Forescout eyeExtend Connect

Forescout 플랫폼과 손쉽게 통합하여 상황에 맞는 디바이스 관련 정보 획득 및 전사적 차원의 위협 대응 가속화

보안 및 IT 기술 투자에서 파생되는 가치를 증대하기 위해, Forescout 고객은 별도의 구성 절차 없이 바로 9가지 인기 보안 기술 분야의 제품과 통합할 수 있는 이점을 누리고 있습니다. 이러한 통합은 보안 워크플로의 오케스트레이션을 통해 놀라울 정도로 효율성을 높여주고 있습니다. 이러한 사전 제작 제품 외에도, 이제 Forescout는 고객이 기존에 보유한 기술을 더 많이 Forescout 플랫폼과 더욱 빠르고 쉽게 통합할 방법을 제공하고
있습니다. 고객 및 파트너 커뮤니티는 이제 Forescout의 신제품인 eyeExtend Connect를 사용해 Forescout 플랫폼을 다른 기술과 연결해주는 eyeExtend Apps를 빠르게 빌드, 사용 및 공유할 수 있습니다. 커뮤니티에서는 이를 통해 Forescout의 심층적인 디바이스 컨텍스트로 기존 보안 제품의 잠재적 가치를 끌어내고, 별개의 솔루션 간에 보안 워크플로와 정책 적용을 자동화하고, 시스템 전체의 응답을 가속화해 위험을 완화할 수 있습니다.

솔루션

Forescout eyeExtend Connect는 사용 및 배포하기 쉬운 앱의 생성을 단순화해 줍니다. 이제 Forescout eyeExtend Apps를 통해 Forescout 플랫폼을 IT 및 보안 기술과 수월하게 통합하고 여러 가지 사이버 보안 기술 사이의 보안 워크플로를 오케스트레이션할 수 있습니다.

eyeExtend Connect가 있으면 기존의 보안 기술에서 디바이스 속성, 보안 태세, 디바이스의 회사 정책 컴플라이언스 여부, 네트워크상의 위치, 사용자 컨텍스트 등을 비롯하여, Forescout eyeSight 데이터의 심층적인 디바이스 컨텍스트를 활용할 수 있습니다. 다른 IT 또는 보안 제품이 이 디바이스 데이터를 자동으로 풀하거나 Forescout 플랫폼으로 자체 데이터를 푸시할 수 있습니다. 또한, eyeExtend Connect는 시스템 전반의 정책 기반 작업을 자동화하여 위협, 사고 및 컴플라이언스 격차를 완화할 수 있게 함으로써 위협 대응을 가속화하는 데도 도움이 됩니다.

eyeExtend Connect는 워크플로 오케스트레이션과 디바이스 컨텍스트 공유를 사용할 수 있는 다음 도구를 제공합니다.

eyeExtend connect

도전 과제

- Forescout 또는 기술 파트너의 사전 제작 통합 제품에 대한 의존으로 다른 사내 보안 기술과의 워크플로 오케스트레이션 배제
- 맞춤 제작 방식의 통합을 위한 개발 주기가 길어 기존 보안 투자의 가치 실현 시간이 늘어남
- 보안 사고에 대응할 때 디바이스 및 사용자 컨텍스트 정보를 공유하지 않고 독자적으로 작동하는 보안 도구를 사용하면 많은 수작업이 필요하므로,

이점

- 모든 유형의 타사 도구와 통합함으로써 기존의 기술 투자 수익률 극대화
- eyeExtend Apps를 통해 Forescout 플랫폼과 쉽고 빠르게 통합함으로써 가치 실현 시간 단축
- IT 및 보안 도구가 함께 더 잘 작동하도록 하고, 실행 가능한 디바이스 관련 정보를 더 빠르게 획득하고, 위험과

주요 사항

- 개방형 Forescout 플랫폼과 통합할 수 있도록 eyeExtend Apps를 쉽게 빌드 및 배포
- 커뮤니티와 앱을 공유하여 피드백을 주고받음
- Python 스크립트와 JSON 구성으로 이식 가능한 앱 빌드
- 광범위하고 다양한 타사 웹 서비스 통합
- 타사 디바이스 컨텍스트와 컨트롤로 Forescout의 가시성 및 제어 기능 확장
- 개방형의 표준 기반 REST API로 양방향 통합 지원
- 표준 SQL(Structured Query Language) 안팎으로 정보를 푸시 및 풀
- 표준 LDAP 서버 안팎으로 정보를 풀하고 푸시하기 위한 사용자 지정 쿼리 생성

