Forescout eyeSight

지속적으로 장치를 탐색, 분류, 평가하여 상황을 파악하고 위험요소를 줄입니다.

정보관리책임자는 네트워크에 연결된 시스템, 특히 IoT나 OT 장치가 늘어나는 상황에서 보안을 책임져야 합니다. 보이지 않는 것™을 보호할 수는 없기 때문에, 장치의 개수와 유형이 급증함에 따라 네트워크에 연결된 모든 물리 및 가상 장치에 대한 가시성이 절실히 요구됩니다. 여기에는 직원, 계약자, 고객 혹은 운영자가 연결한 관리, 미관리, 미확인 장치가 포함됩니다. 또한 캠퍼스, 데이터 센터, 개인 및 공용 클라우드, OT/ICS 환경 등 네트워크 상의 위치에 상관없이 모든 장치를 적절하게 감지하고 개요와 상세 정보를 파악할 수 있어야 합니다.

도표 1: 캠퍼스, IoT, 데이터 센터, 클라우드 및 운영 기술 전반의 세부사항 가시화

Forescout eyeSight은 중요한 비즈니스 프로세스를 방해하지 않으면서도 전체 장치 환경에 대한 탁월한 인사이트를 제공합니다. 먼저 기업 전체 네트워크의

IP에 연결된 모든 기기를 탐색합니다. 그러나 탐색은 완전한 가시성 확보를 위한 첫 번째 단계일 뿐입니다. 적절한 보안 정책을 만들고 관리하려면 종합적인 상황 파악이 반드시 필요합니다. eyeSight는 연결된 장치를 발견하면

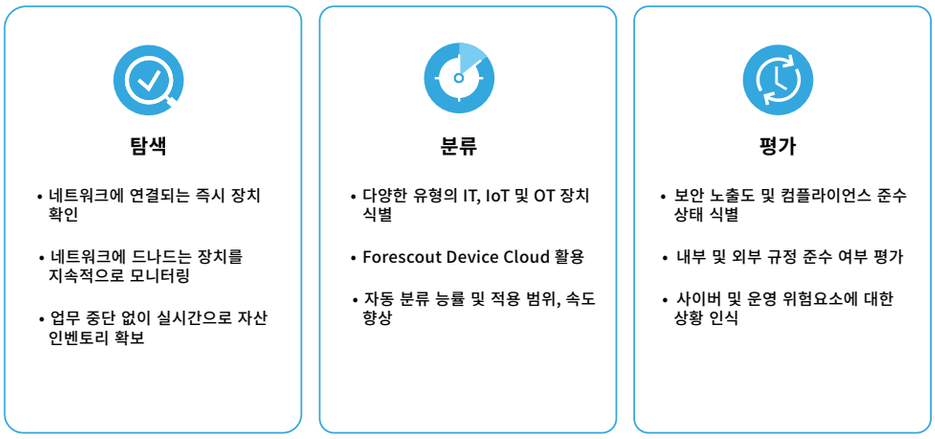
기업의 보안 정책에 따라 해당 장치를 자동으로 분류하고 평가합니다. 탐색, 분류, 평가라는 세 가지 강력한 기능을 통해 올바른 정책을 수립하고 관리하는데 필요한 가시성을 확보할 수 있습니다.

eyeSight

주요 기능

- 비에이전트 방식으로 네트워크 연결 장치의 통합 인벤토리 실시간 확보
- 정확한 장치 프로파일링을 통해 선제적 보안 및 컴플라이언스 정책 구축
- 악성 혹은 취약한 비규격 장치를 식별하고 위험성 제한 정책 생성
- 보안 툴 및 컴플라이언스 관리 작동 여부 실시간 확인
- 컴플라이언스 준수 상태와 사이버 위험 노출의 효율적인 측정 및 보고
- 공통적인 작업을 자동화하여 인적 오류를 최소화하고 효율성을 높임

도표 2: eyeSight가 제공하는 필수 가시성 기능



비에이전트 방식의 지속적인 탐색

IoT 및 OT 장치에는 가시성 부족이라는 고유의 문제가 있습니다. 이러한 장치의 수가 급증하자 기존의 수동 탐색 방식을 사용할 수 없게 되었습니다. 또한 IoT 및 OT 장치는 대부분 에이전트를 지원하지 않으며, 능동적인 탐색 기술 적용이 어려워 시스템 및 업무 중단을 일으킬 수 있습니다. eyeSight은 20가지 이상의 수동 및 능동 모니터링 기술(도표 3 참조)을 사용하여 다음과 같은 장치를 자동으로 발견해 잠재적인 가시성 문제를 방지합니다.

