ForeScout CounterACT®

사물인터넷(IOT) 장치를 포함한 모든 IT 자산을 실시간으로 탐지하고 네트워크 및 단말을 정책기반으로 통제합니다.

ForeScout CounterACT®는 실시간 자산 탐지 및 네트워크와 단말을 정책으로 제어하며 조직내 보안규정에 맞도록 운영 및 지원합니다. CounterACT는 사용자와 소유자, 운영 체제는 물론 장치 구성, 소프트웨어, 서비스, 패치 상태 및 보안 에이전트의 존재도 빠르게 확인합니다. 그런 다음 이러한 장치를 교정 및 제어하고 지속적으로 모니터링합니다.

CounterACT는 회사에서 지급한 장치와 개인 소유의 BYOD 단말, 비정형 장치를 대상으로 이러한 조치를 수행하며, 소프트웨어 에이전트나 장치에 대한 사전 지식이 필요 없습니다. CounterACT는 기존 환경에 빠르게 구축할 수 있고 인프라 변경이나 업그레이드, 단말 재구성을 거의 요구하지 않습니다.

고객이 CounterACT를 선택하는 이유

이기종 지원: 널리 사용되는 네트워크 인프라, 운영 체제, 단말 소프트웨어 및 타사 보안 솔루션과 연동됩니다.

비에이전트 방식: 인증 및 네트워크 접근 제어에 단말 에이전트가 필요하지 않습니다.

탁월한 가시성: 다른 솔루션은 보지 못하는 장치를 봅니다.

- 데스크톱과 노트북, 서버, 라우터, 스마트폰, 태블릿
- 유/무선 LAN 및 프린터
- IoT 장치(프로젝터, 산업용 제어기, 의료, 제조, POS 장치 등)

자동 제어: 다음과 같은 광범위한 조치를 자동으로 처리합니다.

- 장치의 보안 태세 및 보안 정책에 따라 네트워크 접근 허용, 거부 또는 제한
- 악성/고위험 단말의 격리와 교정

신속한 가치 창출: 수 시간 내에 신속하게 구축하여 네트워크 가시성을 확보합니다.

정책 적용: 네트워크 접근 제어와 단말 컴플라이언스, 모바일 장치 보안 정책을 적용합니다.

생산성: 업무를 방해하는 개입이나 직원의 관여 없이 사용자와 장치에 적절한 네트워크 접근 권한을 부여합니다.

신뢰도: 로그 인프라를 식별하고 제거함으로써 네트워크 안정성을 개선합니다.

비용 절감: 게스트 접근을 위해 네트워크 포트를 여닫는 수동 작업이 사라집니다.

컴플라이언스: 자동으로 정책 위반을 식별하고 단말 결함을 교정하며 컴플라이언스 요건의 준수 상태를 측정합니다.

네트워크 보안 위험 및 사각지대

전통적인 네트워크 보안은 방화벽과 IPS(침입방지시스템)로 외부 공격을 차단하는 데 초점을 맞추었습니다. 그러나 이러한 보안 도구는 보안 사고와 침입을 더욱 빈번하게 유발하는 압도적인 내부자 위협으로부터 네트워크를 보호하는 데에는 아무런 역할도 하지 못합니다. 이러한 위협에는 다음이 포함됩니다.

- **방문자:** 손님과 계약자가 회사에 자신의 컴퓨터를 가져옵니다. 모두 인터넷 접속이 필요하고 계약자의 경우 추가 리소스가 필요할 수도 있습니다. 이러한 방문자에게 무제한의 접근 권한을 준다면 네트워크가 공격에 노출됩니다.
- **무선 및 모바일(BYOD) 사용자:** 직원이 개인 소유의 스마트폰과 태블릿, 노트북을 회사 네트워크에서 사용하고 싶어 합니다. 충분한 제어가 뒷받침되지 않을 경우 이러한 장치는 네트워크를 감염시키거나 데이터 손실을 유발할 수 있습니다.
- **사물인터넷(IoT) 장치:** 비정형 장치가 IP 연결 프로젝터와 온도 조절기, 조명 제어기, 보안 카메라 등 비관리형 장치를 추가함으로써 공격 면적을 계속 확장합니다.
- **로그 장치:** 직원들이 값싼 유선 허브와 부서 서버, 라우터, 무선 접근 지점 등을 이용하여 의도와는 무관하게 네트워크를 확장함으로써 불안정성과 취약성을 유발할 수 있습니다.
- **멀웨어 및 봇넷:** 네트워크 보안이 침해되면 네트워크에 연결된 장치들은 "피벗 공격"에 사용될 수 있으며 그 경우 외부 인원이 네트워크를 스캔하고 데이터를 훔칠 수 있습니다.
- **컴플라이언스:** 잘못 구성된 단말과 가상 컴퓨터는 잘못된 설정이나 부적절한 소프트웨어를 포함하고 있을 수 있습니다. 게다가 사용자나 멀웨어가 의도적으로 작동을 중지시켜 보안 제어가 비활성화될 수 있습니다.