eyeExtend Apps

주요 Forescout 플랫폼 기능을 활용하는 앱을 빌드하여 엔드포인트 컨텍스트를 학습 및 공유하고, 네트워크 제어 조치를 취하고, 시스템 전체의 정책을 적용합니다. eyeExtend Connect는 eyeExtend Apps를 이식 가능하게 만들도록 파라미터, 태그 및 사용자 제어 구성을 정의하기 위해 사용하기 쉬운 JSON 스키마를 제공합니다(테스트에서 프로덕션으로, 리전 A에서 B로, IT 환경에서 OT 환경으로 마이그레이션). 또한, 타사 API 상호 작용은 빌드할 수 있는 통합의 유형을 확장함으로써 상당한 유연성을 제공하는 인기 Python 스크립트로 정의됩니다. 앱에 빌드할 수 있는 정책 템플릿으로 위협 완화, 사고 대응, 컴플라이언스 관리와 같은 필수적인 사용 사례와 적용을 자동화할 수 있습니다.

eyeExtend Apps의 주요 특징:

- 플러그 앤 플레이
- 새 디바이스 및 속성 검색
- 외부 타사 제어 작업
- 사용자 지정 정책 템플릿
- 스크립트 가능한 API 상호 작용
- 사용자 지정 가능한 타사 아이콘

WebAPI 및 DEX(DataExchange)

Forescout 플랫폼은 외부 애플리케이션을 사용하여 Forescout 디바이스 속성과 정책 정보를 검색할 수 있는 RESTful API 집합을 제공합니다. DEX(Data Exchange) 플러그인은 실시간 디바이스 컨텍스트를 공유하기 위해 Forescout 플랫폼과 타사 RESTful API 사이의 양방향 통신을 지원합니다.

SQL

DEX 플러그인은 표준 SQL 데이터베이스 안팎으로 정보를 푸시하고 풀할 수 있습니다. 이러한 유형의 통합으로 자체 개발 애플리케이션이 외부 또는 내부 데이터베이스를 통해 인터페이스할 수 있는 타사 제품과 정보를 공유할 수 있습니다. 외부 데이터베이스에서 정보를 쿼리하고 Forescout 플랫폼이 검색하는 데이터를 저장하는 호스트 속성을 생성할 수 있습니다. 이러한 호스트 속성을 Forescout 정책에서 사용하고 NAC(네트워크 운영 체제) 및 인벤토리 뷰에서 볼 수 있습니다. 또한, 일반적으로 타사 제품이 작동하는 Forescout 플랫폼에 의해 수집된 정보를 기반으로 외부 데이터베이스를 업데이트할 수도 있습니다.