- 캠퍼스 네트워크에 연결된 노트북, 태블릿, 스마트폰, BYOD/게스트 시스템, IoT 장치
- 데이터 센터의 가상 머신, 하이퍼바이저, 물리 서버
- 개인 및 공용 클라우드의 AWS, Azure, VMware
- 운영 기술 네트워크에 연결된 의료, 산업, 건설 자동화 장치
- 스위치, 라우터, VPN, 무선 액세스 포인트, 컨트롤러 등 물리 및 소프트웨어 정의 네트워크 인프라

이러한 탐색 기능을 통합하여 운영상의 위험을 최소화하고, 네트워크 사각지대를 제거하여 기업 전반에 걸쳐 완전하고 지속적인 장치 인벤토리를 제공합니다.

도표 3: 능동 및 수동 탐색 기술.

인프라 수동 탐색	엔드 디바이스 수동 탐색	엔드 디바이스 능동 탐색
SNMP 트랩	네트워크 인프라 조사	비에이전트 방식의 윈도우 검사 • WMI • RPC • SMB
SPAN 트래픽	SDN 통합 • Meraki • Cisco ACI	비에이전트 방식의 MacOS, 리눅스 검사 • SSH
플로 분석 • 넷플로우 • 유연한 넷플로우 • IPFIX • sFlow	개인/공용 클라우드 통합 • VMware • AWS • Azure	NMAP
DHCP 요청	쿼리 디렉토리 서비스(LDAP)	SNMP 쿼리
HTTP 사용자 에이전트	쿼리 웹 애플리케이션(REST)	HTTP 쿼리
TCP 핑거프린팅	쿼리 데이터베이스(SQL)	SecureConnector®
프로토콜 파싱	eyeExtend 오케스트레이션	
RADIUS 요청		

과제

- 사일로화된 팀, 보안 도구, 프로세스의 가시성 차이
- 오류가 발생하기 쉬운 수동 프로세스로 인한 운영 및 비지니스 위험
- 불완전한 장치 인텔리전스로 상황파악이 미흡해 보안 방어 정책 수립이 어려움
- 보안 툴의 올바른 설치, 설정, 작동 여부 확인 불가
- 탐지되지 않은 악성 기기로 인해 보안 및 컴플라이언스에 불필요한 위험 발생
- 특정 시간에만 이뤄지는 구식 검사 기능으로 컴플라이언스 준수 상태에 대한 신뢰도 부족 초래

