FORESCOUT

Forescout 8.2의 새로운 특징

"2023년이 되었을 때 전 세계적으로 '연결된' 전체 IoT 디바이스 대수는 352억 대 이상으로 증가할 전망입니다."

– Worldwide IoT Forecast, 2019-2023, IDC

우리는 지난 10년간의 공격 양상을 보며 기업의 네트워크에서 단 한 군데라도 약점이 있으면 보안 침해에 취약하게 된다는 사실을 깨달았습니다. 더 많은 IoT 및 기타 관리되지 않는 디바이스가기업 네트워크에 연결하여 디지털 전환의 원동력이 됨에 따라, 이런 디바이스와 네트워크의 보호라는, 혁신과 똑같이 중요한 목표를 혁신 목표와 조화롭게 추구할 긴급한 필요가 있습니다.

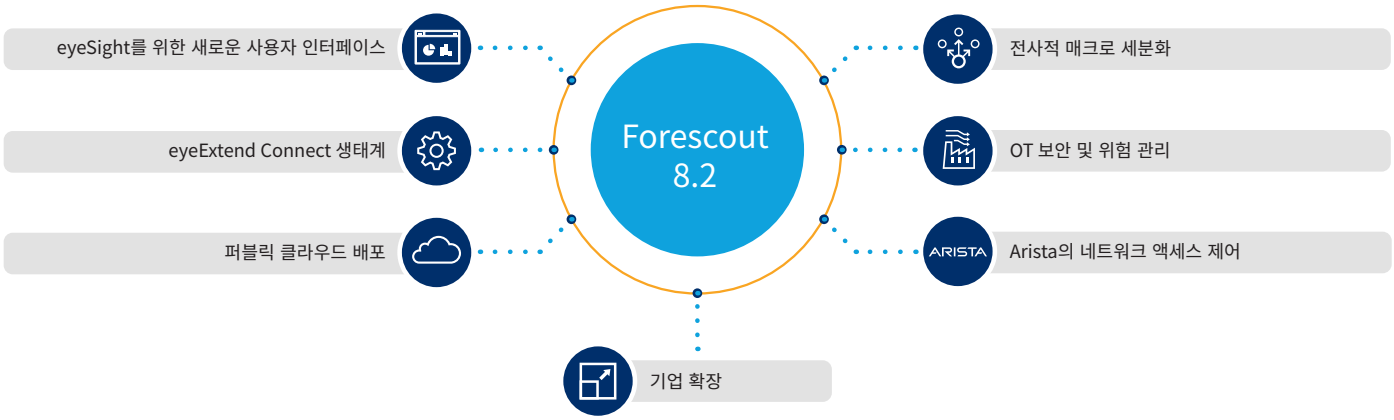
네트워크 도메인 전체에 걸쳐 연결된 디바이스에 대해 완전히 파악하지 못할 경우, 위험 완화를 위해 빠르게 대응하는 능력을 거의 잃게 됩니다. 레거시 및 취약한 디바이스, 규정 미준수 엔드포인트와 잘못 구성된 엔드포인트, IoT 및 운영 기술을 모두 식별해야 합니다. 상호 연결된 모든 네트워크와 모든 위치에 대한 위험을 계속 평가해야 합니다. 이처럼 완벽한 가시성을 확보하면 빠르게 행동으로 옮길 힘을 갖게 됩니다.

Forescout 8.2: 더 빠르게 식별하고 행동하세요

Forescout 8.2는 연결된 모든 디바이스, 컴플라이언스 격차, 네트워크상의 위험을 더 빠르게 식별할 수 있게 해줍니다. 이를 통해 자신 있고 빠르게 행동하여 확장된 엔터프라이즈 네트워크 전체에 걸쳐 보안 노출을 완화하고 평균 응답 시간(MTTR)을 줄일 수 있습니다.

