IoT/OT 보안의 재정의

한 플랫폼에서 가시성, 제어, 위협 방지

CATO NETWORKS

소개

IoT/OT 보안이란?

오늘날 급속히 발전하는 디지털 비즈니스 환경에서 IoT(사물인터넷)와 OT(운영 기술) 장치는 소매, 제조, 의료, 유틸리티 등 여러 산업 분야에서 운영 효율성을 높이기 위한 핵심으로 자리 잡았습니다.

이러한 장치들은 실시간 모니터링, 물리적 프로세스 제어, 자동화를 가능하게 하여 전례 없는 수준의 생산성과 민첩성을 실현합니다. IoT 및 OT 장치가 확산됨에 따라 상당한 보안 문제 또한 야기되고 있습니다. 대부분의 IoT 및 OT 장치에는 견고한 내장 보안 기능이 부족하며, 구형 또는 패치되지 않는 소프트웨어에서 실행되고, 또한, 대단위 규모로 모니터링하기 어렵습니다. 대부분의 이러한 특성을 가진 장치들은 원격 또는 모니터링되지 않는 환경에 설치되는 경우가 많아 더 위험합니다.

IoT/OT 보안에는 해당 장치의 작동에 대한 가시성을 제공하고, 접근 및 사용 방침 정책을 시행하며, 알려진 위협과 새로운 위협을 모두 방지하는 솔루션이 모두 포함됩니다. 기업들이 이러한 기술에 점점 더 의존함에 따라 IoT/OT 환경을 보호하는 것은 더 이상 부차적인 고려 사항이 아닌 운영 연속성, 안전, 신뢰를 위한 아주 기본적인 필수사항이 되었습니다.

IoT/OT 장치로 인해 발생하는 취약점

IoT 및 OT 장치는 유틸리티에서 의료에 이르기까지 산업의 필수 시스템을 뒷받침하는 기업 운영의 중요한 구성 요소가 되었습니다. 그러나 이러한 장치는 고유한 취약점과 기본 보안 부족으로 인해 사이버 공격의 주요 타겟이 됩니다. 위협 행위자들은 IoT/OT 의 취약점을 악용하여 운영을 방해하고, 안전사고를 일으키며, 민감한 데이터를 훔칠 수 있습니다.

공격자가 각각의 새로운 IoT 및 OT 장치를 통해 진입할 수 있기 때문에 기업이 보안에 취약해질 수 있습니다. 더 많은 장치가 배치될수록 공격 표면이 기하급수적으로 증가합니다. 이러한 장치들은 종종 쉽게 패치하거나 업그레이드할 수 없는 레거시 시스템에 의존하기 때문에 취약점이 영구적으로 지속될 수 있습니다. 많은 기업이 연결된 IoT 및 OT 장치를 식별하고 관리하는 데 어려움을 겪고 있으며, 이로인해 보안 침해가 매우 쉽게 발생할 수 있는 환경이 만들어집니다.

IoT/OT 환경에서의 보안 침해는 광범위한 문제를 초래할 수 있습니다. 제조업의 경우 생산 설비가 중단되어 재정적 손실을 볼 수 있습니다. 의료 분야에서는 환자의 안전이 위협당할 수 있습니다. 이러한 위험으로 인해 IoT/OT 보안은 CIO, CISO 및 보안 설계자들의 최우선 과제가 되었습니다.

IoT/OT 보안에는 무엇이 필요할까요?

IoT/OT 환경을 보호하는 첫 번째 단계는 모든 장치에 대해 완전한 가시성을 확보하는 것입니다. 여기에는 각 장치의 유형, 제조업체, 소프트웨어 버전뿐만 아니라 동작과 네트워크 활동을 식별하는 것이 포함됩니다. 그러나 가시성만으로는 완전히 보호할 수 없습니다. 기업은 장치가 내부 및 외부 네트워크와 상호 작용하는 방식을 제어하기 위해 엄격한 접근 및 사용 방침을 시행해야 합니다. 마지막으로 IoT/OT 환경은 알려진 위협과 새로운 위협 모두에 취약하기 때문에 기업에 통합 위협 방지 도구가 필요합니다. 통합 위협 방지 도구는 보안 관리를 복잡하게 만들기보다는 단순화하는 방식으로 제공되어야 합니다.

