FORESCOUT

Active Defense for the Enterprise of Things™

Network Access Control – 통합 네트워크 접근제어 솔루션

CUDO COMMUNICATION

FORESCOUT

Active Defense for the Enterprise of Things™

EoT의 적극적인 방어

Why Forescout

EoT(Enterprise of Things, 사물 기업)의 적극적인 방어

EoT로의 변화는 순식간에 일어났습니다.
PC, 모바일 기기, 클라우드 워크로드, 그 밖의 기존 IT 시스템, 그리고 비에이전트 방식의 IoT 및 OT 장치. 말 그대로 전 세계의 인터넷 사용자가 폭증함에 따라 접속기기가 다양해지고 보안에 대한 부담감이 높아졌습니다.
가장 큰 문제는 기업 네트워크에 연동 되어있는 디바이스가 기업 운영에 영향을 주는 직접적인 요인으로 확인이 되며 잠재적 위험에 노출되고 있다는 점입니다. 따라서, EoT 위험에 관한 확인 및 보호가 Forescout는 기업과 조직의 규모에 따라 EoT를 적극적으로 방어하는 탁월한 솔루션을 제공합니다.

Forescout 제품

eyeSight

네트워크에 연결된 단말 탐지 및 자산분류, 평가를 할 수 있습니다

eyeControl

eyeSight가 탐지해 분류한 단말을 통제, 차단, 관리할 수 있습니다.

eyeSegment

기업 전사적으로 제로 트러스트 네트워크를 세분화하여 설계, 계획 및 구현을 가속화합니다.

eyeInspect

실시간 리스크 관리를 위해 패시브 방식으로 OT/ICS 장치를 지속적으로 검색, 분류, 모니터링합니다.

eyeExtend

타사 솔루션과 호환 가능한 보안 프로세스 및 보안 대응의 자동화를 통해 단말 컴플라이언스 강화, 운영 생산성 향상, 전반적인 보안 상태 개선을 이루어냅니다.

eyeExtend connect

고객의 사용자 지정 Application 보안 툴 및 관리시스템을 Forescout 플랫폼과 쉽게 커스텀 연동할 수 있습니다.

eyeManage

다수의 Forescout 장비들을 중앙집중관리할 수 있습니다.

eyeRecover

페일오버 클러스터링(Failover Clustering) 및 고가용성 페어링 옵션을 통해 단일 또는 다중 사이트 배포에서 Forescout 서비스의 연속성을 보장합니다.

Forescout
제품 소개

Forescout은 Agentless/Agent 방식을 모두 지원하는 Network Access Control (NAC) 글로벌 1위 제품입니다.
통합된 가시성과 제어를 통해 엔터프라이즈의 모든 자산을 식별 및 분류하고 내부 네트워크를 보호합니다.

가시성

- Agentless 방식으로 네트워크에 연결된 모든 장치를 실시간 탐지 및 분류
- 장치의 정확한 프로파일링을 통해 선제적 보안 컴플라이언스 구축
- 실시간 보안 설정 및 컴플라이언스 준수 여부 확인
- 탐색, 분류, 평가의 과정을 통해 기업의 보안 정책 수립 및 관리

탐지
- 네트워크 연결 즉시 장치 식별
- 네트워크 장치의 상태 변화 지속 모니터링
- 사각지대없이 실시간 자산 인벤토리 확보

분류
- 다양한 유형의 IT, IoT 및 OT 장치 식별
- Forescout Device Cloud 활용
- 자동 분류, 적용 범위, 탐지 속도 향상

