Forescout eyeControl

공격 노출도 감소와 신속한 사고 대응을 위해 정책 기반 제어를 적용하고 자동화합니다.

IT 보안 팀이 보고받는 보안 및 규정 준수 문제는 점점 넘쳐나고 있습니다.

방대한 보안 툴 모음은 적절한 조치를 취하지 못하고 계속 경고 알림만 전송합니다. 안타깝게도 이러한 툴은

우선순위를 결정할 수 있는 충분한 장치 컨텍스트 및 위험 경감을 제어하는 자동화 기능이 부족합니다. 결국 보안 팀의 고급 인력은 경미한 문제를 수동으로 해결하는 데

시간을 낭비하느라, 사전에 위험을 경감하거나 위협에 신속하게 대응하지 못합니다.

정책 기반 제어 적용

Forescout eyeControl은 Forescout eyeSight의 풍부한 장치 컨텍스트를 기반으로, 보안 팀이 안심하고 정책 기반 제어의 우선 순위를 지정, 적용 및 자동화할 수 있도록 합니다. 기업은 보안 예방 개선, 공격 노출도 감소, 대응 및 수정 기능 가속화를 통해 보안 위협, 사고 및 규정 준수 결함을 신속하게 완화할 수 있습니다.

eyeControl을 이용해 기업의 보안 정책에 맞춰 네트워크와 엔드포인트 기능을 실행할 수 있습니다. 네트워크 기능의 오케스트레이션을 위해 eyeControl은 스위치, 무선, VPN, 소프트웨어 정의 및 클라우드 기반 네트워킹 등 이기종의 물리/가상 네트워킹 인프라와 직접 통합됩니다. 엔드포인트 기능은 윈도우, Mac, 리눅스 엔드포인트에서, 또는 SecureConnector™를 이용하여 에이전트 없이 실행 가능합니다.

eyeControl

주요 기능

- 외부 위협으로부터 민감한 데이터 보호
- 감염되거나 취약한 장치 또는 비규격 장치의 멀웨어 확산 방지
- 타겟 공격으로 인한 데이터 탈취나 네트워크 다운 방지
- 직원, 계약자, 고객의 네트워크 접근 및 가용성 확보 지원
- 내부 정책 및 외부 규정 준수 강화
- 개별 상황에 적절한 조치를 제공하는 제어 기능 자동화

도표 1. 네트워크 및 엔드포인트 정책 적용을 통한 자동화 지속 향상

보통

네트워크

- 스트 네트워크로 이동
- 무선 사용자 역할 변경
- 자체 수정 VLAN에 할당 로그
- 장치/인프라 제한

호스트

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

정책 기반 제어 자동화

엄격

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
- 시정 조치/시스템 가동

신뢰할 수 있는 제어 자동화

eyeControl은 기업이 세밀한 타겟 제어를 할 수 있도록 직관적이고 탄력적인 정책 엔진을 사용합니다. 정교한 워크플로와 복합 기능이 사용하기 편한 동적 범위 지정, 불 논리, 워터폴 방식으로 구현됩니다. 정책 그래프를 이용하여 정확한 보안 정책을 생성하고, 정책 흐름을 분석해서 실제 실행에 앞서 정책을 세밀하게 조정할 수 있습니다.

제어 기능은 처음에는 보안 팀에서 수동으로 진행할 수 있지만 보안 운영의 효율성을 높이기 위해 점진적으로 자동화를 도입할 수 있습니다. 기초적이고 반복적인 작업부터 복잡한 제어기능까지 자동화하여 숙련된 IT 인력이 더 심각한 문제에 집중할 수 있습니다. 이는 네트워크 접근, 장치 컴플라이언스, 네트워크 분할, 초기 사고 대응 능력을 급격히 향상시켜 비즈니스 중단을 최소화 할 수 있습니다.

"대부분의 엔드포인트 작업을 자동화 할 수 있지만, 수동 개입이 필요한 경우 간단히 마우스 우클릭 한 번만 하면 됩니다."
ㅡ、Joseph Cardamone, Haworth 정보보안 선임연구원 겸 북미지역 개인정보보호 책임자

과제

- 네트워크상의 비규격 및 미인증 장치의 위험성
- 세그먼트가 부족한 플랫 네트워크로 인해 기업이 측면 공격에 취약하게 됨
- 보안 위협이나 사고에 신속하고 효과적인 대응이 어려움
- 보안 툴을 통해 장치 상태를 유지하기에 용량이 부족함
- 비즈니스 중단 위험으로 인한 보안 제어 자동화의 한계

네트워크 접근 시행

사용자 정보(게스트, 직원, 계약자), 장치 유형, 보안 상태에 따라 기업 자료 접근을 관리합니다.

