FORTINET

백서

IIoT와 5G 확산에 대응하는 OT 운영기술 보안 구현

목차

서론

불과 얼마 전까지만 해도 대부분 OT 운영기술(OT) 프로세스는 특정 프로토콜을 사용하는 격리된 네트워크에서 실행되었습니다. 그래서 보안은 물리적 공격을 보호하는 데만 치중하게 되었습니다. OT 네트워크를 모든 것에서 분리하는 '공극'이 있으면 데이터 센터와 비즈니스 네트워크에서 발생하는 위험한 사이버 보안 문제를 쉽게 외면할 수 있었습니다.

지난 10년 사이에 OT 프로토콜은 라우팅 가능한 인터넷 기반 프로토콜(예: TCP/IP(Transmission Control Protocol/Internet Protocol))에 점차 포함되기 시작했습니다. 지금은 산업 네트워크도 IT 네트워크와 융합되고 있습니다. 퍼듀(Purdue) 모델을 참고해서 말씀드리면, 물리적 프로세스와 운영, 제어 영역이 아직 비즈니스 및 물류 영역과 분리기는 하지만 기존의 공극은 사라지고 있습니다. 네트워크 방화벽이 있는 DMZ가 이들 영역을 분리합니다. 그러나 방대한 정보가 생겨나면서 이 영역을 오가야 할 필요가 생겼습니다. OT 시스템을 오가는 데이터가 늘어날수록 위협에 대한 노출도 커집니다.

게다가 센서와 컨트롤이 소형화되고 응용 인공 지능(AI)이 적용되는 등의 움직임이 기술 분야에서 생겨나면서 OT 시스템의 방대한 데이터를 더욱 쉽게 활용할 수 있게 되었습니다. 보안의 관점에서 보면 무선 연결성이 가장 중요할 수 있는데, 기존 OT 네트워크 연결을 우회해 직접 인터넷에 연결할 수 있습니다. 요즘은 대부분 산업 도구와 기기는 무선 연결 기능이 내장됐기 때문에 프로세스 데이터와 원격 측정 데이터를 비즈니스 정보 시스템에 바로 업로드하거나, 유지관리 데이터를 시스템 제조사에 직접 제공할 수 있습니다. 인터넷을 통해 다양한 기기 유형을 연결하는 것을 일컬어 사물 인터넷(IoT)이라고 합니다. IoT 기기를 OT 환경 내에서 실행하는 경우에는 산업용 사물 인터넷(IIoT)이라고 합니다.

IoT와 IIoT가 얼마나 기술적으로 유사하고 차이가 있든, 두 인프라는 사이버 위험으로부터 보호하고 산업 표준과 모범 사례를 따르는 최소한의 기본 보안 조치를 적용해야 합니다. 이 백서에서는 Wi-Fi, 5G를 포함한 IIoT 및 다른 트렌드가 생산 인프라의 보호에 미치는 영향을 알아보겠습니다. IIoT 무선 연결의 대표적인 사용 사례를 몇 가지 설명한 후, 이런 기기를 보호하는 데 적절한 기술 아키텍처를 정의합니다. 이 아키텍처는 유선과 무선이 서로 혼재하며 연결되는 첨단 OT 인프라에 적절한 사이버 보안을 적용하는 데 필요한 전략과 전술을 마련하는 토대가 됩니다. 또한, 포티넷 제품 포트폴리오의 예시를 들며 보안 전략을 설명합니다.

IIoT, 무선, 5G 등의 트렌드는 OT 환경에 영향을 미치는데, 이들 환경은 주로 PERA(Purdue Enterprise Reference Architecture)를 기반으로 구축됩니다. 이 모델은 애플리케이션과 컨트롤의 계층적 레벨을 보여줍니다. 레벨 0, 1, 2(물리적 제어 영역)는 물리적 프로세스, 센서, 액추에이터, 관련 계측 장비, 이러한 구현을 감독하는 시스템을 정의합니다. 레벨 3(운영 및 제어 영역)은 여러 프로세스에 걸쳐 있는 전체적 제조 OT 운영기술을 나타냅니다. 이 레벨들을 합쳐 OT 환경이라고 합니다. 레벨 4와 5는 비즈니스 영역이라고 하는데, 엔터프라이즈 IT 시스템과 애플리케이션으로 구성됩니다. 1990년대에 처음 소개된 원래의 퍼듀(Purdue) 모델에는 IIoT, 무선, 클라우드 연결이 반영되지 않습니다. 5G 기술이 정식으로 출시된 이후로는 기존 퍼듀 레벨을 우회하는 과정이 더욱 가속화될 전망입니다.