지능형 자동 분류

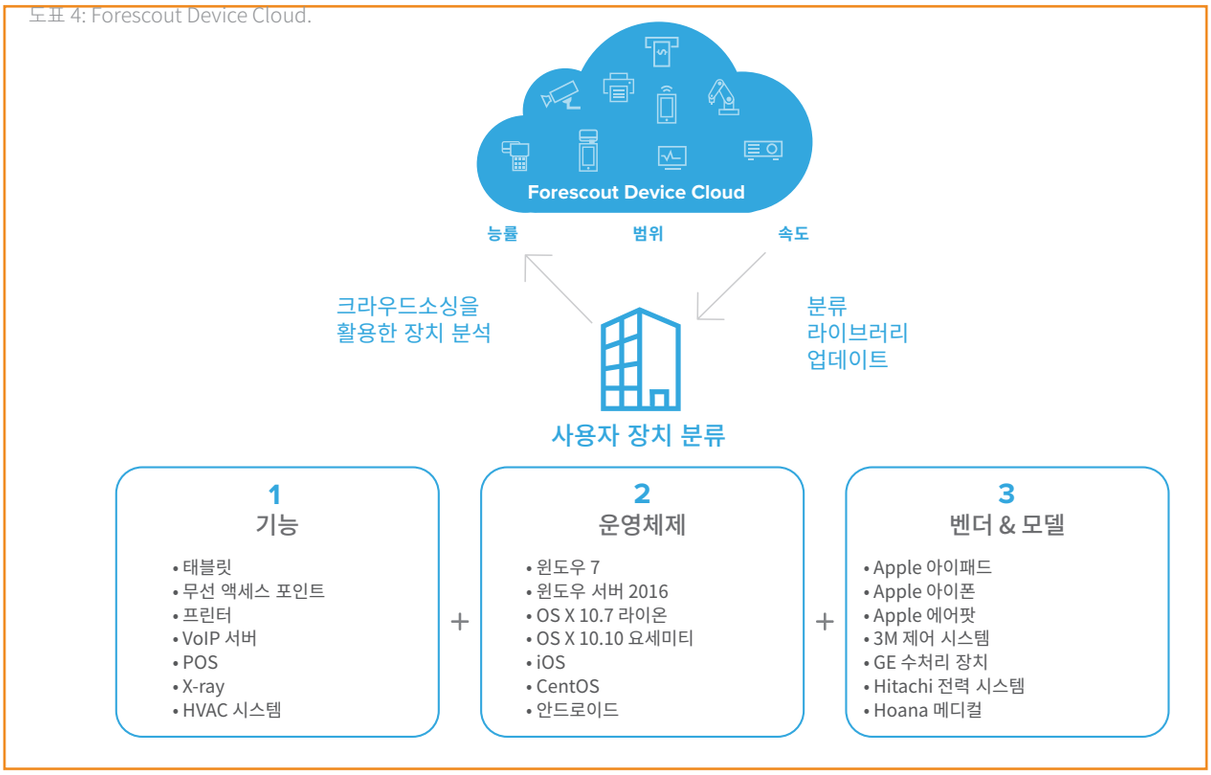
모든 장치에 대한 완벽한 컨텍스트는 세밀한 정책 생성에 필요한 핵심입니다. 각 장치의 작동 컨텍스트나 목적을 알면 최적의 보안 및 관리 방법을 찾을 수 있습니다. 장치의 수와 종류가 많아지면서 수동으로 컨텍스트를 수집하는 것이 불가능해졌습니다. 그러나 적절한 컨텍스트 없이 정책을 수립하면 보안 운영이 위험에 처할 수 있습니다. eyeSight는 다차원 분류 체계를 이용하여 장치 기능과 종류, 운영체제 및 버전, 벤더, 제품 모델에 따라 기존 장치 및 IoT/OT 장치를 자동으로 분류합니다. eyeSight는 100개 이상의 IT /OT 프로토콜 심층 패킷 검사를 통해 IoT 및 OT장치를 면밀히 식별할 수 있습니다.

eyeSight는 다음을 자동으로 분류합니다.

- 500가지 이상의 운영 체제 버전
- 5,000종이 넘는 장치 벤더 및 모델
- 350종 이상의 유명 의료 기술 벤더의 의료 장치
- 제조, 에너지, 석유 및 가스, 유틸리티, 광산업 등 주요 인프라 산업에서 사용되는 수천 종의 산업용 제어 및 자동화 장치

Forescout Device Cloud 가 eyeSight의 자동 분류 능력을 향상시켜, 풍부한 컨텍스트 자료가 장치의 성장 및 다양성을 지속적으로 따라잡을 수 있도록 합니다. Forescout Research는 장치 클라우드*를 통해 800만 대 이상의 실제 장치에서 정보를 얻어 인텔리전스를 개선합니다. 또한 장치 프로필을 자주 갱신하여 모든 장치 환경에서 분류 능률, 적용 범위 및 속도를 개선합니다.

도표 4: Forescout Device Cloud.