탐지가 불가능한 장치는 통제할 수 없습니다.

가시성이 제한되면 보안 사각지대가 발생합니다. 대부분의 단말 보안 시스템은 가시성 확보와 관리를 위해 장치마다 최신으로 업데이트된 에이전트를 요구합니다. 일반적으로 IT 보안 관리자는 비관리형 BYOD 단말과 매일 네트워크에 등장하며 점점 수가 증가하는 IoT 장치에 대한 가시성을 확보하지 못하고 있습니다.

분석가와 고객, 파트너가 선택하는 CounterACT

- ForeScout은 비전을 실행하고 완성하는 역량을 인정받아 Gartner 네트워크 접근 제어 매직 쿼드런트** 리더로 선정되었습니다(4연속 보고서).
- SC Magazine 최고의 NAC 솔루션, 2015년 6월
- SC Magazine 최고의 제품, 2014년 10월

> 우리는 비즈니스 개입의 위험이 없이 빠르게 구축할 수 있는 NAC 솔루션이 필요했습니다. 뿐만 아니라, Aruba®와 Cisco®가 혼합된 당사의 IT 인프라를 지원해야 했습니다. ForeScout CounterACT는 이 모든 요구를 충족하고 그 이상을 제공했습니다. 기존에 사용하던 FireEye® 및 ArcSight® 보안 도구와의 인상적인 통합 기능도 그 중 하나였죠. 그래서 우리 정보 보안 부서에서는 CounterACT가 '스위스 군용 칼'로 통합니다. 다수의 자동화된 보안 점검과 컴플라이언스 제어를 가장 효율적인 방식으로 가능하게 하니까요."
>
> **— KKB 정보 보안/위험 관리 책임자, Ali Kutluhan Aktaş**

ForeScout CounterACT®의 작동 방식

ForeScout CounterACT는 IP 및 MAC 연결된 장치들을 탐지하고 제어하며, 기존 시스템과 상호 연동을 통해 유기적인 보안시스템 구축을 지원합니다. 그 방식은 다음과 같습니다.

가시성 CounterACT 어플라이언스가 네트워크에 아웃오브밴드(Out of Band)로 구축됩니다. 그리고 그 시점부터 CounterACT는 네트워크 트래픽을 계속 모니터링하고 네트워크 인프라와 통합하여, 장치가 네트워크에 접근하는 즉시 식별합니다. CounterACT는 IP로 연결된 광범위한 단말과 사용자, 애플리케이션을 확인할 수 있는 고유한 기능을 갖추고 있습니다. 사실, CounterACT의 정교한 기술은 경쟁 제품에는 보이지 않는 장치까지 탐지합니다.

CounterACT는 여기에서 멈추지 않고, 수동 및 능동 심문 기술을 통해서 네트워크의 단말을 정확하게 분류합니다. CounterACT는 장치의 유형, 위치, 사용자와 장치가 도메인의 구성원인지 여부를 비롯하여 기타 기본적인 정보를 식별할 수 있습니다. 또한 관리자 자격 증명으로 회사 소유 장치에 쿼리함으로써 장치의 보안 태세에 관한 세부정보를 수집합니다.

