriterien von SESW war die leichte Handhabung der Lösung (d. h. so wenig manueller Aufwand wie möglich). Michael Cock erklärt: „Viele IT-Lösungen, speziell Sicherheitslösungen, erfordern eine kontinuierliche Überprüfung der Regeln und der Ergebnisse dieser Regeln – unser IPS ist ein gutes Beispiel dafür. Für mich bietet die perfekte Lösung alle Vorteile automatisch und ForeScout ist davon nicht weit entfernt.“

Integration in Sicherheitsprodukte

Dank der ControlFabric-Technologie von ForeScout kann CounterACT Daten mit anderen IT-Systemen austauschen und ein breites Spektrum an Problemen beheben. SESW macht sich diese Möglichkeiten zunutze, indem sie CounterACT in ihre zentrale Sicherheits-Management-Software und ihre Antivirenlösungen von McAfee ePolicy Orchestrator® (McAfee ePO™) integriert.

Ein Blick in die Zukunft

Für Sutton and East Surrey Water ist CounterACT mehr als nur Network Access Control und das Unternehmen rät anderen Versorgungsunternehmen in Großbritannien, die eine NAC-Lösung implementieren möchten, Folgendes:

„CounterACT erhöht unsere Netzwerksicherheit und erfordert minimale manuelle Eingriffe, wodurch sowohl Risiken als auch Kosten reduziert werden. Zudem stellt es sicher, dass wir ein hohes Maß an Sicherheitsrichtlinien-Compliance erreichen, was essentiell ist.“