IoT/OT 보안 요구사항의 도전 과제

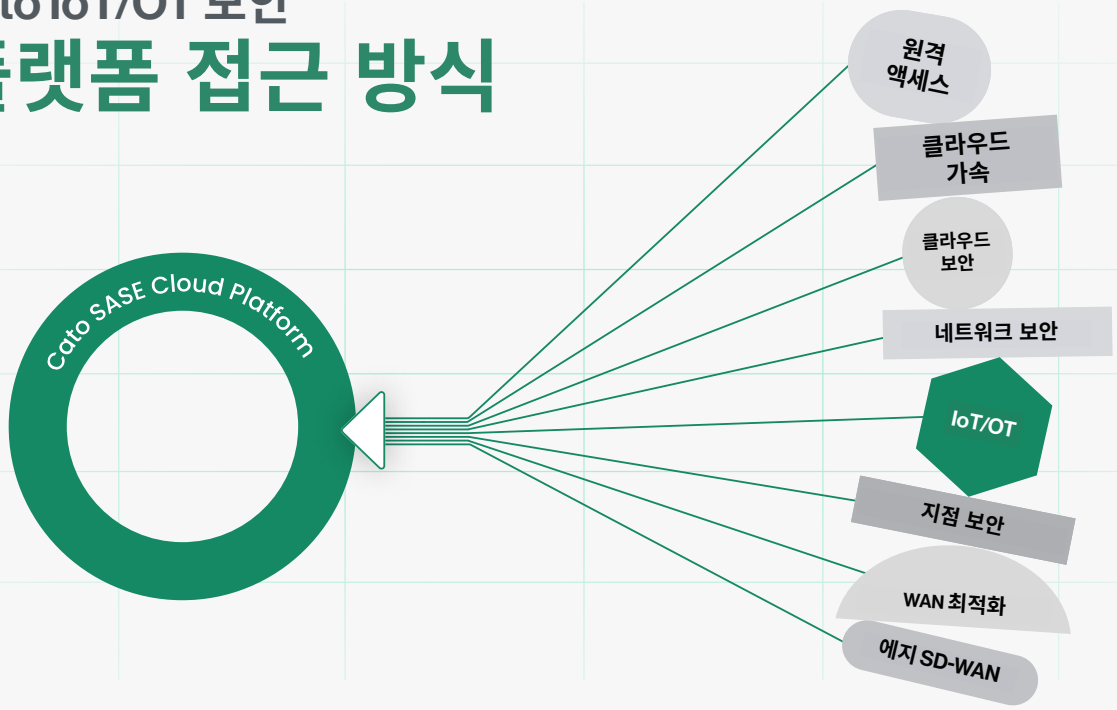
IoT/OT 보안의 명확한 필요성에도 불구하고 기업들은 시스템을 효과적으로 보호하는 데 여러 가지 장애물에 직면합니다.

첫째, 많은 도구가 장치 활동에 대한 부분적인 통찰만 제공하여 중요한 자산이 모니터링되지 않은 채로 남게 됩니다. 둘째, 전통적인 솔루션들은 종종 번거로운 설치와 통합이 필요하여 다양한 환경에 배포하기 어렵습니다. 마지막으로 많은 솔루션들이 장치 검색, 정책 시행, 위협 방지를 위해 여러 개로 분리된 다양한 종류의 제품에 의존합니다. 이와 같은 단편화로 인해 전반적으로 보호 효과는 감소되며 운영 복잡성과 비용은 증가합니다.

즉, 이러한 문제는 IoT/OT 취약점을 악용하기 위한 새로운 방법이 지속적으로 진화하는 위협 환경으로 더욱 복잡해집니다. 이러한 문제를 해결하기 위해 기업은 IoT/OT 보안에 대해 통합되고 간소화된 접근 방식이 필요합니다.

Cato IoT/OT 보안

플랫폼 접근 방식



장치 검색 및 가시성

Cato IoT/OT 보안은 IoT, OT, IT 환경 전반에 걸쳐 즉각적이고 수월한 가시성을 제공하여 사각지대를 제거합니다. AI 기반 검색을 사용하여 도구 설치 없이 장치의 유형, 제조업체, 버전을 식별하고 분류합니다.

정책 시행

Cato IoT/OT 보안은 장치를 유형이나 제조업체, 운영 체제와 같은 범주로 그룹화하여 정책 관리를 단순화합니다. 보안 팀이 장치 속성을 기반으로 세분화된 접근 및 사용 정책을 정의할 수 있게 합니다.

위협 방지

Cato IoT/OT 보안은 추가 도구 없이 모든 장치에 걸쳐 일관된 보호를 제공합니다. IPS, DNS 보안, 안티멀웨어를 포함한 고급 보안 엔진을 통합하여 알려진 위협과 새로운 위협 모두로부터 보호합니다.

Cato 의 SASE 클라우드 아키텍처는 이러한 기능들이 원활하게 함께 작동하여 운영 부담을 더하지 않고 포괄적인 보호를 보장합니다.