장치 상태 평가

장치 분류는 장치의 목적에 대한 운영 컨텍스트를 제공하여 해당 장치가 실제로 어떤 장치인지를 알려 줍니다. 그러나 완벽한 컨텍스트를 위해 각 장치의 보안 상태를 측정하려면 다른 평가 기준이 필요합니다.

eyeSight는 네트워크를 지속적으로 모니터링하고 연결된 장치의 구성과 보안 상태를 평가하여 장치의 위험도와 보안 및 규정 준수 여부를 확인합니다. eyeSight은 다음과 같은 항목을 평가합니다.

- 보안 소프트웨어가 설치 및 작동 중이며 현재 최신 패치가 적용되었습니까?
- 미승인 애플리케이션을 실행하거나 구성 표준을 위반하는 장치가 있습니까?
- 기본 비밀번호나 너무 쉬운 비밀번호를 사용합니까(IoT 장치에서 특히 위험함)?
- 스푸핑을 이용해 합법적인 장치로 위장한 장치 등 악성 장치가 감지되었습니까(그리고 해당 장치의 네트워크 연결 여부는 어떻습니까)?
- 연결된 장치 중 최신 위협에 가장 취약한 장치는 무엇입니까?

장치 인텔리전스의 능력

탐색, 프로파일링, 자동 분류, 평가를 통해 eyeSight가 제공하는 장치 가시성은 Forescout 콘솔에서 쉽게 확인할 수 있습니다. 맞춤형 대시보드를 통해 높은 수준의 인사이트를 얻을 수 있고, 위험도 및 목표한 컴플라이언스 진행 상황을 담은 스냅샷을 공유할 수 있습니다. 이와 같은 동적 보기는 다음과 같은 방식으로 팀을 지원합니다.

- 특정 정책이 성공적으로 적용되었는지 평가
- 신속한 사고 대응을 위해 위험에 취약한 장치를 식별
- 시간 경과에 따른 특정 컴플라이언스 준수 상태를 추적
- 경영진 및 감사관이 잠재적인 취약성을 비롯해 위험요소, 컴플라이언스 준수 상태를 즉시 파악 가능
- 특정 정책, 장치 유형, 위치 등의 문제를 해결하기 위해 드릴다운 분석을 진행

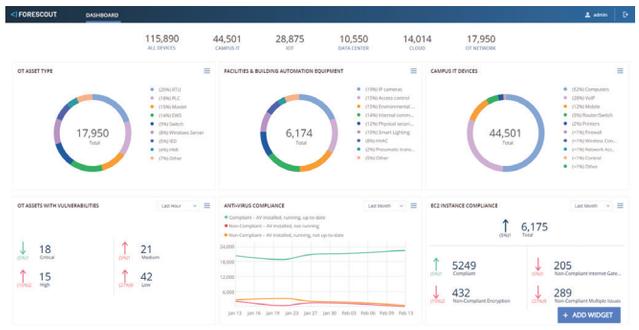


도표 5: 대시보드를 맞춤화하여 여러 관계자들이 필요에 따라 상황을 파악할 수 있게 합니다.

eyeSight의 장치 가시성은 알림 기능과 API를 통해 다양한 분야의 IT 관계자와 공유할 수 있습니다. eyeExtend 포트폴리오는 해당 장치의 컨텍스트를 다른 주요 정보 보안 제품과 공유하여 워크플로를 자동화하고 시스템 전체의 대응을 조정합니다.

기업에서 신뢰할 수 있는 제어 정책을 구현하기 위해서는 먼저 eyeSight를 통해 장치 컨텍스트를 정확히 파악해야 합니다. 불충분한 정보는 비즈니스 운영에 위험을 초래할 수 있기 때문입니다.

eyeSight는 사용자에게 심층적인 인사이트를 제공하며, 이를 통해 세분화된 정책을 설계 및 구현하여 자산 관리, 컴플라이언스 준수, 네트워크 접근, 네트워크 세분화, 사고 대응 등의 기능을 자동화할 수 있습니다. 또한 Forescout eyeControl 및 Forescout eyeExtend 제품을 사용하여 효과적으로 정책 기반 제어를 수립하고 기능을 오케스트레이션 할 수 있습니다.

자세히 알아보기 : Forescout.com

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA
수신자 부담 (미국) 1-866-377-8771
전화 (국제) +1-408-213-3191
지원 +1-708-237-6591