ForeScout

조직의 과제

- 전반적인 네트워크 보안 개선
- 외부 위협으로부터 민감한 데이터 보호
- 직원과 계약자, 고객의 접근을 방해하지 않음
- 내외부 정책 별도 설정 및 보안 준수
- ROI & 시스템 최적화 지원

기술적 과제

- Agent/Agentless 모드를 지원, Agentless 모드 사용시, 기존 단말에 에이전트를 미설치해도 Agent 와 동일한 기능 제공
- 단말 유형/위치/사용자 정보/무결성 상태와 같은 다양한 정보 제공
- 악성 소프트웨어 및 바이러스 등이 감염 탐지된 단말의 원천적인 네트워크 차단
- 내외부의 비인가된 접근 및 공격 사전 탐지 및 방어를 통한 시스템 보호
- 시스템 자동화를 통한 조직 보안수준 유지 및 적절한 보안 교정 프로세스 정립
- 보안 제어의 효과 측정 및 규정 컴플라이언스 입증

네트워크 접근 제어

네트워크 상의 모든 장치를 실시간으로 확인하고 제어할 수 있습니다.

ForeScout 사는 IOT 장치를 포함하여 네트워크에 연결 및 접근하는 모든 IT 자산들을 탐지 및 분류, 이를 통제하는 솔루션을 제공합니다. ForeScout 사의 CounterACT 제품은 IT 자산들에 대한 가시성을 제공하고, 인증 프로세스를 통하여 자산을 분류, 이에 맞는 역할별 네트워크 제어를 실시간으로 제공합니다.

과제

오늘날의 기업 네트워크는 PC와 태블릿, 스마트폰에서 산업용 제어기, 가상 서버, 무선 접근 지점, 클라우드 기반 애플리케이션에 이르기까지 방대한 전통적 장치 및 비정형 장치와 기타 단말을 수용합니다. 또한, BYOD, 사물인터넷(IOT), 복합적 IT 환경이 확장되고 해커의 기술이 갈수록 정교해짐에 따라 장치와 관련된 문제의 범위가 계속해서 확대될 것은 너무도 분명합니다. 따라서 네트워크 접근 제어(NAC) 솔루션은 회사와 직원 소유의 장치는 물론 알려지지 않은 더욱 많은 수의 미인증 장치를 관리해야 합니다.

포괄적이며 고도의 인텔리전스를 갖춘 NAC 보안 솔루션이 더욱 필요한 이유로는 다음과 같은 몇 가지 사실을 들 수 있습니다.

- 2020년까지 260억개 이상의 사물인터넷(IOT) 장치가 증가할 것으로 예상됩니다.[1]
- 75% 의 모바일 어플리케이션들이 기본적인 보안테스트 평가를 통과하 못했습니다.[2]
- 2014년 보안침해사고 결과, 98.7%가 외부로부터의 해킹시도로 확인되었습니다.[3]

조직의 IT 보안담당자 및 관리자는 현존하는 장치 및 시스템들의 내부 네트워크 사용여부 및 접근 상태, 로그인 상태, 통제 및 정책들이 조직의 보안수준에 적합한지 확인 및 인지하여야 합니다.

FourScout의 솔루션

ForeScout CounterACT는 네트워크 상의 모든 IT 자산들을 실시간으로 탐지, 분류, 통제하는 기능을 제공합니다. 또한 네트워크를 지속적으로 모니터링하고 조직/비조직/파트너/개인 등의 장치들을 분류하여 정책에 따른 역할별 네트워크 접근 통제를 실행합니다. 또한 단말들의 무결성을 보장하며, 모바일 장치들의 탐지 및 보안상태 수준을 확인합니다. CounterACT는 조직 내 정책 프로세스를 자동화하며 보안수준을 최상으로 유지하고 작업의 유연성 및 연속성을 보장합니다.

CounterACT 인텔리전스와 기능의 기반은 다음 세 단어로 요약할 수 있습니다.

가시성 CounterACT는 Agent/Agentless 모드를 지원하며 네트워크 상의 모든 IT 자산을 실시간으로 탐지하고 모니터링합니다. 단말장치의 상태 및 사용자, 어플리케이션, 운영체제, 보안 유지 상태를 지속적으로 확인합니다.