Cato IoT/OT 보안의 차별점

Cato IoT/OT 보안은 **통합 복잡성을 제거합니다**. 검색과 시행을 위해 여러 도구가 필요한 다른 솔루션과 달리 Cato IoT/OT 보안은 Cato SASE 플랫폼에 완전히 융합되어 있습니다. 이를 통해 복잡하게 배포할 필요가 없어 기업은 즉시 보안 기능을 활성화할 수 있습니다.

Cato IoT/OT 보안은 **단순한 가시성을 넘어섭니다**. 많은 도구가 장치를 검색하는 데 그치는 반면, Cato 는 완전한 보안 솔루션을 제공합니다. 가시성과 세분화된 방침 시행, 강력한 위협 방지를 결합하여 IT 팀이 IoT/OT 환경을 효과적으로 보호할 수 있게 합니다. Cato 의 자동화된 프로세스는 수동 작업을 최소화하여 IT 팀이 일상적인 관리보다는 전략적 이니셔티브에 집중할 수 있게 합니다. 이러한 효율성은 자원이 제한된 기업에서 더욱 빛을 발합니다.

Cato IoT/OT 보안 구현의 일반적인 사용 사례

사용 사례

01 공격 표면 감소

보안 팀은 Cato IoT/OT 보안을 사용하여 IoT/OT 사각지대를 제거하고 사전에 위험을 평가하고 완화할 수 있습니다. 이를 통해 기업은 장치에 대한 무단 접근 및 활동을 방지하여 더 안전한 보안 환경을 만들 수 있습니다.

사용 사례

02 위험 완화

Cato IoT/OT 보안의 실시간 위협 방지 기능으로 보안 사고의 가능성을 줄일 수 있습니다. 이는 중요한 업무 운영을 위한 안전망을 제공하여, 진화하는 위협에 직면하더라도 비즈니스 연속성을 보장합니다.

사용 사례

03 보안 공급업체 통합

Cato IoT/OT 보안을 사용하면 검색, 시행, 위협 방지를 단일 플랫폼으로 제공하여 여러 보안 도구를 사용하지 않아도 됩니다. 이를 통해 관리를 단순화하고 비용을 절감하여 조직이 강력한 보안 태세를 더 쉽게 유지할 수 있습니다.

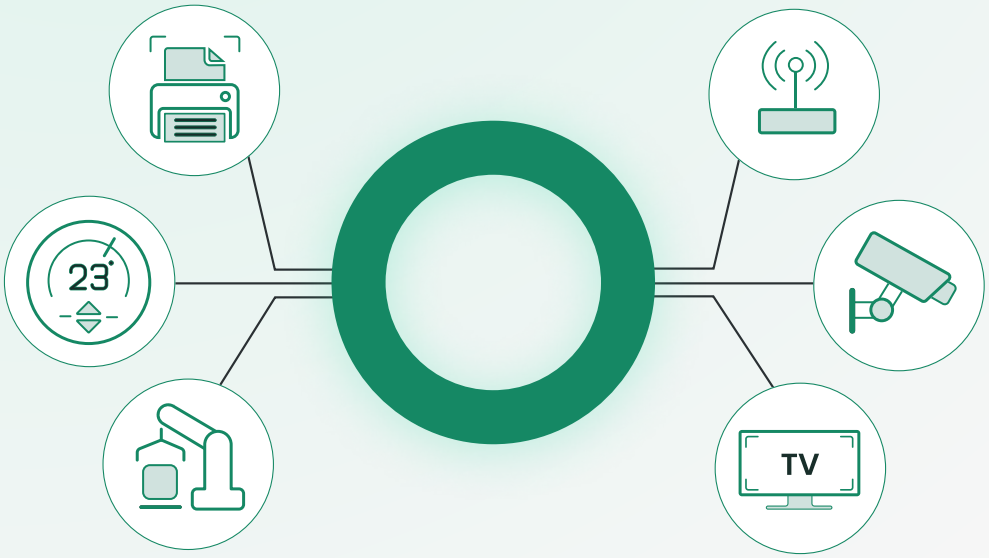
요약

IoT/OT 장치는 현대 기업의 핵심이지만 중대한 보안 문제를 야기하기도 합니다. 적절한 가시성, 제어, 위협 방지가 없다면 기업은 운영 중단, 재정적 손실, 평판 손상과 같은 위험에 노출될 수 있습니다.