이 백서에서는 현대 OT 환경에서 IIoT 및 5G가 보안에 미치는 영향을 살펴봅니다. 또한, 기업에서 안전한 연결을 제공하기 위해 아키텍처에서 고려해야 할 사항이 무엇인지 검토하고 최신 기술이 어떻게 지금의 기업에 필요한 보안과 유연성을 지원하는지 설명합니다.

IIoT 및 무선 배포 사용 사례

IIoT 기기에 내재된 보안 위험은 직간접적인 인터넷 연결에서 발생합니다. OT 보안 경계 내의 IIoT와 무선 기기에서 발생하는 위험을 살펴보기 전에 IIoT 및 관련 정보에 대한 기본 사용 사례를 설명하겠습니다. OT 배포는 세 가지 주요 사용 사례를 복합적으로 적용할 수 있습니다.

IIoT 및/또는 무선: 아웃바운드 전용 통신

이 사용 사례는 디지털 자산과 연결되어 (대부분 타사) 원격 모니터링 센터로 데이터를 보내 자산 성능 관리, 조건 기반 유지관리 등을 수행하는 스마트 센서를 사용합니다. 이 사례는 정보 흐름이 센서에서 밖으로 나가는 방향에만 국한되기 때문에 가장 위험이 낮습니다. 연결이 안전한 OT 경계 밖으로 향하든, 내부 게이트웨이로 향하든 센서는 명령이나 지시를 받지 않습니다. 그러므로 범죄자가 정보를 가로채 HMI에 숨길 수는 있지만, 센서에 직접 영향을 미칠 수는 없습니다.

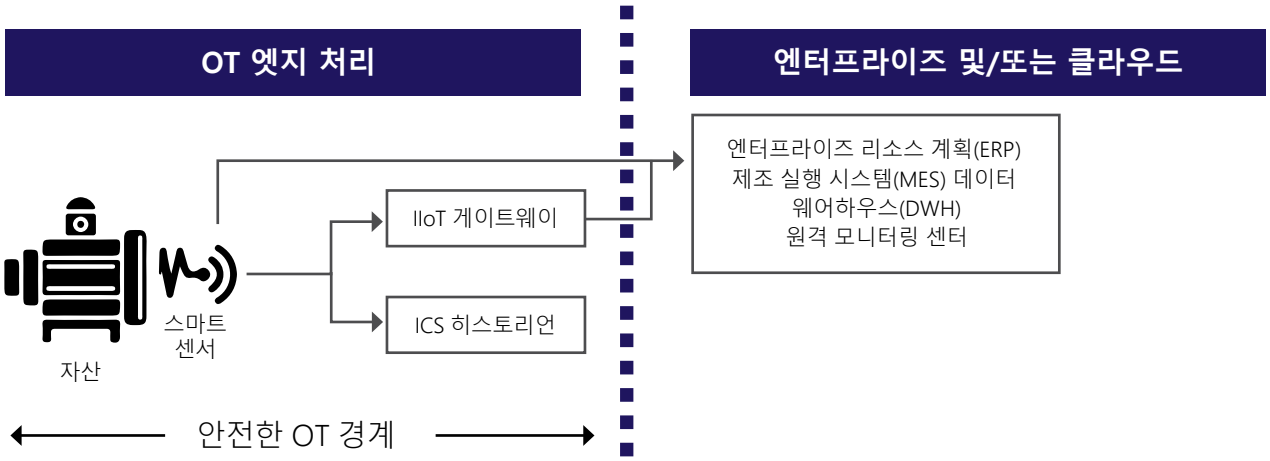


그림 1: 아웃바운드(이그레스) 전용 통신

IIoT 및/또는 무선: 아웃바운드 및 인바운드 통신

이 사용 사례는 위와 같은 아웃바운드 흐름에 더해 센서에 (상태 등을) 쿼리하기 위한 인바운드 흐름이 추가되었습니다. 엔터프라이즈, 클라우드 IT 환경이나, IIoT 제조사 등이 분석 정보를 요청하는 쿼리와 명령을 보내 데이터를 수집하거나 문제 해결을 위해 정보에 액세스할 수 있습니다. 흐름이 양방향이기 때문에 아웃바운드 전용 사례보다 위험이 큽니다.