평가
- 보안 위험도 감소 및 컴플라이언스 상태 식별
- 내·외부 규정 준수 여부 평가
- 운영 위험 요소 확인

컨트롤

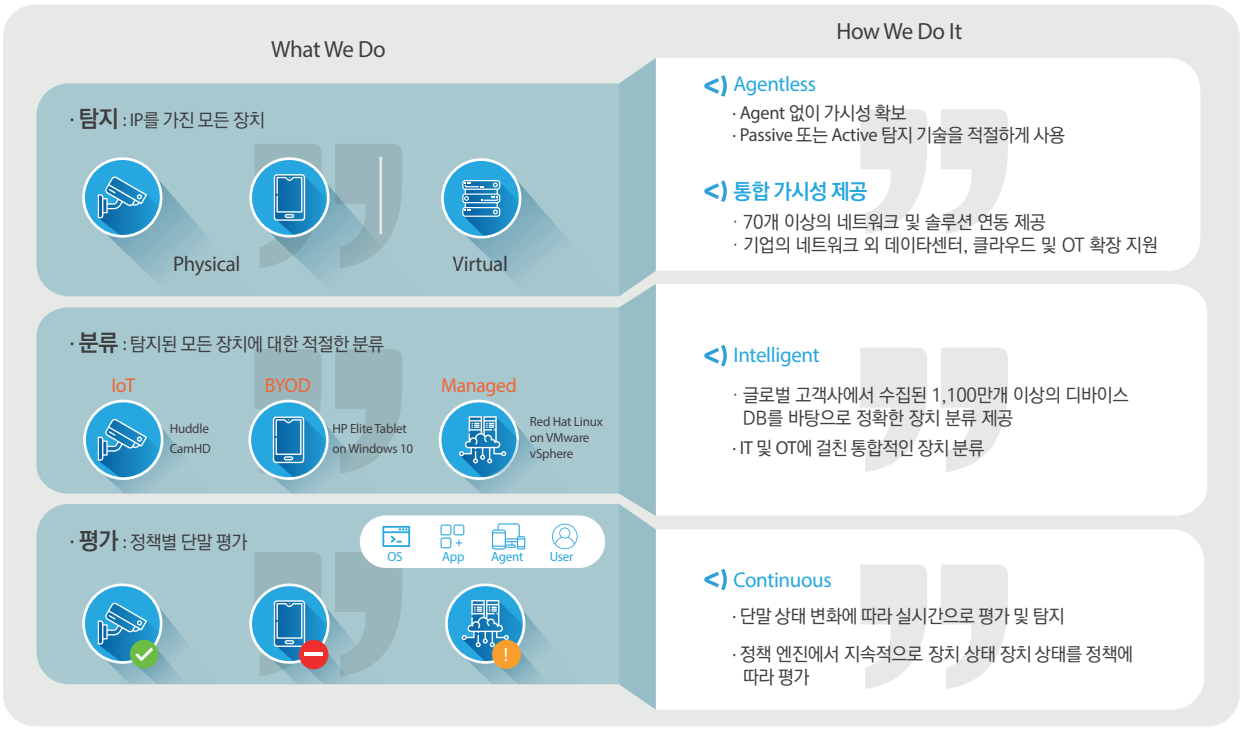
- 외부 위협으로부터 민감한 데이터 보호
- 취약한 장치에 대한 멀웨어 확산 및 감염 방지
- 직원, 관계사, 협력사, 방문자별 네트워크 접근제어
- 개별 상황에 적절한 조치를 제공하는 제어 기능 자동화

알림
- 네트워크 관리자 및 기타 IT/보안 시스템
- 호스트 또는 최종 사용자

제어
- 네트워크 및 호스트 기반 제어 기능을 통해 리스크 완화
- 보안 미준수 사용자에 대한 컴플라이언스 개선

통제
- 고위험, 감염 및 악의적인 엔드포인트 검역 또는 차단
- 위험성이 높은 컴플라이언스 미준수 단말 차단

Forescout의 eyeSight는 기업의 네트워크에 연결된 단말기를 100% 확인하고 분류합니다.



Forescout의 eyeControl은 세분화된 정책을 기반으로 모든 단말을 제어합니다.

일반적인 보안 설정

네트워크
- 게스트 네트워크 변경
- 미등록 무선 사용자 제한
- 각 장치별 VLAN 할당
- 장치/인프라 제한

호스트
- 필수 애플리케이션/프로세스 시작
- 안티바이러스/보안 에이전트
- 업데이트 OS 업데이트/패치 적용
- 외부 드라이브 규정 준수

정책 기반 제어 자동화

강도 높은 보안 설정

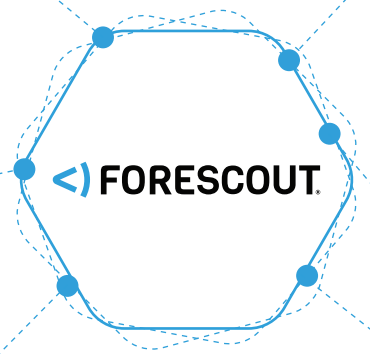
네트워크
- 장치 격리 (VLAN, 가상 방화벽)
- 스위치 포트 끄기
- 무선 또는 VPN 접근 차단
- ACL을 이용하여 접근 제한

호스트
- 인증되지 않은 앱 종료
- NIC/이중 네트워크 비활성화
- 주변 장치 비활성화
- 교정 조치/시스템 가동

정책 기반 제어 적용

- 802.1X Radius 설정 / Switch RO, RW 연동 및 정책 설정 지원
- AD 연동을 통해 Host 무결성 교정 조치 수행
- 단말 상태를 지속적으로 모니터링하고 교정 조치 수행
- 네트워크 구성 변경없이 비인가 장치 격리
- 게스트 단말 및 무선 단말에 자동 평가 관리