Cato IoT/OT 보안은 이러한 문제에 대한 강력하고 간소화된 솔루션을 제공합니다. Cato SASE 클라우드 플랫폼에 내장되어 있어 종합적인 가시성, 세분화된 방침 시행, 강력한 위협 방지 기능을 제공하며, 기존 도구의 복잡한 통합 과정 없이 이 모든 것이 가능합니다. Cato 를 통해 IoT/OT 환경을 보호함으로써 기업은 중요한 자산을 보호하면서 자신 있게 디지털 혁신을 진행할 수 있습니다.

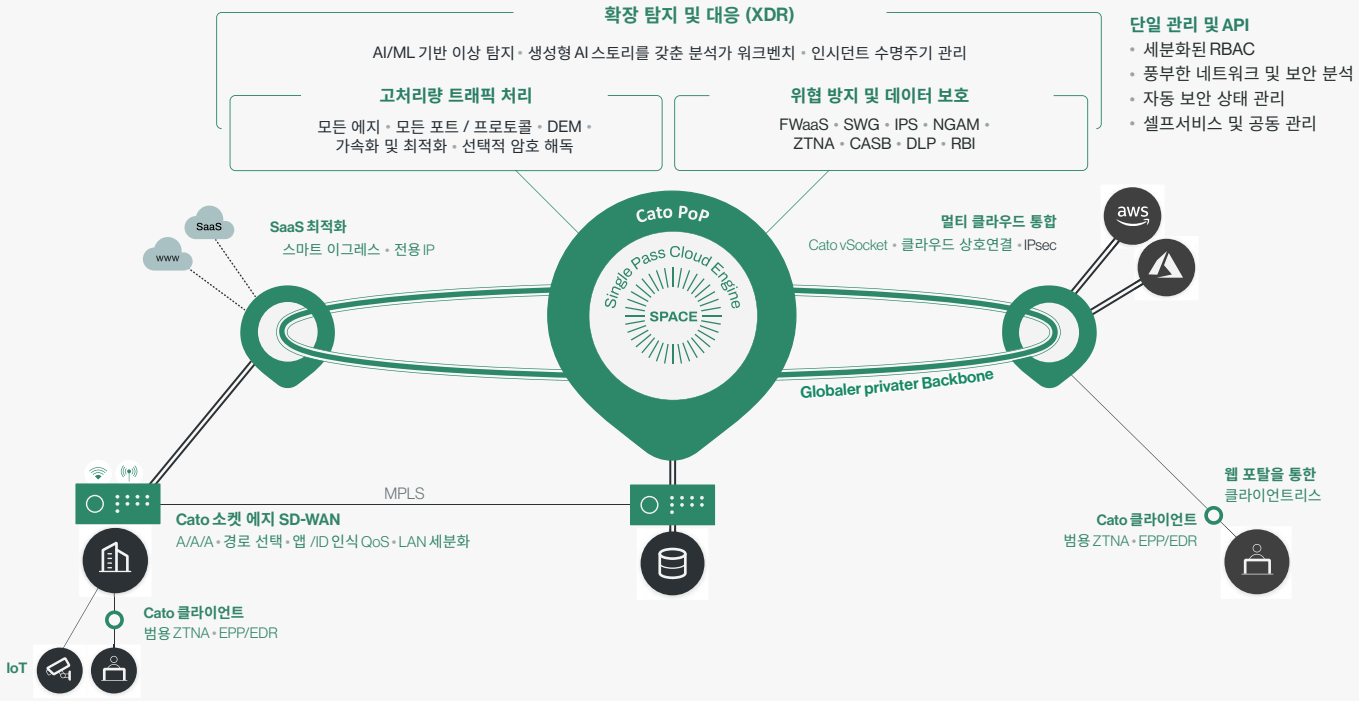
주요 시사점

Cato IoT/OT 보안은 기업이 점점 더 상호 연결된 세계에서 복잡성을 줄이고, 보안을 강화하며, 운영 연속성을 보장할 수 있도록 지원합니다.



CATO
NETWORKS

Cato SASE 클라우드 플랫폼



Cato. 우리가 진정한 SASE 입니다.

Cato SASE 클라우드 플랫폼

연결
클라우드 네트워크
클라우드 온램프

보호
네트워크 보안
엔드포인트 보안

탐지
인시던트 수명주기 관리

운영
통합 관리 및 API

사용 사례

네트워크 혁신
MPLS 에서 SD-WAN 으로 마이그레이션
글로벌 액세스 최적화
하이브리드 클라우드와 멀티 클라우드 통합

비즈니스 혁신
공급업체 통합
비용 최적화
M&A 및 지리적 확장

보안 혁신
안전한 하이브리드 업무
안전한 다이렉트 인터넷 액세스
안전한 애플리케이션 및 데이터 액세스
인시던트 탐지 및 대응

문의하기