ForeScout

ForeScout

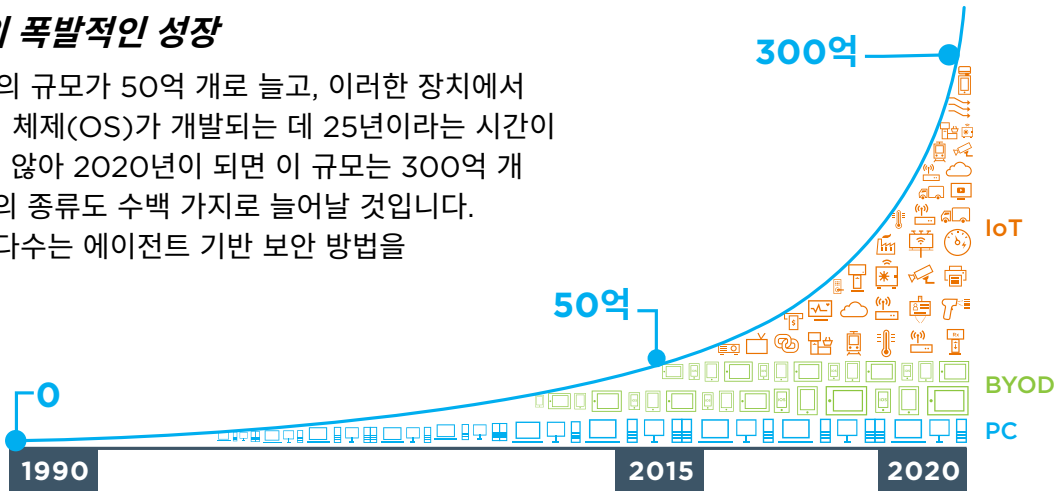
Transforming Security Through Visibility™ (가시성을 통한 보안 혁신)

가시성

과제:

플랫폼과 IoT 장치의 폭발적인 성장

네트워크에 연결된 장치의 규모가 50억 개로 늘고, 이러한 장치에서 실행되는 적은 수의 운영 체제(OS)가 개발되는 데 25년이라는 시간이 걸렸습니다. 그러나 머지 않아 2020년이 되면 이 규모는 300억 개 이상으로 늘어나며, OS의 종류도 수백 가지로 늘어날 것입니다. 그리고 이러한 OS의 대다수는 에이전트 기반 보안 방법을 사용하여 관리할 수 없습니다. 근본적으로 새로운 접근 방식이 등장하지 않으면 네트워크 사각지대가 보편화되고 공격 서비스는 계속 확대될 것입니다.



ABI 연구, 2017년

사물인터넷(IoT)과 새로운 OS, 모빌리티의 급성장으로 인해 관리되지 않는 장치가 폭발적으로 늘고 있습니다.

솔루션:

비에이전트 가시성 및 제어 능력

ForeScout는 장치를 실시간으로 탐색, 분류, 평가, 모니터링할 수 있는 비에이전트 보안 접근 방식을 개척했고 이를 통해 구내에서 클라우드에 이르기까지 네트워크 실시간 확인 및 안전한 관리가 가능해졌습니다.

구현 방법:

오늘날의 비즈니스 운영 환경은 천편일률적인 표준 네트워크가 아닙니다. 다분히 역동적이고 끊임없이 변화하는 환경입니다. ForeScout는 **이기종 보안** 기능을 제공하므로 구내의 장치는 물론 데이터센터 및 프라이빗/퍼블릭 클라우드 환경의 워크로드에 이르기까지, 네트워크 전반에 걸친 가시성을 확보할 수 있습니다. 또한 **유연성이 탁월한 벤더 애그노스틱** 접근 방식을 취하여 802.1X나 비802.1X, 또는 양쪽 모두를 실행하는 유무선 네트워크에서 Cisco, Aruba, Juniper Networks 등을 지원합니다.

보안의 첫걸음은 네트워크상의 항목을 파악하는 것입니다. 따라서 ForeScout는 인프라, 물리적/가상 컴퓨터, 관리형/비관리형 단말, IoT 및 로그 장치의 **탐지**를 수행합니다. 소프트웨어 에이전트나 이전 장치에 대한 지식은 없어도 됩니다. 그런 다음 솔루션을 통해 장치 위생을 **평가**하고 보안 상태를 **지속적으로 모니터링**합니다.

