Palo Alto Networks 엔터프라이즈 디바이스 보안

기업의 모든 디바이스를 발견, 평가 및 보호

오늘날 빠르게 변화하는 위협 환경에서 보안에 대한 단편화된 접근 방식은 더 이상 선택 사항이 아닙니다. 디지털 혁신, M&A 활동의 증가, 분산된 인력으로 인해 기존 IT 엔드포인트에서 비관리형 BYOD(Bring Your Own Device) 및 전문 IoT/OT 시스템에 이르기까지 디바이스의 확산이 촉진됩니다. 이러한 단편화된 접근 방식으로 인해 위험 정보가 사일로화되고 가시성 사각지대가 발생하여 AI 기반 공격자가 이를 빠르게 악용할 수 있습니다.

하지만 이제 모든 연결된 디바이스가 사이버위협의 잠재적 진입점이 되었기 때문에, 진짜 과제는 잠재적 위협을 파악하고 이에 즉시 대응하는 능력을 갖추는 것입니다. Muddled Libra 공격에서 드러난 것처럼, 공격자는 네트워크 지속성과 방어 회피를 위해 비관리형 자산을 사용하고 있습니다. 조직에서는 비정상적인 동작과 기타 손상 지표를 식별하기 위해 모든 관리형, 비관리형 및 IoT 자산과 이러한 자산의 동작에 대한 완전한 가시성이 필요합니다.

자산 및 잠재적 위험에 대한 가시성 확보를 위한 디바이스 보안

Palo Alto Networks 디바이스 보안은 전체 공격 표면에서 포괄적인 보호와 모니터링을 제공하는 통합된 AI 우선 솔루션을 제공합니다. 이를 달성하기 위해 이 솔루션은 연결된 모든 디바이스를 발견하고, 가장 노련한 정보 보안 전문가에게도 보이지 않거나 파악하기 어려운 숨겨진 위험을 식별하여 완화합니다.

디바이스 보안은 모든 디바이스 및 위험 데이터에 대한 단일 진실 공급원입니다. 수십 개의 도구를 전환하고, 여러 스프레드시트를 관리하고, 자산에 태그를 지정하고 상관 관계를 수동으로 지정하고, 데이터를 추출하거나 정리하기 위한 사용자 정의 스크립트를 만들고, 끝없는 회의 메모를 수집하는 데 몇 주가 걸립니다. 그런 다음 이 모든 데이터를 자동화된 사전 예방적 보호를 통해 몇 분 안에 해결할 수 있는 즉각적인 인사이트로 전환합니다.

보안팀은 자동화를 통해 전체 환경을 파악하고 가장 중요한 위험에 대해 사전에 조치를 취할 수 있습니다. 디바이스 보안은 기존 Palo Alto Networks 차세대 방화벽(NGFW), Prisma® Access 및 SD-WAN 보안 인프라 또는 스탠드얼론 가상 메타데이터 수집기를 사용하여 48시간 이내에 자산의 98%를 즉시 모니터링하고 발견을 시작할 수 있습니다. 35개 이상의 사전 구축된 통합 플레이북 중 하나를 사용하면 타사 시스템을 Cortex XSOAR®을 통해 디바이스 보안과 쉽게 통합할 수 있습니다.