주요 사항:

- 위험을 정확히 파악해 우선순위를 정하고 사전 예방적으로 위험을 완화하기 위해 실행 가능한 디바이스 컨텍스트를 포함하여 Forescout eyeSight를 위한 새로운 페르소나 중심 사용자 인터페이스
- 고객과 파트너가 Forescout 플랫폼과 통합하기 위한 앱을 더 쉽게 빌드, 사용 및 공유할 수 있도록 지원하는 새로운 커뮤니티 기반 앱 생태계인 Forescout eyeExtend Connect
- AWS 및 Microsoft Azure 퍼블릭 클라우드 환경에 Forescout 어플라이언스를 배포하기를 원하고 클라우드 우선주의를 채택한 기업을 위한 새로운 배포 유연성과 더욱 빨라진 가치 실현 시간
- Forescout eyeSegment를 사용한 전사적 세분화를 통해 기업이 여러 네트워크 도메인과 다양한 적용 지점에 걸쳐 자신 있게 정책을 설계하고 구현할 수 있도록 지원
- IP 범위가 겹치는 복제 네트워크를 포함하여, IT 및 OT 도메인에 걸쳐 통합 가시성을 위해 Forescout SilentDefenseTM뿐 아니라 동일한 어플라이언스에 내장된 IT/OT 센서와 통합
- IT 및 IoT 디바이스를 위해 802.1X에 의존하거나 에이전트를 사용할 필요 없이 Arista 인프라와의 직접적인 통합을 통한 네트워크 액세스 제어



새로운 사용자 인터페이스

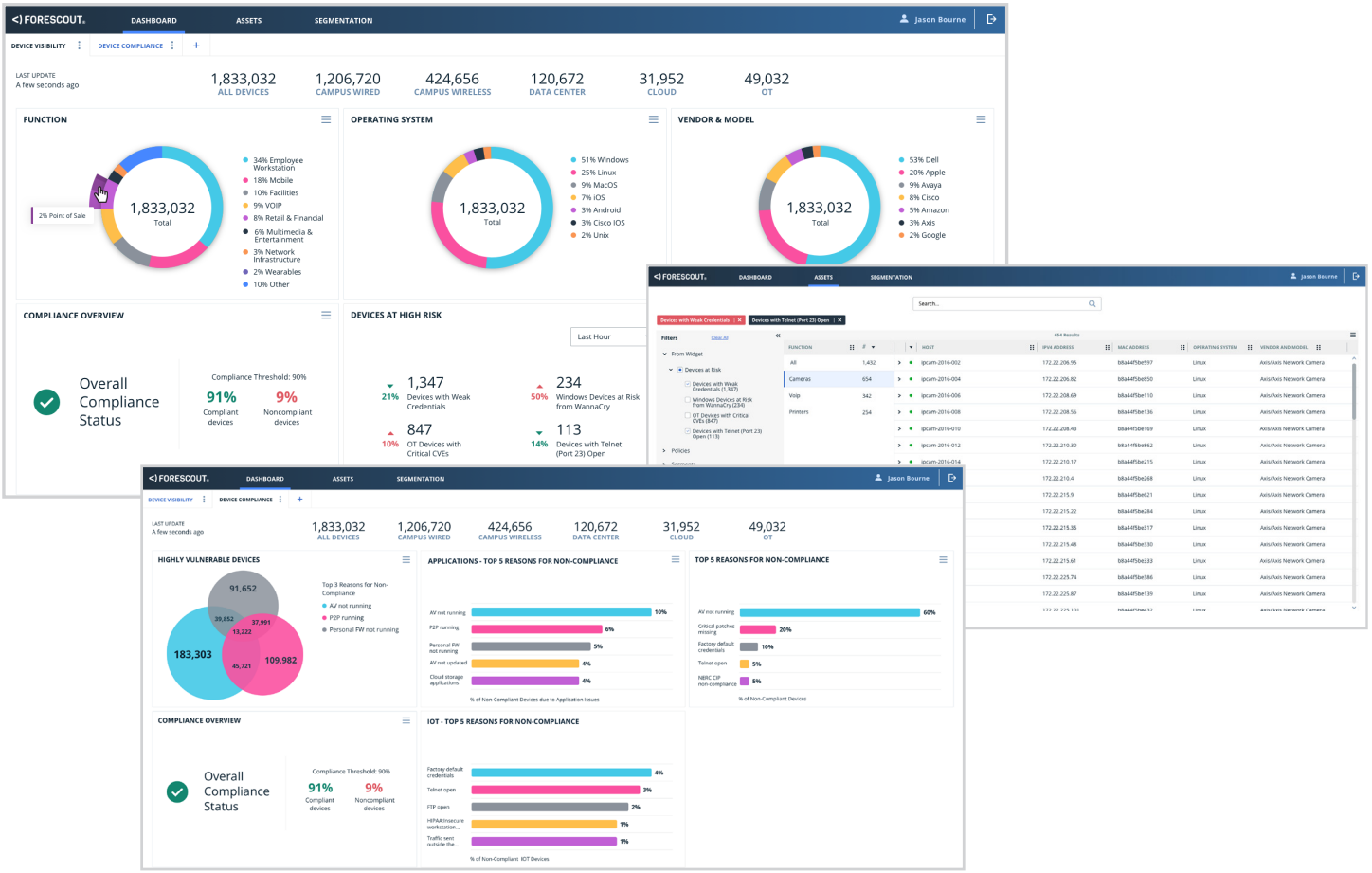
모든 이해관계자가 새로운 웹 기반 사용자 인터페이스를 통해 제공되는 페르소나 중심의 컨텍스트와 실행 가능한 인사이트의 이점을 누립니다. 대시보드는 연결된 디바이스를 시각화하고, 위험성이 가장 높은 영역을 팀에 경고하고, 컴플라이언스 목표 대비 진행 상황을 강조 표시해 줍니다. 운영자는 풍부한 드릴다운 기능을 가진 실시간 디바이스 인벤토리를 통해 디바이스를 빠르게 찾아 기업이 위협에 한발 앞서 대응할 수 있습니다. 간단한 사용자 지정 및 공유 옵션 덕분에 용이하게 IT 직무 담당자 전체에게 위험을 알려 빠르게 대응하도록 할 수 있습니다.