또한 **적응형 데이터 수집** 기능을 통해 **선택한 데이터 집합을 지원**하며, 오른쪽에 나열된 고급 활성 및 수동 기술을 사용하여 면밀한 가시성을 확보할 수 있습니다. ForeScout의 솔루션은 장치 및 애플리케이션을 빠르게 평가하여 장치의 사용자, 소유자, 운영 체제, 장치 구성, 소프트웨어, 서비스, 패치 상태, 보안 에이전트의 존재를 파악합니다. 이러한 지식을 통해 접근 제어, 적용, 교정과 관련하여 정확한 정책을 추진할 수 있습니다.

ForeScout의 가시성 지원

1. 연결된 장치 목록에 대한 스위치, VPN 집선 장치, 접근 포인트, 컨트롤러 폴링
2. 스위치 및 컨트롤러에서 SNMP 트랩 수신
3. 내장 또는 외부 RADIUS 서버에 대한 802.1X 요청 모니터링
4. DHCP 요청을 모니터링하여 신규 호스트가 IP 주소를 요청하는 시점 탐지
5. 네트워크 스위치 포트 분석기 포트를 선택 모니터링하여 HTTP 트래픽 및 배너와 같은 네트워크 트래픽을 확인
6. 네트워크 매퍼(Nmap) 스캔 실행
7. 자격 증명을 사용하여 장치에서 스캔 실행
8. NetFlow 데이터 수신
9. 외부 미디어 접근 제어 주소 분류 데이터 가져오기 또는 LDAP 데이터 요청
10. 퍼블릭 및 프라이빗 클라우드에서 가상 컴퓨터 모니터링
11. SNMP를 갖춘 PoE(이더넷 전원 장치)를 사용하여 장치 분류
12. 옵션 에이전트 사용

까다로운 사용 사례의 해결책

사물인터넷:

에이전트 없이 네트워크에 연결되는 즉시 IoT 장치를 탐지할 수 있습니다. 장치와 사용자, 애플리케이션, 운영 체제를 분류 및 프로파일링하고 장치를 자동 할당하여 VLAN(가상 근거리 네트워크) 세그먼트를 확보하며 동작을 모니터링합니다.

네트워크 접근 제어:

네트워크에 접근하는 장치와 사용자, 애플리케이션, 운영 체제를 실시간으로 확인할 수 있습니다. 사용자 및 IT 담당자에게 문제를 알리고 VLAN 세그먼트에 대한 장치 제한, 차단, 격리, 재할당 등 적절한 접근 제어 기능을 자동으로 적용합니다.

게스트 네트워킹:

방문자, 계약자, 파트너 등록을 자동화하고 적절한 온보딩 옵션을 사용하여 정책 컴플라이언스를 시행합니다. 장치 보안 상태 세부정보를 공유하고 엔터프라이즈 모빌리티 관리 및 단말 보호 도구를 사용하여 시행 조치를 오케스트레이션합니다.

BYOD 보안:

직원 소유의 노트북, 태블릿, 스마트폰의 네트워크 연결 시 비에이전트 가시성을 제공합니다. 접근 제어 및 단말 컴플라이언스 정책을 시행하며, 네트워크 포트를 열고 닫을 때 이와 관련한 수동 작업이 없습니다.

단말 및 규제 컴플라이언스:

네트워크에 드나드는 장치를 모니터링하고 보안 소프트웨어, 운영 체제, 구성 설정의 기간 만료 또는 표준 미달과 같은 정책 위반 문제를 사용자에게 알립니다. 사용자를 자체 교정 포털로 자동 리디렉션합니다.

보안 클라우드 컴퓨팅:

구내는 물론 프라이빗 클라우드 및 퍼블릭 클라우드 환경에 이르기까지 장치와 가상 컴퓨터의 가시성 및 제어 범위를 확장합니다. 물리적 환경 및 가상 환경 전체를 한 눈에 확인할 수 있으며 동시에 기존 보안 운영 팀의 기술 및 프로세스를 활용합니다.

제어

> **"현재는 5% 수준이지만 2020년에는 기업의 25% 이상이 IoT 보안을 위해 실시간 탐지 및 가시성, 제어 메커니즘을 활용할 것입니다."**
>
> —Gartner, *IoT 보안의 필수 요소: 실시간 탐지, 가시성 및 제어,* Saniye Burcu Alaybeyi & Lawrence Orans, 2016년 11월 3일

과제:

과도한 보안 경고와 불충분한 시행

대부분의 보안 도구가 경고 전송 기능은 탁월하지만 조치 시행 기능은 미흡합니다. 결국 보안 팀은 수동으로 평가하고 해결해야 하는 수많은 경고를 주체하지 못하게 됩니다. 긍정 오류여서 무시해야 하는 경고가 있는 반면, 리소스 제약으로 인해 놓치는 경고도 있습니다.