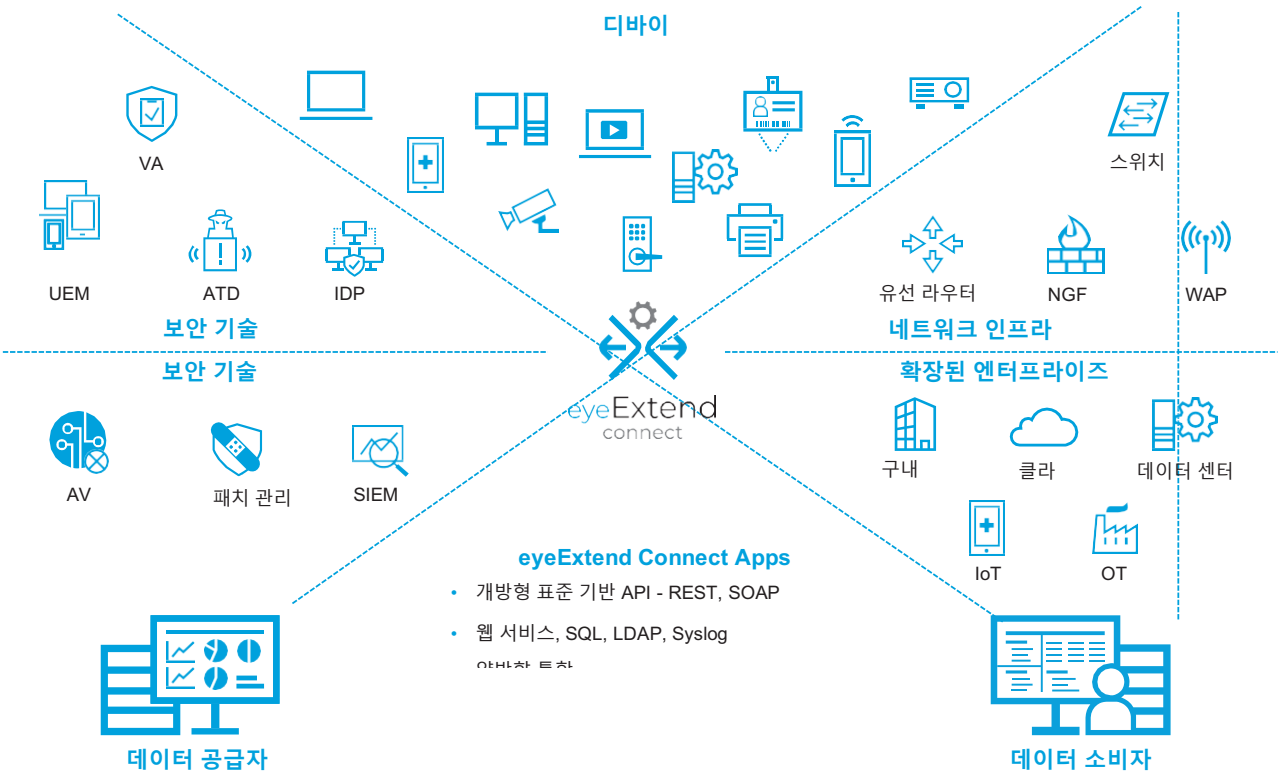
LDAP

표준 LDAP 서버 안팎으로 정보를 푸시하고 풀하기 위해 DEX 플러그인을 통해 사용자 지정 쿼리를 생성합니다. 예를 들어, LDAP 서버에서 정보를 쿼리하고 검색된 데이터를 저장하는 Forescout 호스트 속성을 생성할 수 있습니다. 이러한 호스트 속성을 Forescout 플랫폼 정책에서 사용하고 NAC 및 인벤토리 뷰에서 볼 수 있습니다.

Syslog

Syslog를 통해 지정된 서버로 정보를 송수신하도록 DEX 플러그인을 구성할 수 있습니다. 이 유형의 인터페이스는 보안 정보 및 이벤트 관리(SIEM) 제품처럼, 로그를 집계하고 로그 분석을 지원하는 제품 또는 이러한 방식으로 경고를 송수신할 수 있는 다른 솔루션과의 다양한 통합용으로 사용됩니다. 메시지 형식은 사용자 지정 가능합니다.

그림 1: 다양한 디바이스, 환경 및 보안 기술에 걸친 워크플로 오케스트레이션



VA: 취약점 평가, ATD: 고급 위협 보호, IDPS: 네트워크 침입 방지, UEM: 통합 엔드포인트 관리,
AV: 바이러스 백신, SIEM: 보안 정보 및 이벤트 관리, WAP: 무선 액세스 포인트, NGFW: 차세대 방화벽

일반적인 사용 사례

Forescout는 특정 사용 사례에 대한 해결책을 제시하기 위해 바로 사용 가능한 25가지 솔루션을 제공하는 반면, eyeExtend Apps를 사용하면 고객의
사용자 지정 사용 사례를 해결할 수 있습니다. 몇 가지 예를 들면 다음과 같습니다.

네트워크 연결 디바이스가 연결되는 순간에 그 모든 디바이스 검색, 분류 및 평가

Forescout eyeSight로 구동되는 Forescout eyeExtend Connect는 통합 IT 또는 보안 제품이 구내, 데이터 센터, OT 및 클라우드 환경에서 디바이스를 더 잘 식별하기 위한 컨텍스트를 제공할 수 있도록 지원합니다. 예를 들어
eyeExtend App for Ubiquiti는 고객이 Wi-Fi 연결 디바이스에 대한 가시성을 높이고 발견하는 디바이스 특성을 사용하여 Forescout 플랫폼에서 더 나은 정책 의사결정을 내리는 데 도움이 됩니다. eyeExtend App for Ubiquiti는 이제 다른 IT 서비스 관리(ITSM) 또는 자산 관리 제품에 Ubiquiti Wi-Fi 연결 디바이스 정보를 제공하여 CMDB를 올바르게 만들 수 있습니다. 또 다른 중요한 앱인 eyeExtend App for Google Cloud는 Google Cloud와 통합하고 Google Cloud 인벤토리 컨텍스트를 끌어옴으로써 고객이 진화하는

클라우드 컴퓨팅 인스턴스에 대한 실시간 가시성을 얻는 데 도움이 됩니다.