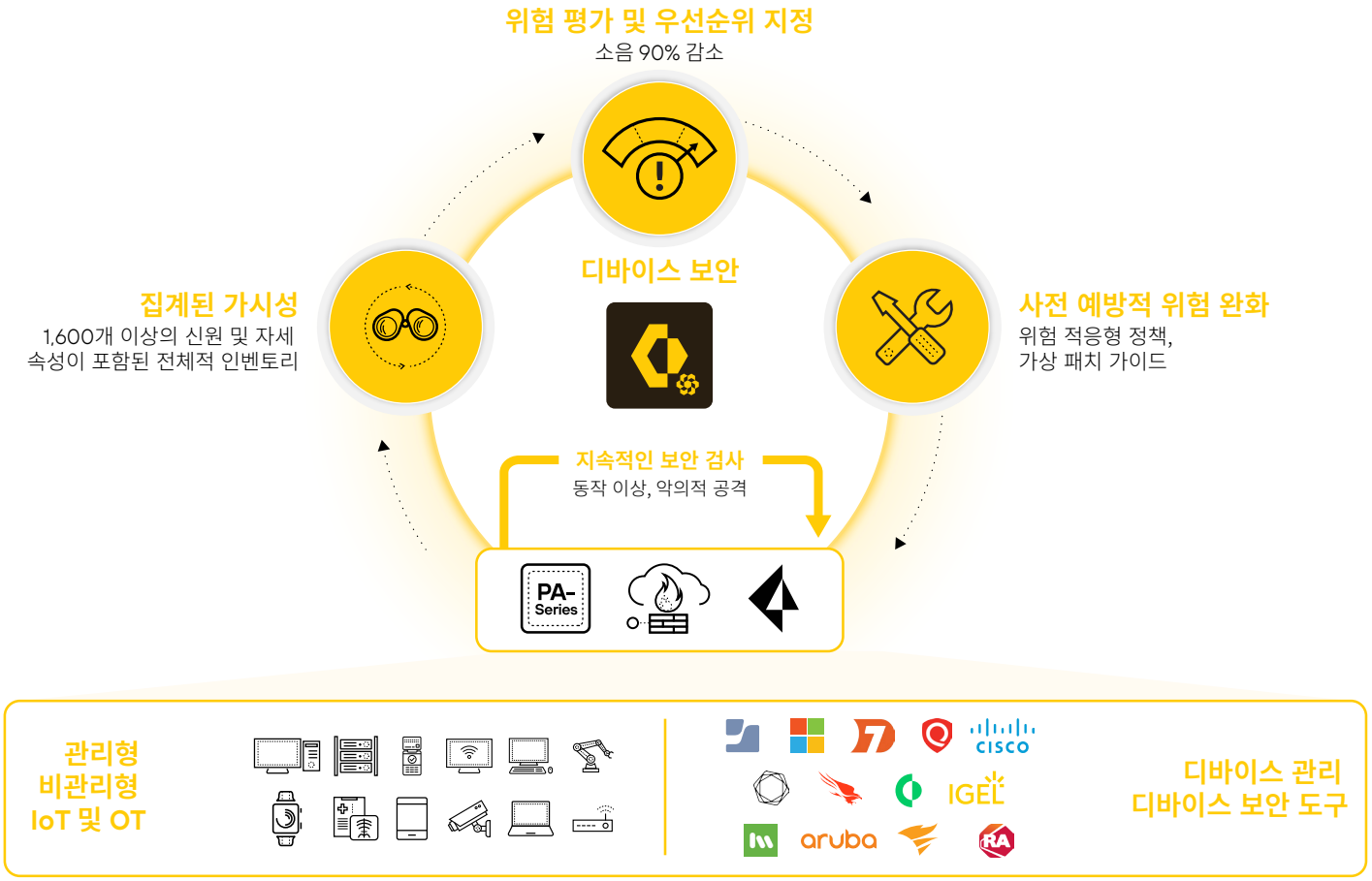

그림 1. 디바이스 보안 워크플로

모든 자산에 대한 통합된 가시성, 위험 우선순위 지정 및 사전 예방적 완화를 제공하는 디바이스 보안

팀이 더 빠르게 움직이고, 더 현명한 결정을 내리고, 더 적은 자원으로 더 많은 일을 할 수 있도록 하기 위해, 디바이스 보안은 조직이 가시성을 확보하고 전체 공격 표면을 보호하는 데 도움이 되는 포괄적이고 실행 가능한 접근 방식을 제공합니다. 당사의 AI 우선 보안 플랫폼을 사용하면 보안팀이 운영을 간소화하고 총 소유 비용을 줄여 보안 성과를 개선할 수 있습니다.