Forescout
6가지 주요 기능



자산 탐지 및 통합 관리
내부 네트워크의 모든 단말을 탐지하고
자동 자산 분류

3rd Party 솔루션 연동
고객만의 커스텀 에코시스템
구축 지원

사용자 인증
인증 서버와 연동 또는 자체인증
DB를 통해 사용자 인증 제공

단일 장비 구성
단일 Appliance로 모든 보안정책 구현이 가능하고
Out-of-Band(미러링) 방식으로 기존 네트워크에
영향을 주지 않는 구성

접근 제어
사용자 및 분류에 따른 구간별 네트워크 접근제어

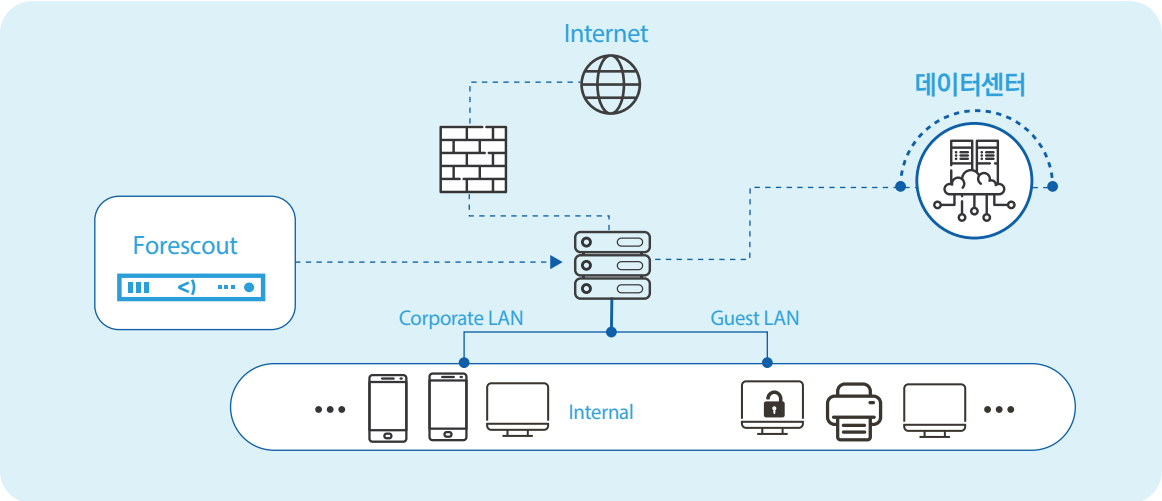
다양한 운영체제 지원
다양한 운영체제 (Windows, Linux, Mac 등) 에 대해
Agent / Agentless 방식으로 선택적 정책 운영 지원

Forescout
상세 기능 분류

구분	세부사항
OS 분류	Windows, Mobile, Linux, Mac, 공유기, VoIP, 네트워크 장치, 프린터 등
단말 정보	Hostname, Domain Name, User/ Name/ Email/ Title/ Groups (AD 연동 시) IP, MAC, Function, Nice Vendor, Browser Agent, Open ports, Protocols 탐지 H/W 정보 (Serial Number, 메인보드, CPU, Memory, Hard Disk 정보, 모니터 정보 등)
네트워크 정보	단말에 연결된 Switch/ Controller 에 대한 Port 정보
네트워크 접근제어	내부 직원, 협력사 직원, 방문자, 비인가 PC에 따라 네트워크 구간별 통제 ACL, Port Block, VLAN 이동, Virtual Firewall, HTTP Notification 등의 사용자 제어 IP/MAC에 대한 실시간 탐지 및 IP 충돌 방지 및 통제
외부 장치 제어	USB, Bluetooth, 핫스팟, 테더링 등 외부 장치 제어
OS 패치	Windows, Mac 최신 패치 확인 및 업그레이드 통제
포트 정보	Open 포트 확인, 사용자 별 서비스 포트 통제
S/W 설치 확인	Application Install, Service Running, Process Running 탐지
프로세스 제어	Process 실시간 구동 모니터링 및 비인가 프로세스 종료
Anti Virus 연동 및 제어	카스퍼스키, 안랩, 알약, 시만텍 등 국내외 38 종 백신 연동 백신 설치 유도, 미실행 단말 자동 실행, 최신 업데이트 자동화
방문자 인증 프로세스 지원	방문자 네트워크 사용 신청, 승인, 기간 및 게스트 별 네트워크 접근 제어
알림 및 공지	사용자 안내페이지 전송 및 관리자 또는 사용자의 Email 알림 전송
보안 기능	공유 폴더 제어, 비밀번호 유효성 검사, 화면보호기 제어, IE 보안 설정 제어, 윈도우 방화벽 제어, Windows / Mac / Linux Shell 스크립트 지원