더 빠르게 통찰력 확보. 기본 제공 디바이스 가시성과 컴플라이언스 대시보드를 사용하여 다음을 수행할 수 있습니다.

- 연결된 모든 디바이스의 기능, 운영 체제, 벤더 및 모델 식별
- 유효한 모든 정책에 대해 컴플라이언스의 임계 수준 설정 및 모니터링
- 다음과 같이 위험도가 높은 디바이스를 정확히 파악
  - 약한 자격 증명, 열린 포트 또는 기타 구성이 잘못된 IoT 디바이스
  - 보안 업데이트 또는 취약점이 없는 Windows 디바이스
  - 보안 에이전트가 손상되거나 권한이 없는 애플리케이션이 있는 디바이스
  - 중요한 공통 취약점 및 노출(CVE)을 가진 OT 디바이스
- 자주 발생하는 장애를 포함한 정책 위반뿐 아니라, 여러 정책에 걸쳐 호환되지 않는 디바이스 식별(예: 방화벽 또는 바이러스 백신 없이 실행 중인 P2P 애플리케이션).

격차를 미리 해결. 새로운 웹 기반 자산 뷰를 사용하여 다음 작업을 신속히 수행합니다.

- 구내, 데이터 센터, 클라우드 및 OT에 걸쳐 전체 디바이스 인벤토리 검색
- 정책, 네트워크 세그먼트 및 디바이스 속성을 기준으로 필터링
- 더욱 빠른 MTTR을 위해 디바이스 위치를 정확히 파악