통합된 디바이스 가시성

디바이스 보안은 단순한 발견을 넘어 관리형 IT, 비관리형 BYOD, IoT/OT를 포함한 모든 연결된 디바이스에 대한 1,600개 이상의 ID 및 상태 속성을 통합하여 가시성을 제공합니다. 자산 발견은 네트워크 트래픽을 수동으로 처리하고 적극적으로 수집하는 3계층 머신 러닝 모델을 기반으로 합니다. 디바이스 보안은 대규모 언어 모델 지식 기반과 주요 엔드포인트 탐지, Mobile Device Management(MDM), 취약점 관리 시스템의 텔레메트리를 포함한 다양한 소스의 자산 데이터를 강화합니다. 이 포괄적인 데이터 세트는 사각지대를 제거하고 포괄적인 보안 태세 인사이트를 위한 단일하고 통합된 뷰를 제공합니다.

위험 평가 및 우선순위 지정

효과적인 우선순위 지정이 없으면 중요한 위험이 묻힐 수 있습니다. 디바이스 보안은 다중 요소 위험 평가를 통해 위험 분류에 소요되는 시간을 90% 줄입니다. 심각도(공통 취약점 점수 시스템[CVSS] 또는 악용 예측 점수 시스템[EPSS]), 자산 중요도, 비즈니스 영향, 악용 상태, 보완 통제, 사용자 정의 사용자 정의 요소와 같은 요소를 고려합니다. 이렇게 하면 보안팀은 비즈니스 상황에서 가장 우선순위가 높은 위험에 집중할 수 있습니다.

사전 예방적 위험 완화

문제를 보는 것만으로는 충분하지 않습니다. 팀에는 행동할 수 있는 능력이 필요합니다. 디바이스 보안은 1,700만 개가 넘는 디바이스에서 수집한 크라우드소싱 기준과 비교하여 디바이스의 고유한 ID, 위험 태세 및 고유한 동작을 기반으로 위험 적응형 레이어 7 정책을 활성화하고 권장합니다. 공급업체 지원 부족, 운영 다운타임 또는 시스템 호환성 등의 이유로 패치할 수 없는 취약점의 경우, 디바이스 보안은 Palo Alto Networks의 업계 최고 수준의 고급 위협 방지 시그니처를 사용하여 Strata™ Cloud Manager에서 가이드형 가상 패치를 제공합니다.

지속적인 모니터링

빠르게 변화하는 위협 환경에 발맞추기 위해 조직에서는 실시간으로 위협을 포착할 수 있는 능력이 필요합니다. 디바이스 보안은 모든 디바이스 트래픽을 지속적으로 모니터링하고 머신 러닝을 사용하여 컨텍스트별 기준과 크라우드소싱(3,500명 이상의 고객) 기준에 대해 디바이스 동작 기준을 개발하고 지속적으로 재평가합니다. 악의적, 비정상적 또는 고위험 동작이 관찰되면 디바이스 보안에서 알림을 생성하여 전체 네트워크에 걸쳐 24시간 연중무휴 모니터링을 제공합니다.

활용 사례: 여러 디바이스에서 위험 식별 및 완화

오늘날의 기업 환경에는 관리형, 비관리형, 특수 목적 IoT/OT 자산이 혼합되어 있습니다. 이러한 자산에는 회사에서 지급한 노트북, 비관리형 섀도 IT 서버, 레거시 라우터, IoT 공기 질 모니터와 같이 보안이 심각하게 고려되지 않은 디바이스 등이 포함됩니다. 각 상황은 고유한 보안 문제를 나타내며, 위험 관리에 대한 고유한 접근 방식이 필요합니다. 다음 사용 사례는 디바이스 보안이 어떻게 팀이 모든 환경에서 위험을 줄이고, 통제력을 강화하고, 더 빠르게 대응하는 데 도움이 되는지 보여줍니다.