솔루션:

정책 기반 세분화와 적용

ForeScout은 정책 기반의 접근 제어와 함께 장치와 사용자, 애플리케이션의 적용을 자동화하여 적절한 리소스에 대한 접근을 제한하고 게스트 온보드를 자동화하며 단말 보안의 허점을 찾아 해결하는 동시에 산업 규정 컴플라이언스의 유지 및 개선에 도움을 줍니다.

구현 방법:

ForeScout를 통해 광범위한 활성 또는 수동 조치를 **자동화**할 수 있으며, 정책 및 상황의 심각성에 따라 **연결 시 제어 기능을 적용**할 수 있습니다. 이를 위해 ForeScout는 정책 엔진을 사용하여, 네트워크에서 장치의 동작을 지시 및 시행하는 정책 집합과 대조하여 장치를 **지속적으로** 확인합니다. 주기적으로 장치를 확인 또는 쿼리하는 다른 벤더의 제품과 달리 ForeScout의 정책 엔진은 한 번의 구축으로 100만 개가 넘는 장치에 대해 **실시간으로** 동작을 모니터링할 수 있습니다.

정책의 가동은 특정 장치에서 발생하는 이벤트를 기반으로 합니다. 그러한 이벤트로는 네트워크 승인 이벤트(스위치 포트 또는 IP 주소 변경 플러그인), 인증 이벤트(RADIUS 서버에서 수신하거나 네트워크 트래픽에서 탐지된 이벤트), **사용자/장치 동작 변화**(안티바이러스 소프트웨어 비활성화, 금지된 주변 장치 추가, 포트 여닫기), 특정 **트래픽 동작**(예: 장치 통신 방식 및 특정 프로토콜 사용) 등이 있습니다.

알림

- 사용자/관리자에게 이메일
- 화상 알림 메시지 전송
- 웹 페이지로 리디렉션
- 최종 사용자 응답 요청
- Syslog/CEF 메시지 전송
- 헬프데스크 티켓 열기
- IT 시스템을 통한 상황 정보 공유

준수

- 게스트 네트워크로 이동
- 무선 사용자 역할 변경
- 자체 교정 VLAN에 할당
- 로그 장치 제한
- 애플리케이션/프로세스 시작
- 안티바이러스/보안 에이전트 업데이트
- OS 업데이트/패치 적용

제한

- 장치 격리
- 스위치 포트 끄기
- 무선 또는 VPN 접근 차단
- ACL을 이용하여 접근 제한
- 인증되지 않은 앱 종료
- NIC/주변 장치 비활성화
- 교정 시스템 가동

ForeScout는 사용자의 보안 정책을 기반으로 보통에서 엄격한 수준까지 적절한 수준의 제어를 시행할 수 있습니다.

오케스트레이션

과제:

파편화된 보안

규모가 큰 기업의 경우 연결되지 않은 수십 개의 보안 시스템을 각각 운영합니다. 이렇게 사일로화된 접근 방식은 기업 전반의 체계적인 보안 대응을 저해하여 공격자에게 시스템 취약점을 익스플로잇할 수 있는 더 많은 시간을 허용합니다.

솔루션:

보안 자동화

ForeScout는 최고의 IT 및 보안 관리 제품으로 정보 공유 및 정책 기반 보안 시행 작업을 오케스트레이션하여 보안 워크플로를 자동화하고 사람의 개입 없이 위협에 대한 대응 속도를 높입니다.

> **"늦은 밤, 직원들이 잠을 자는 동안에도 ForeScout는 다른 보안 솔루션과 협력하며 여러 위협에 대해 즉각적인 조치를 취하고 있습니다. 그러한 유형의 자동화는 가격을 매길 수 없을 만큼 중요한 부분이죠."**
>
> — Michael Roling, 미주리 주 정부 최고정보보안책임자

구현 방법:

ForeScout는 가시성 및 제어 기능을 기본 기능으로 사용하여 **보안 사일로를 허물고** 기존 보안 투자를 활용하게 됩니다. ForeScout 모듈을 사용하면 장치 위생 및 위협, 동작, 컴플라이언스 관련 데이터를 지속적으로 교환하여 기존 보안 도구 및 분석의 스마트 및 상황 인식 기능을 더욱 강화할 수 있습니다. 보안 인프라에 중요한 제어 기능을 향상시켜 **정책의 수동 시행 자동화**, **응답 속도 가속화**, **보안 상태의 현저한 향상**이 가능해집니다. ForeScout의 솔루션에서 사용자의 여러 도구를 계층화하여 시스템 전반에 걸친 보안 오케스트레이션을 수행하는 방법에 대해 몇 가지 예를 소개합니다.