eyeExtend Connect App 생태계

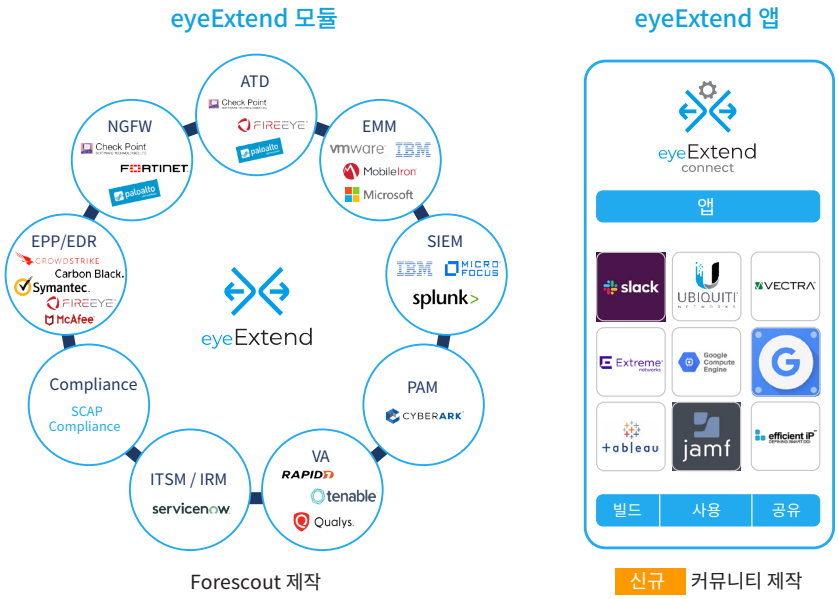
고객은 Forescout 플랫폼을 활용해 다른 IT 및 사이버 보안 기술과 통합하여 디바이스 컨텍스트를 공유하고 워크플로를 오케스트레이션하고 응답을 자동화합니다. Forescout의 현재 eyeExtend 모듈 포트폴리오는 25개 이상의 선도적인 제품과의 기본 제공 통합을 제공하고 기존 투자의 가치를 확장할 수 있도록 지원합니다. Forescout가 만들고 지원하는 이러한 솔루션 외에, Forescout 8.2는 추가적인 기술과의 통합을 지원하는 새로운 커뮤니티 기반 앱 생태계를 제공합니다.

eyeExtend Connect는 크라우드소싱의 힘을 활용하여 고객과 파트너가 모두 Forescout 플랫폼과 연결하기 위한 앱을 빠르게 빌드, 사용 및 공유할 수 있도록 해줍니다. 손쉽게 다른 도구와 디바이스 컨텍스트를 공유하고, 워크플로를 자동화하고, 시스템 전체의 응답을 가속화해 MTTR을 줄이는 조치를 취할 수 있습니다.

빌드하기 쉽습니다. 가치 실현 시간의 단축을 위해 범용 Python 스크립팅 및 JSON 데이터 교환 표준을 사용하여 자체 앱을 만드는 유연성을 확보하십시오.

사용하기 쉽습니다. 쉽게 배포하고 사용자 지정할 수 있고 여러 네트워크 환경 간에 이식할 수 있는 다양한 커뮤니티 제작 앱 중에서 원하는 앱을 선택하십시오.

공유하기 쉽습니다. 커뮤니티 모범 사례에 기여하고 그로부터 배우며, 동료들과 앱을 공유하고, 크라우드소싱을 활용하여 IT 투자의 가치를 확장하십시오.



전사적 매크로 세분화

Forescout 8.2는 여러 네트워크 도메인과 다양한 적용 지점에 걸쳐 전사적 세분화를 위해 eyeSight와 eyeControl의 최신 혁신 기술로 eyeSegment를 보완합니다. 이처럼 완벽한 경험을 할 수 있도록, 네트워크 세분화와 Zero Trust 보안을 자신 있게 적정 규모로 설계 및 구현할 수 있습니다.

- 사용자, 디바이스, 애플리케이션 및 서비스의 논리적 분류 체계 간의 트래픽 흐름 매핑 및 시각화
- 정책을 적용하기 전에 정책의 영향을 파악하기 위해 논리적 세분화 정책 설계, 시뮬레이션 및 구체화
- 실시간으로 세분화 안전 상태 모니터링 및 정책 위반에 대응
- 네트워크 도메인과 다양한 적용 지점 전반에 걸쳐 자신 있게 세분화 제어 적용

OT 환경에서 보안 및 위험 관리

SilentDefense와 Forescout 8.2 사이에서 통합을 활용하여 OT 및 통합된 환경에서 다양한 보안 및 위험 관리 사용 사례를 다룹니다.