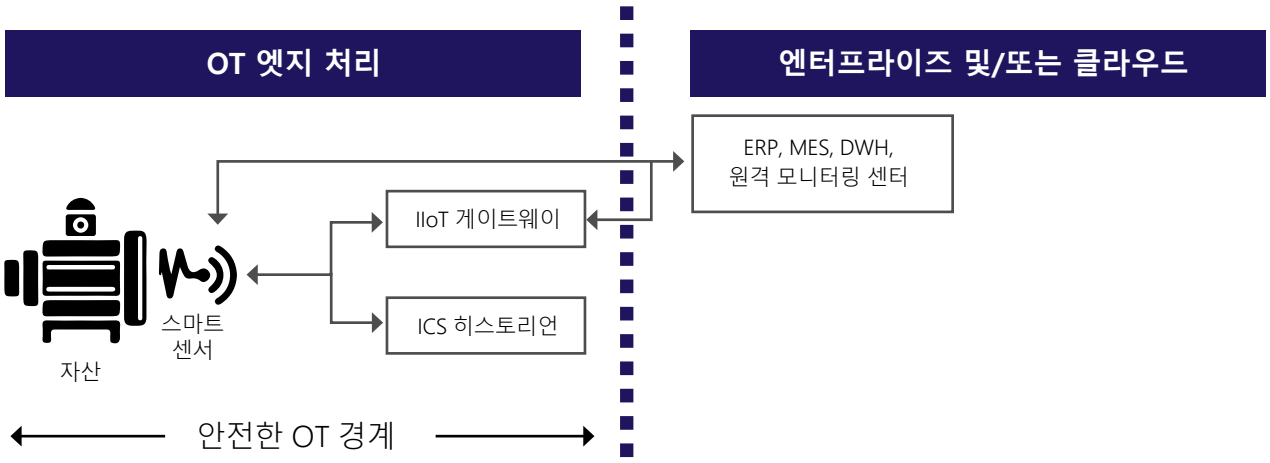


그림 2: 아웃바운드(이그레스) 및 인바운드(인그레스) 통신

IIoT 및/또는 무선: 원격 액세스, 유지관리, 진단

이 사용 사례는 가장 위험이 큰데, 그 이유는 (정보를 제공하기만 하는) 센서뿐만 아니라 생산 환경을 수정하는 액추에이터도 포함되기 때문입니다. 위의 사용 사례에서 나온 센서와 마찬가지로, 엔터프라이즈/클라우드 IT 시스템과 액추에이터 사이에 양방향 통신이 존재합니다. 액추에이터는 명령에 반응하고 그에 따라 동작을 취할 수 있습니다.

예를 들어 액추에이터는 상태, 프로세스 속도, 플로를 변경하는 명령을 보낼 수 있습니다. IIoT 기기나 공장 전체가 관여하는 프로세스의 원격 제어 사례도 마찬가지입니다. 프로세스를 원격으로 실행하면 편리하기는 하지만, 이런 기능으로 인해 발생하는 보안 위협을 인지하고 위협 노출을 차단해야 합니다.