지능형 위협 탐지(ATD) ATD 제품은 맬웨어 및 침해 지표(IOC)를 탐지하는 즉시 ForeScout 플랫폼에 알립니다. 그러면 ForeScout 솔루션에서 정책을 기반으로 감염된 장치를 격리하고 교정 조치를 수행합니다. 또한 기존 및 신규 장치에 IOC가 있는지 스캔한 다음 위험경감 작업을 시작합니다.

보안 정보 및 이벤트 관리(SIEM): ForeScout 플랫폼은 네트워크에 연결된 장치를 탐지 및 파악하고 장치 세부정보를 SIEM과 공유하므로 더욱 지능적인 작업을 수행할 수 있게 됩니다. SIEM은 수집된 이벤트 및 로그를 기반으로 하는 장치 평가를 통해 응답합니다. ForeScout는 이러한 정보를 조치로 변환하여 보안 정책에 따라 장치를 허용, 거부 또는 격리합니다.

동적 네트워크 세분화: 방화벽, 스위치, 라우터와 관련하여 업계 선두 벤더의 제품과 긴밀하게 통합함으로써 정책 엔진이 VLAN 또는 ACL(접근 제어 목록)을 자동으로 적용하므로 장치 및 사용자를 적절한 네트워크 세그먼트에 배치하거나 다시 할당할 수 있습니다. 게스트, 계약자, 특정 직원, IoT 장치를 세분화하면 피벗 공격, 래터럴 공격, 내부 공격, DDoS 공격의 방지에 도움이 됩니다.

오케스트레이션 기능의 전체 목록을 확인하려면 웹사이트 **forescout.com/modules**를 방문하십시오. ForeScout와 협력 중인 파트너는 다음과 같습니다.

amazon web services · Check Point SOFTWARE TECHNOLOGIES LTD · CYBERARK · FireEye · IBM

McAfee · MobileIron · paloalto NETWORKS · QUALYS · RAPID7

servicenow · splunk> · Symantec · tenable · vmware

“ForeScout가 네트워크 접근 제어(NAC) 기술 면에서 이룬 성과는 확실히 혁신적입니다.”

— Frost & Sullivan 선정 2016년 최고의 네트워크 보안

“ForeScout 덕분에 JPMorgan Chase는 기업 네트워크에 연결된 수많은 장치 전반에 대한 탁월한 가시성을 확보하고 이를 관리할 수 있습니다.”

— Rohan Amin, JPMorgan Chase & Co. 글로벌 CISO

회사 스냅샷

산업: 사이버/IoT 보안

고객 수: 전 세계 60여 개국 2,000개 기업 및 정부 기관*

시장: 재무 서비스, 정부 및 방위, 의료, 제조, 교육, 소매, 핵심 인프라

설립연도: 2000년

CEO: Michael DeCesare

2016년 수상 경력 및 우수 기업 평가:

- JPMorgan Chase 명예의 전당 보안 혁신 기술 부문 이노베이션 어워드 수상
- Gartner IoT 보안 시장 가이드
- Gartner NAC 시장 가이드
- Forbes 선정 상위 100대 클라우드 기업
- Deloitte 선정 기술 분야 고속성장 500대 기업™
- Nanalyze 선정 강력한 9대 사이버 보안 신생기업
- CRN(Computer Reseller News) 선정 최고의 보안 회사
- Inc. 선정 5000개 고속성장 기업
- SC Magazine 선정 유럽 최고의 NAC 솔루션

보안 프레임워크/컴플라이언스 요건:

최고의 보안 표준 기관 및 프레임워크가 공유하는 기본 원칙이 하나 있다면, 보안은 가시성에서 시작된다는 것입니다. ForeScout는 다음 요건에 대한 기업 및 정부 기관의 컴플라이언스 활동을 지원합니다.

- 인터넷 보안 CSC(크리티컬 보안 제어) 센터
- CDM(상시 진단 및 위험경감)
- FISMA(연방 정보보안관리법)
- HIPAA(건강 보험 이전 및 책임법)
- HITECH(경제적 및 임상적 건전성을 위한 의료정보기술에 관한 법률)
- ISO/IEC 27001(국제표준기구/국제전기기술위원회)
- NIST(국립표준기술연구소) 위험 관리 프레임워크
- PCI-DSS(지불카드산업 데이터 보안 표준)
- SCAP(보안 콘텐츠 자동화 프로토콜)
- SOX(사베인스-옥슬리 법)

ForeScout

전 세계 지사:
새너제이(캘리포니아 주, 본사)
댈러스
런던
뉴욕
시드니
텔아비브
워싱턴 D.C.

2016년 12월 31일 기준