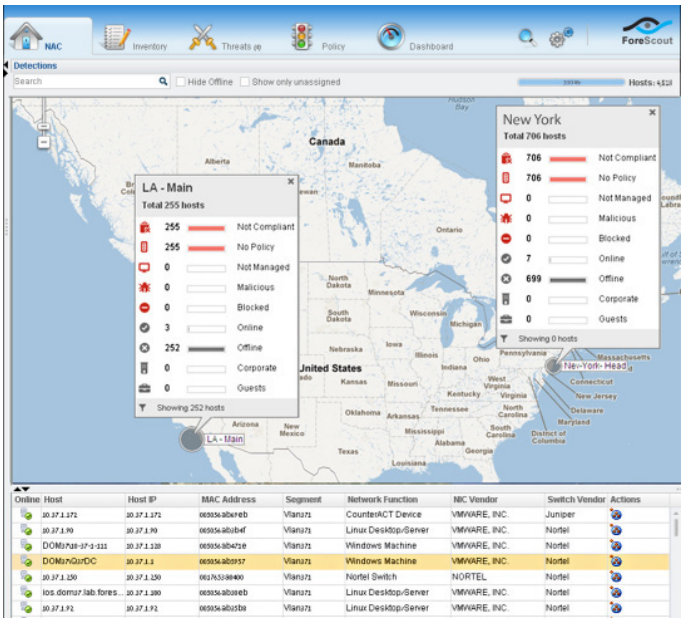

그림 1: ForeScout CounterACT는 네트워크의 장치에 관한 상위 수준 정보와 세부정보를 모두 제공합니다.

제어 CounterACT가 임의의 단말에서 보안 문제를 탐지하면, 정교한 정책 관리자가 문제의 중요도에 따라 다양한 대응을 자동 실행할 수 있습니다. 경미한 위반이 발생하면 최종 사용자에게 경고 메시지가 전송될 수 있습니다. 개인 장치를 가져온 직원과 계약자는 자동화된 온보딩 포털로 리디렉션됩니다. 심각한 위반 발생 시에는 장치의 차단이나 격리, 보안 에이전트의 재설치, 에이전트나 프로세스의 재시작, 단말의 운영 시스템 패치 트리거 및 기타 교정 조치로 이어질 수 있습니다.

ControlFabric 아키텍처의 가치

ControlFabric 아키텍처는 타사 네트워크와 보안, 모빌리티, IT 관리 제품에 ForeScout CounterACT의 기능을 연결해주는 접착제의 역할을 합니다. ControlFabric 아키텍처는 보안 관리 사일로를 제거하여 다음을 가능하게 합니다.

- 시스템 전반의 보안 관리 단일화
- 더욱 뛰어난 운영 효율성 달성
- 위협 대응 가속화
- 보안 투자수익 증대
- 네트워크 보안 및 컴플라이언스 상태 대폭 개선

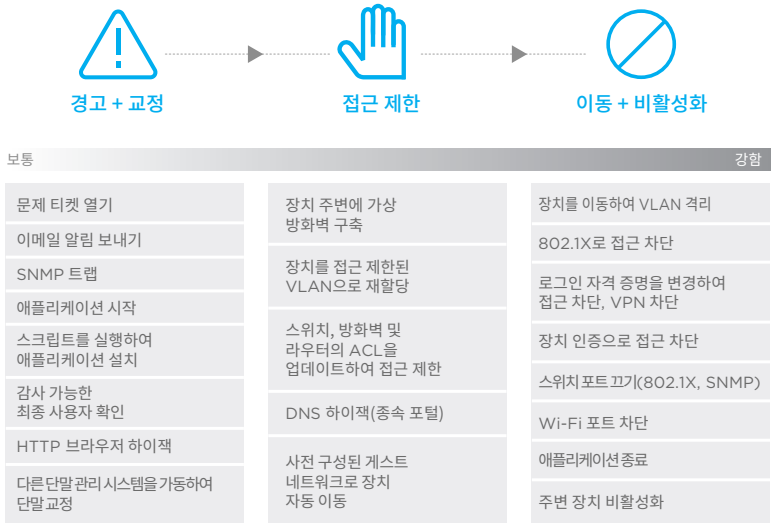

그림 2: ForeScout CounterACT는 모든 범위의 제어 조치를 다룹니다.