관리형 디바이스 보호: 디바이스 적용 범위의 격차 해소

잘 관리되는 환경에서도 엔드포인트 도구가 일관되지 않게 배포되거나 정책이 사업부 간에 차이가 나는 경우 격차가 발생하는 경우가 많습니다. 디바이스에 EDR 에이전트가 없거나, 오래된 구성을 실행 중이거나, 취약점 스캔에서 제외되었을 수 있습니다. 자산 및 위험 데이터가 수십 개의 시스템에 사일로화되어 있는 경우 이러한 문제를 파악하기 어렵습니다. 디바이스 보안은 1,600개 이상의 ID 및 상태 속성을 사용하여 연결된 모든 디바이스에 대한 포괄적인 프로파일을 구축합니다. 통합 엔드포인트 탐지, MDM 및 취약점 관리 시스템에서 자산을 지속적으로 모니터링하고 텔레메트리 데이터를 집계합니다. CVSS, EPSS, 자산 중요도, 비즈니스 영향 및 보완 통제의 다중 요인 위험 우선순위 요소를 통해 가장 중요한 위험을 강조합니다.

통합된 자산 가시성과 포괄적인 위험 우선순위 지정을 통해 보안팀은 가장 큰 영향을 미치는 규정 준수 격차를 신속하게 파악하고 위험 적응형 Device-ID 정책을 통해 즉각적인 조치를 취하거나 Cortex XSOAR 또는 NGFW를 통해 기존 도구 내에서 직접 시행을 트리거할 수 있습니다. 디바이스 보안을 통해 팀은 몇 주에 걸쳐 수동으로 격차를 파악하는 데 드는 노력을 절약할 수 있습니다. 또한 위험을 분류하고 해결하는 프로세스도 자동화하여 보안팀이 위험 사례를 추적하는 데 소요되는 시간을 줄이고 전략적 보안 이니셔티브에 더 많은 시간을 할애할 수 있도록 합니다.

관리형 자산 사용 사례

- 불완전하거나 오래된 자산 인벤토리
- 일관되지 않은 보안 도구 배포
- 승인되지 않은 소프트웨어가 설치됨
- 취약점을 스캔하지 않음

비관리형 디바이스 보호: 섀도 IT 발견 및 제어

개인용 노트북, 불법 액세스 포인트, 계약자 소유 시스템 등 관리되지 않거나 승인되지 않은 디바이스는 가시성이나 제어 없이 기업 네트워크에 연결되는 경우가 많습니다. 이러한 자산은 표준 보안 제어를 우회하고 숨겨진 위험을 초래합니다.

디바이스 보안은 머신 러닝 기반 발견과 여러 데이터 소스의 풍부한 메타데이터를 사용하여 공식적인 IT 관리 외부에 있는 디바이스를 포함하여 네트워크에 연결된 모든 디바이스를 밝혀냅니다. 또한 각 디바이스에 대한 행동 및 위험 프로파일을 구축하고 Device-ID를 사용하여 NGFW에서 활성화할 수 있는 ID 인식 세분화 정책을 권장합니다. 지속적인 트래픽 모니터링을 통해 비정상적이거나 위험성이 높은 행동을 감지하고 실시간으로 알림을 생성합니다. 팀은 위험 적응형 Device-ID 정책을 통해 비관리형 디바이스에서 발생하는 위험을 신속하게 식별하고 격리하여 보안이 확보되거나 제거될 때까지 제어할 수 있으며, 이를 통해 섀도 IT 노출 위험을 없앨 수 있습니다.

비관리형 자산 사용 사례

- 타사 시스템의 가시성 사각지대
- 무단 네트워크 액세스
- 섀도 IT
- 패치되지 않은 악용 가능한 취약점

IoT/OT 디바이스 보호: 안전하지 않은 프로토콜이나 지원되지 않는 시스템을 사용하여 디바이스 보호

많은 운영 환경은 Server Message Block(SMB) 프로토콜과 같은 안전하지 않은 프로토콜을 사용하거나 오래되고 지원되지 않는 운영 체제를 실행하는 특수 디바이스에 의존합니다. 이러한 시스템은 공급업체의 제한, 운영상의 제약 또는 중단 위험으로 인해 패치를 적용할 수 없는 경우가 많습니다. 적절한 통제가 없으면 이러한 자산은 지속적인 노출 위험을 초래합니다.