제어 CounterACT는 장치의 보안 태세 및 보안 정책에 따라 네트워크 접근을 허용 또는 거부하거나 제한합니다. 악성 또는 고위험 단말을 평가하고 교정함으로써 조직을 위험에 빠뜨릴 수 있는 데이터 침해와 멀웨어 공격의 위협을 최소화합니다. 뿐만 아니라, CounterACT는 네트워크의 장치를 상시 모니터링하고 보안 정책에 따라 제어함으로써 산업 요건과 규정에 대한 컴플라이언스를 입증하는 데 필요한 노력을 대폭 줄여줍니다.

오케스트레이션 CounterACT는 ForeScout ControlFabric® 아키텍처를 통해 70개 이상의 네트워크, 보안, 모빌리티, IT 관리 제품**과 연동됩니다. 시스템 간에 실시간 보안 인텔리전스를 공유하고 단일화된 네트워크 보안 정책을 적용하는 기능은 시스템 전반의 위협 대응을 자동화함으로써 취약 시간대를 감소시킵니다. 뿐만 아니라, 워크플로우 자동화를 통해 시간을 절약하고 기존 보안 도구에서 보다 높은 투자 효율을 달성할 수 있습니다.

ForeScout CounterACT는 단말정보(위치, 소유자, 상태)를 수집하여 제공합니다. ForeScout CounterACT는 다음의 정보들을 제공합니다.

- 미인증 장치 및 비인가 어플리케이션이 구동되는 장치들을 네트워크에서 분리/격리하여 피해를 사전방지 및 최소화
- 인증 및 인가된 장치들의 보안수준을 최상으로 유지하고, 최신의 OS 패치, 백신엔진의 업데이트 상태를 최신으로 설치 유지하는 등의 무결성 보장
- 기존 시스템과의 연동을 통해, 암호화 및 정보 유출 방지 에이전트 구동 및 확인
- 비인가된 어플리케이션이나 외부장치 사용을 사전 차단하여 사용자 임의 조작 방지

일부 단말이 조직에서 설정한 보안수준 및 정책을 위반하고 이가 적발될 경우, CounterACT 는 해당 정책의 액션을 적용하여 네트워크 차단/경고/격리/교정 조치를 강제적으로 실행합니다. 정책의 액션은 종류가 경고부터 강제차단까지 다양하며, 이는 관리자가 상황에 맞게 설정하여 적용하면 됩니다. 또한 방문자 관리 정책, 시스템 위치 확인, 스위치 및 무선 AP & 컨트롤러의 통합 제어를 통해 역할별 네트워크 통제를 지원합니다.

ForeScout 사는 현재 60개국 2,000개 이상에서 공공 및 엔터프라이즈기업들을 보유하고 있으며, 특허된 기술력을 바탕으로 사물인터넷(IOT)을 포함한 모든 IT 자산들의 탐지 및 제어를 제공합니다. CounterACT 는 일반 서버(Vmware & MS Hyper V)위에서 가상으로 구동되는 Virtual CounterACT 타입과 어플라이언스 타입을 제공하며, 고객 환경에 맞춰서 선택이 가능합니다. 또한 Out-Of-Band 방식을 지원함으로써 기존 네트워크 변경 및 영향없이 바로 구축 및 설계가 가능합니다. 중앙집중/분산/복합 형태로 배포 및 설치가 가능하며 Enterprise Manager 장비를 통해 하나 이상의 어플라이언스 장비를 통합관리 할수 있습니다.

자세히 알아보기:
www.ForeScout.com

ForeScout®

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

1 Gartner 연구, http://www.gartner.com/newsroom/id/2636073
2 Gartner 연구, 2014년 9월 http://www.scmagazine.com/gartner-75-percent-of-mobile-apps-will-fail-security-tests-through-end-of-2015/article/372424/
3 Privacy Rights Clearinghouse 연구, http://www.securityweek.com/data-breaches-numbers

*개인 장치 사용(Bring Your Own Device: BYOD), 사물인터넷(Internet of Things: IoT)
*2016년 1월 현재