오케스트레이션 CounterACT는 OpenAPI 인 ControlFabric 아키텍처를 제공, 이를 통해 기존의 보안제품 및 시스템과 연동을 지원하며, 유기적으로 정보교환을 바탕으로 정책수립 및 액션을 수행합니다. ControlFabric 아키텍처는 맞춤 통합 또는 플러그 앤 플레이 소프트웨어 모듈을 통해 이를 달성하도록 지원합니다. ForeScout 기술 파트너와 공동 개발한 ForeScout Base 및 Extended Modules는 CounterACT의 기능을 70개 이상의 업계 상위 네트워크와 보안, 모빌리티, IT 관리 제품에 결합하여 다음을 지원합니다.

- IT 보안 및 관리 시스템과 상황 정보 공유
- 시스템 간 공통 워크플로, IT 작업 및 보안 프로세스 자동화
- 위험 및 데이터 침해의 신속한 경감을 위해 시스템 전반의 반응 가속화

특징

일반

아웃오브밴드(Out of Band) 구축: 대기 시간 증가 또는 잠재적인 네트워크 장애 지점 없이 네트워크에 아웃오브밴드 (Out of Band)를 구축합니다.

가시성: 자산 인벤토리 기능이 실시간 다차원 네트워크 가시성과 제어를 제공하여 사용자, 애플리케이션, 프로세스, 포트, 외부 장치 등을 추적하고 제어할 수 있습니다(그림 1 참조).

개방형 상호 운용성: CounterACT는 인프라 변경이나 장비 업그레이드 없이도 대중적인 스위치, 라우터, VPN, 방화벽, 단말 운영 체제(Windows®, Linux, iOS, OS X, Android), 패치 관리 시스템, 안티바이러스 시스템, 디렉터리, 티켓팅 시스템과 연동됩니다.

보고: 완벽하게 통합된 보고 엔진이 정책 컴플라이언스 수준을 모니터링하고 규정 감사 요구사항을 이행하며 실시간 인벤토리 보고서를 생성할 수 있도록 지원합니다.

확장성: 단말 백만 개 이상의 고객 네트워크에서 그 역량이 검증되었습니다. CounterACT 어플라이언스는 다양한 크기로 이용할 수 있습니다.

인증: CounterACT는 군사 등급으로 다음과 같은 인증을 받았습니다.

- 미국 해병대 운영 인증(ATO)
- 미국 육군 CoN(최종 가치 인증)
- UC APL(단일 기능 승인 제품 목록)
- 공통 기준 평가 보증 레벨(EAL) L4+

작업을 방해하지 않는 방식: 사용자나 장치에 영향을 주지 않고 구축이 가능합니다. 자동화 통제로 전환하려 할 때 점진적으로 진행할 수 있으며, 가장 문제가 될 만한 장소에서 시작해서 적절한 적용 조치를 선택할 수 있습니다.

정책 관리: 기업에 적합한 보안 정책을 생성합니다. 내장된 정책 템플릿, 규칙 및 보고서를 이용하여 빠르고 손쉽게 구성과 관리가 가능합니다.

ControlFabric 아키텍처: ControlFabric® 아키텍처는 광범위한 타사 벤더 상호 운용성과 오픈 통합 아키텍처를 제공합니다.

단말

비에이전트 방식: 에이전트 없이 네트워크 접근을 식별하고 분류, 인증 및 제어합니다. CounterACT가 단말에 관리자 자격 증명을 보유하고 있다면 비에이전트 방식으로 심층적인 단말 검사를 수행할 수 있습니다. BYOD처럼 CounterACT가 관리자 자격 증명을 보유하지 못한 상황에서는 옵션으로 제공되는 SecureConnector 에이전트의 도움으로 심층 검사를 수행할 수 있습니다. SecureConnector는 CounterACT에 포함되어 있으며 추가 비용이 필요하지 않습니다.

단말 무결성: 네트워크의 단말이 안티바이러스 정책을 준수하고 적절히 패치가 이루어지며 불법 소프트웨어를 사용하지 않도록 보장합니다. CounterACT는 자동으로 정책 위반을 식별하고 단말 결함을 교정하며 컴플라이언스 요건의 준수 상태를 측정합니다.

위협 탐지: 일부 장치는 네트워크를 잠시 드나들기 때문에 상시 모니터링을 통해서 시점 방식 취약점 스캔보다 더욱 적시적이고 정확한 정보를 제공합니다.