- SilentDefense에서 받은 OT 디바이스 분류 및 취약점 정보를 eyeSight와 공유하고 IT 및 OT 네트워크 전체에서 통합된 가시성을 위해 새로운 eyeSight 사용자 인터페이스를 사용함
- 같은 어플라이언스에 내장형 IT 및 OT 센서를 설치하여 통합된 환경에서 디바이스를 검색하고 분류함
- 여러 사이트, 생산 라인 또는 플랜트에서 중복 IP 주소 범위를 재사용하는 복제 네트워크 환경에서 디바이스를 고유하게 식별하고 정책을 적용함
- 향상된 NERC CIP 컴플라이언스 보고, 더욱 심도 깊은 가시성을 위한 선택적 검사와 비침입적 능동 검사, 여러 위험 요소를 영향을 기반으로 하는 점수로 집계하는 자산 위험 프레임워크를 포함하여, OT 환경에서 SilentDefense의 최신 기능을 사용함

Arista 환경의 네트워크 액세스 제어

Forescout 8.2에는 Arista뿐 아니라 유형이 다른 환경에서 네트워크 액세스 제어를 적용하기 위해 Arista 인프라와의 직접적인 통합도 포함됩니다. 이를 통해 에이전트를 사용하거나 802.1X에 의존할 필요 없이 IT 및 IoT 디바이스를 모두 식별하고 조절할 수 있습니다.

- IoT 및 IT 디바이스가 네트워크에 연결될 때 이들을 모두 실시간으로 식별 및 평가
- 디바이스 유형, 소유권, 사용자 역할, 디바이스 컴플라이언스 및 보안 태세를 포함하여, eyeSight와 타사 컨텍스트를 기반으로 하는 알맞은 네트워크 액세스 프로비저닝
- 디바이스 제한, 구분, 격리 또는 차단과 같은 상황에 따라 다양한 네트워크 응답을 자동화하여 위험 완화

퍼블릭 클라우드 배포

기술에 대해 클라우드 우선 접근 방식을 채택한 기업은 디바이스 가시성과 제어를 위해 온프레미스 환경의 물리적 배포 또는 가상 배포에 제한을 받아왔습니다. Forescout 8.2를 사용하면 구내에 따로 설치 공간을 둘 필요 없이 Amazon Web Services 또는 Microsoft Azure 클라우드 환경에 Forescout 센서 어플라이언스와 엔터프라이즈 관리 기능을 배포할 수 있습니다. 또한, VMware, Hyper-V 또는 KVM 프라이빗 클라우드 인프라에 있는 물리적 어플라이언스 및 가상 어플라이언스와 퍼블릭 클라우드 배포를 혼합할 수 있는 유연성도 확보합니다.

물리적 | 가상 | 퍼블릭 클라우드 | 하이브리드
상기 사항 중 일부 또는 전부를 혼합

기업 확장

Forescout 8.2는 대기업의 엄격한 요구 사항을 충족시키고 구내, 데이터 센터, 클라우드, IoT 및 OT 환경 전체에 걸쳐 연결된 디바이스의 폭발적 증가세에 보조를 맞추기 위해 최고의 확장성을 제공합니다.

- 연결된 IoT, OT 및 IT 자산의 더욱 정확하고 빠른 식별을 위해 1,100만 개 이상의 엔터프라이즈 디바이스에 대한 최대의 디바이스 클라우드 기술 자료를 사용하여 디바이스 분류
- 물리적, 가상, 클라우드 또는 하이브리드 구현 여부에 상관없이, 단 한 번의 배포로 2백만 개의 디바이스 관리

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Forescout.com에서 자세히 알아보세요