- 게스트와 BYOD 장치에 차별화된 접근 권한 부여
- 802.1X 인증 유무에 관계없이네트워크 접근 정책 적용
- 네트워크상의 의심스러운 악성/섀도우 IT 장치에 대한 조치 시행
- 손상됐거나 악성 장치의 네트워크 접근 제한 및 차단
- 컴플라이언스 위반 장치는 문제가 해결될 때까지 격리

"Forescout 플랫폼을 선택한 이유 중 하나는 802.1X 프로토콜에 의존하지 않아 배포가 매우 쉽기 때문입니다. 에이전트를 설치하지 않아도 되기 때문에 성능이 뛰어나면서도 간편합니다."
— Juan Ignacio Gordon, ACCIONA IT보안 책임자

장치 컴플라이언스 개선

컴플라이언스 평가를 자동화하고, 내부 보안 정책과 외부 표준 및 산업 규정을 계속 준수할 수 있도록 시정 관리를 실행합니다.

- 엔드포인트가 제대로 구성되었는지 확인하고, 취약한 암호 설정 등 중요 위반 사항에 대한 시정 착수
- 필수 애플리케이션과 보안 에이전트의 설치와 실행, 업데이트 여부 확인
- 네트워크 대역폭이나 자원 생산성 측면에서 불필요한 부담을 주거나 위협이 될 수 있는 미인증 애플리케이션 사용 금지 및 차단
- 위험도 높은 취약점이나 누락된 중요 패치를 식별하여 시정 조치 실행
- 필수 보안 소프트웨어 설치, 에이전트 업데이트, 보안 패치 적용 등의 시정 조치 사전 설정
- AWS와 Azure, VMware®같은 클라우드 환경의 구성 규정 준수를 위한 정책 구현 및 제어 자동화

"Forescout 솔루션을 사용하고 나서 문제 발생 건수와 복구 작업이 줄어들었고, 덕분에 감사가 급격히 빨라져 수백만 달러를 절약할 것으로 기대하고 있습니다."
— Phil Bates, 유타 주 정부 최고정보보안책임자

동적 네트워크 분할 실시

공통의 정책 프레임워크를 이용하여 확장된 기업 환경의 서로 다른 기술 전반에 걸쳐 동적 네트워크 분할 정책을 적용합니다.

- 장치 속성과 유형, 보안 상태에 따라분할 그룹에 동적으로 장치를 할당
- 캠퍼스와 OT 네트워크에서 VLAN, ACL, WLAN 제어및 태그를 통해 분할 제어 적용
- AWS나 VMware NSX같은 공용 및 개인 클라우드 환경에서 보안 그룹/태그를 통해 분할 제어
- 공격 노출도를 줄이면서 비즈니스 연속성을 확보하기 위해 비규격 및 취약한 장치를 별도의 영역(특히 윈도우 정기 보수 시 패치 또는 복구되는 곳)으로 구분
- HIPAA나 PCI, SWIFT CSP 같은 규정에 따라 구역 내 장치와 중요 데이터 흐름을 네트워크 다른 구역과 분할하는 정책 적용

"Forescout는 장치를 격리하고 네트워크를 분할하는 것에 그치지 않고, 이전에는 보지 못했던 네트워크를 발견할 수 있습니다." — 대형 의료 기관의 정보보호 부책임자

사고대응 가속화

사이버 위협과 보안사고에 빠르고 효과적으로 대응하여 운영 중단과 비즈니스 손해를 최소화합니다.

- 제어 또는 복구되지 않은 고위험 장치 식별
- 평균 반응시간(MTTR)을 줄이기 위해 연결 당시 장치의 침해지표(IOCs)를 파악
- 멀웨어가 측면 확산되지 않도록 악성 또는 손상된 장치를 신속히 격리 및 제어
- 사고 대응 자동화 및 손상된 단말의 워크플로를 복구합니다.
- 다기능의 사고 대응 팀과 사일로화된 기술에 중요한 장치 컨텍스트(장치 연결 상태, 위치, 유형, 보안 상태)를 전달하여 평균 반응시간(MTTR) 감소

"Forescout에는 전 세계 네트워크를 넘나들며 밤낮으로 사이버 위협을 뒤쫓는 자동 사냥꾼이 있는 것 같습니다. 우리는 이제 이전에 손대지 못하던 문제를 해결하고 있습니다. 몇 시간을 들여 해결하던 문제들이 이제는 몇 분 만에 해결됩니다."
— Nick Duda, HubSpot 수석 보안엔지니어

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