디바이스 보안은 이러한 디바이스를 식별하고 해당 디바이스의 트래픽을 지속적으로 모니터링하여 행동 기준을 설정하고 개선합니다. 1,600만 개가 넘는 디바이스에서 로컬 컨텍스트와 크라우드소싱 기준을 모두 사용하여 편차나 악의적 패턴이 관찰되면 보안팀에 경고합니다. 레이어 7 Device-ID 정책을 사용하면 조직에서 App-ID™ 및 데스티네이션을 기반으로 최소 권한 정책을 정의할 수 있습니다. 가이드 기반 가상 패치를 통해 조직은 패치할 수 없는 취약점으로 인한 위험을 기본적으로 완화할 수 있습니다. 두 가지 제어 기능 모두 비용이 많이 들거나 업무에 방해가 되는 디바이스 업데이트 없이도 팀이 위협을 억제하는 데 도움이 됩니다.

IoT/OT 자산 사용 사례

- 가시성 사각지대
- 잘못된 세분화
- 수명 종료 시스템
- 안전하지 않은 프로토콜/취약한 자격 증명
- 패치할 수 없는 취약점

왜 Palo Alto Networks인가?

Palo Alto Networks는 전 세계 기업이 신뢰하는 사이버보안 파트너입니다. 위협이 진화하고 환경이 더욱 긴밀하게 연결됨에 따라, 우리는 심층적인 업계 경험과 첨단 보안 기술을 결합하여 실시간으로 귀사의 운영을 보호합니다.

당사의 디바이스 보안 솔루션은 다음과 같은 특징을 제공합니다.

- **관리형, 비관리형 및 IoT/OT 디바이스 전반에 걸친 통합 보호:** 당사의 AI 우선 플랫폼은 물리적 환경과 디지털 환경을 아우르며, 격차를 해소하고 복잡성을 줄입니다. 디바이스 보안은 당사 제품 포트폴리오에 내장되어 있으므로 별도의 시행 하드웨어나 맞춤형 통합이 필요하지 않습니다.
- **적응형 디바이스 ID 및 위험 기반 정책 시행:** 동적 Device-ID를 통한 세부적인 제어를 통해 관리형 IT 엔드포인트에서 전문화된 비관리형 시스템에 이르기까지 운영 우선순위에 맞춰 컨텍스트 인식 세분화 및 시행이 가능합니다.
- **AI 기반 위협 예방:** 인라인 제어를 통해 알려진 위협과 알려지지 않은 위협을 실시간으로 차단하여 위협이 머무는 시간을 줄이고 모든 디바이스 유형에 미치는 영향을 최소화합니다.
- **사전 예방적 위험 완화:** 디바이스 보안은 탐지를 넘어, 패치가 불가능한 시스템이나 기존 시스템에서도 위험을 적극적으로 해결하기 위해 가이드형 가상 패치와 위험 적응형 정책을 제공합니다.
- **배포 용이성을 위해 제작됨:** 디바이스 보안은 단일 용도의 하드웨어를 배포하고 관리할 필요 없이 기존 네트워크 인프라를 사용합니다. 귀하의 팀은 최소한의 구성으로 신속하게 디바이스 보안에 액세스하고 48시간 내에 98% 이상의 디바이스에 대한 포괄적인 가시성과 시행을 확보할 수 있습니다.

디바이스 보안이 빠르게 확장되는 공격 표면을 어떻게 보호할 수 있는지 자세히 알아보세요. 무료 평가판을 원하시면 저희에게 문의해 주세요.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

대표 전화: +1.408.753.4000
판매 문의: +1.866.320.4788
지원 문의: +1.866.898.9087

www.paloaltonetworks.com

strata_sb_enterprise-device-security_080725