로그 장치 탐지: 인증되지 않은 스위치와 무선 접근 지점 등 로그 인프라를 탐지합니다. CounterACT는 민감한 정보를 도용하도록 설계된 스텔스 패킷 캡처 장치 등 IP 주소가 없는 장치도 탐지합니다.

접근

게스트 등록: 내부 네트워크 보안을 침해하지 않고 게스트를 네트워크에 접근하도록 허용합니다. 여러 개의 게스트 등록 옵션을 이용하여 게스트 관리 프로세스를 조직의 요구에 맞게 설정할 수 있습니다.

역할 기반 접근: CounterACT는 적절한 인원이 적절한 장치를 사용하여 적절한 네트워크 리소스에 접근하도록 보장합니다. CounterACT는 사용자 ID에 역할을 지정한 고객사의 기존 디렉터리를 활용합니다.

유연한 제어 옵션: 엄격한 제어와 사용자 영향을 동반하는 "전통적인" NAC 제품과는 달리, CounterACT는 전 영역에 걸친 적챙 적용 옵션을 제공하여 상황에 따른 맞춤식 대응을 설정할 수 있습니다. 위험도가 낮은 위반 사항은 최종 사용자에게 알림을 보내거나 보안 문제를 자동으로 교정하여 해결할 수 있고, 따라서 교정이 진행되는 중에도 사용자는 생산성을 유지할 수 있습니다(그림 2 참조).

802.1X 인증 또는 기타: 802.1X 또는 LDAP, Active Directory®, RADIUS®, Oracle®, Sun 등 기타 인증 기술을 선택할 수 있습니다. 하이브리드 모드로 여러 기술을 동시에 사용하면 대규모의 다양한 환경에서 NAC 구축을 가속화할 수 있습니다.

내장 RADIUS: 내장 RADIUS 서버로 간편하게 802.1X의 롤아웃을 수행할 수 있습니다. 또는 CounterACT를 RADIUS 프록시로 작동하도록 구성하여 기존 RADIUS 서버를 활용할 수도 있습니다.

확장 가능 모델

CounterACT는 단말이 백만 개가 넘는 고객 네트워크에서 그 역량을 입증한 바 있습니다. 다양한 물리 및 가상 어플라이언스 옵션으로 제공되어 고객 비즈니스의 특정한 요구를 충족합니다. 여러 어플라이언스가 필요한 대규모 네트워크는 CounterACT Enterprise Manager를 이용하여 중앙집중식으로 관리할 수 있으며, 각 CounterACT 어플라이언스에는 지정된 개수의 네트워크 장치에 대한 영구 라이선스가 포함됩니다. 라이선스 정책에 관한 자세한 내용은 www.forescout.com/licensing을 참조하십시오.

중앙집중식 관리 및 제어

CounterACT Enterprise Manager는 물리적 또는 가상 어플라이언스로 구축할 수 있으며 CounterACT 구현의 중앙집중식 관리와 제어 기능을 제공합니다. CounterACT Enterprise Manager는 CounterACT의 활동과 정책을 감독하고 각 어플라이언스에서의 악성 활동은 물론 CounterACT가 수행하는 식별, 알림, 제한, 교정 조치에 대한 정보를 수집합니다. 이 정보는 CounterACT 콘솔에서 표시 및 보고하는 데 사용할 수 있습니다.

자세히 알아보기:
www.ForeScout.com

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

수신자 부담(미국) 1-866-377-8771
전화(국제) +1-408-213-3191
지원 1-708-237-6591
팩스 1-408-371-2284

*2016년 1월 현재.
**Gartner, Inc., "Magic Quadrant for Network Access Control(네트워크 접근 제어 매직 쿼드런트)", Lawrence Orans와 Claudio Neiva, 2014년 12월 10일. Gartner는 연구 간행물에 기술된 어떠한 공급업체나 제품 또는 서비스에 대해서도 보증하지 않으며 기술 사용자에게 높은 등급 또는 기타 명칭의 공급업체만을 선택할 것을 권장하지도 않습니다. Gartner의 연구 간행물은 Gartner 연구 조직의 의견으로 구성되어 있으며, 이는 사실 진술서로 해석되어서는 안 됩니다. Gartner는 상품성 또는 특정 목적에 대한 적합성의 보증을 포함하여 이 연구와 관련된 모든 명시적 또는 묵시적 보증을 부인합니다.