구성 방안

Out-of-Band(미러링) 구성으로 설치되며, 기존 네트워크 구성 변경 없이 안전하게 구성됩니다.
(Forescout 장애시 기존 네트워크에 영향 없음)
하나의 Appliance를 통한 All-in-one 구성으로 추가적인 정책 서버, 차단 센서 등이 불필요합니다.(관리포인트의 감소)



구분	세부사항
단일 어플라이언스 시스템	· 별도의 센서 및 정책 서버 없이 단일 장비로 구성 · 장애/관리 포인트의 최소화
장비구성	· Out-of-band 구성 · 장비 설치 및 장애시 기존 네트워크 영향 없음
차단방식	· HTTP Redirect, 가상 방화벽, 스위치 제어(VLAN, 802.1x, ACL 제어), PC 제어
사용자 인증	· Active Directory, Radius (802.1x), LDAP, TACAS 등
VLAN 지원 개수	· 무제한 (Forescout 퍼포먼스 이내)
3rd 솔루션 연동	· Firewall / SIEM / APT / Anti Virus / Endpoint / EMM 연동 지원

Forescout Lineup

Flexx License (S/W 전용 라이선스)
- 탐지 단말 및 연동 스위치 수량 기준 라이선스 산정
- 100개 단위로 라이선스 추가 가능

S/W 모델 성능 사양	Extra-Small	Small	Medium	Large
탐지 단말 수	Up to 100	Up to 1,000	Up to 5,000	Up to 10,000
스위치 연동 개수	Up to 4	Up to 20	Up to 100	Up to 200
트래픽 모니터링 제한	Up to 100 Mb/s 25 KPPS	Up to 1 Gb/s 250 KPPS	Up to 3 Gb/s 750 KPPS	Up to 3 Gb/s 750 KPPS

Forescout
Web & **전용 UI**

자산 탐지 및 통합 관리

IP-MAC기반 모든 자산 실시간 탐지

· Out-of-Band & Agentless 모드 지원

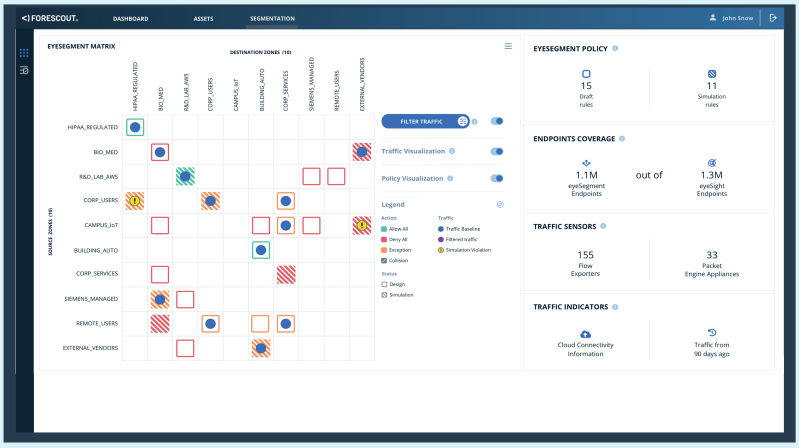
5,500개 이상의 IT, IoT, OT 벤더 및 Device 모델 자동 분류

· 차세대 DPI(Deep Packet Inspection) 기술
· IT, IoT, OT 장치 자동분류
(500+ OS / 5,000+ Vendor & Model)

광범위한 IT-OT-Cloud 전사 네트워크 가시성 제공

· 글로벌 시장 최초 IT-OT-Cloud 통합뷰 제공

Network Segmentation



전방향 트래픽 분석 및 시각화

· Traffic Flow 분석 (IP, User, App, Service 등)
· 실시간 데이터 분석 및 대시보드 제공

망분리 사전 테스트용 시뮬레이터

· 망분리 이전에 관리자가 원하는 정책으로 시뮬레이션
· 위반여부 즉시 확인 및 대응책 수립

최초 SaaS 방식 서비스

· Cloud 기반 SaaS 솔루션
· 엔터프라이즈 지원

CUDO COMMUNICATION

쿠도커뮤니케이션(주)

정보보안사업부: 06665 서울특별시 서초구 방배로 84 유성빌딩 4층
T. +82 2 525 0481 | E. secure@cudo.co.kr | W. www.cudo.co.kr | P. secure.cudo.co.kr | B. blog.naver.com/cudo_secure