네트워크에 액세스하는 VPN 연결 디바이스에 대한 가시성과 제어 기능 개선

eyeExtend Connect는 VPN을 통해 회사 네트워크에 연결하는 모든 디바이스를 식별합니다. 보안 운영자는 Forescout 플랫폼과의 통합을 활용함으로써 VPN을 통해 연결하는 자산이 회사 자산인지 여부를 확인하고 권한 없는 위치에서 연결하는 디바이스의 액세스를 제어할 수 있습니다.

보안 또는 IT 정책 위반 정책 워크플로를 오케스트레이션

다양한 협업 및 메시징 플랫폼을 사용하여 정책 위반에 대한 실시간 경고를 보냅니다. 네트워크 제어 작업을 자동화하기 위해 정책 의사결정을 내릴 때 이메일, 메시징 또는 협업 플랫폼을 통해 Forescout 플랫폼에서 디바이스 사고 데이터를 가져오는 정책을 설정할 수 있습니다. 예를 들어, eyeExtend App for Slack은 협업 플랫폼과 통합하여 Slack을 통해 IT 또는 보안 팀에서 사용하는 채널로 정책 위반에 대한 실시간 경고를 보냅니다.

모바일 디바이스 등록 자동화, 보안 관리 개선 및 지속적인 컴플라이언스 적용

eyeExtend Connect는 유형(PC, Mac, Linux®, 태블릿, 스마트폰), 연결(유선, 무선, VPN) 또는 디바이스의 소유권(회사 또는 개인)에 상관없이 디바이스 정보 공유 및 제어 작업을 UEM 시스템과 오케스트레이션하여 네트워크상의 디바이스에 대한 통합 보안 정책 관리를 제공합니다. 이 포괄적인 디바이스 관리를 통해 디바이스 등록 자동화, 정책 기반 작업을 통한 디바이스 컴플라이언스 적용, 사용자 지정 네트워크 액세스 제어 적용, 응답 동작 및 수정의 가속화가 가능합니다. 예를 들어, 고객은 eyeExtend App for Google Mobile Management를 사용하여 Chromebook 디바이스 컨텍스트를 볼 수 있습니다. 이 데이터는 회사 BYOD 보안 및 액세스 정책의 구체화에 도움이 됩니다.

IT 및 보안 제품 생태계 내에서 작업과 워크플로를 자동화하여 전사적으로 운영 개선 및 보안 강화

eyeExtend Connect는 Forescout 플랫폼 또는 다른 통합 제품에 특정한 조치를 취하도록 지시하는 작업 트리거를 송수신할 수 있습니다. 이러한 트리거는 인간 작업자가 필수적인 플레이북에 기반한 의사결정이 아니라, 정책 기반 자동화에 기반을 둡니다. 이는 전반적으로 더 빠른 응답 시간과 더 안전한 네트워크로 이어집니다.

사고 대응 가속화를 위한 상관관계 분석을 위해 심층적이고 상황에 맞는 디바이스 데이터 활용

eyeExtend Connect 덕분에 Forescout 플랫폼이 상관관계 분석을 위해 SIEM 시스템으로 심층적인 디바이스 데이터를 제공할 수 있습니다. eyeExtend Connect는 전체적인 기업 공격 표면을 완벽하게 파악하게 하여, 통찰에 필요한 시간 단축에 도움이 되고, 수월하게 조사할 수 있게 해줍니다. 또한, Forescout 플랫폼은 정책 기반 작업을 자동화하고 SIEM에서 실시간으로 제공되는 사고 심각도 정보를 기반으로 네트워크에 대한 디바이스의 액세스를 제한함으로써 보안 작업을 간소화하는 데도 도움이 됩니다.

요컨대, eyeExtend Connect는 보안 도구를 손쉽게 공유할 수 있도록 하고 고도로 지능적인 Forescout 플랫폼에 연결하여 위협 완화 및 정책 컴플라이언스를 상당히 자동화함으로써 더 높은 보안 ROI를 빠르게 달성하는 데 도움이 됩니다.

참고: eyeExtend Connect의 일부 기능은 이전에 OIM 제품에 속했던 기능입니다. 이전의 모든 OIM 기능은 현재 eyeExtend Connect에 포함되어 있습니다.

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