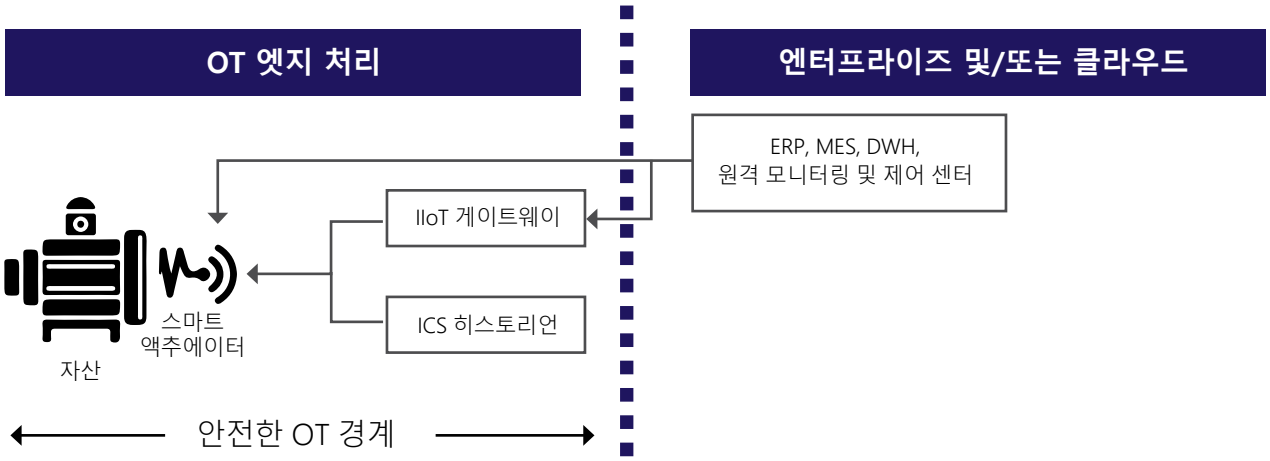


그림 3: 원격 액세스, 유지관리 및 진단

생산 제어 구조에서의 IIoT

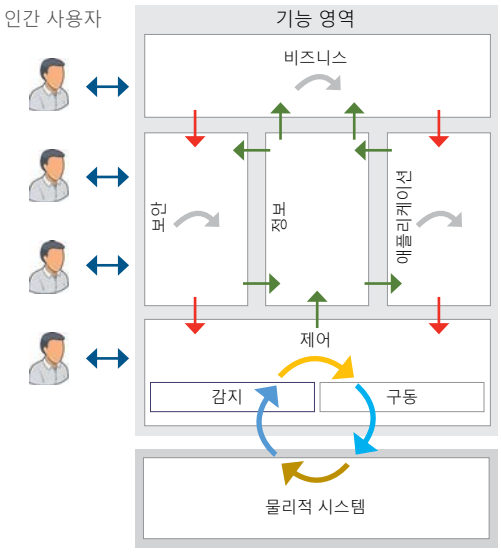
생산 시스템은 앞서 설명한 단일 자산 사용 사례보다 훨씬 복잡합니다. OT 기기가 복잡하게 상호작용하고, 정보가 도관을 따라 퍼듀 모델의 영역 사이를 이동합니다. 수많은 IIoT 기기가 환경에 추가되면서 더욱 관리가 어려워졌습니다. IIoT 환경을 보호하려면 먼저 어떤 구조가 바람직한지 이해해야 합니다.

IIoT의 기능 영역

IIoT 에코시스템의 비즈니스 및 기술 측면을 이해하려면 포괄적인 참조 아키텍처가 필요합니다. Industrial Internet Consortium(IIC)은 Object Management Group(OMG)에서 운영하는 개방적 회원제 기관입니다. IIC는 산업 인터넷의 개발, 도입 및 확산을 촉진하려는 목적으로 설립되었습니다. 산업 인터넷이란 IIoT의 하위 집합으로, 산업 혁명과 인터넷 혁명이 교차하는 지점입니다. IIC가 표준을 수립하는 기관은 아니지만, 회원들은 산업 인터넷의 우선순위를 조정하고 그 기술을 지원하는 데 협력합니다. IIC는 National Institute of Standards and Technology(NIST), MITRE Corporation, IBM, General Electric(GE) 등의 산업 전문 기관과 협력하여 IIoT를 위한 포괄적 참조 아키텍처 가이드, 일명 "산업용 사물 인터넷 볼륨 G1: 참조 아키텍처 가이드(IIRA)"를 개발했습니다.[1] 그림 4는 IIRA 가이드 v1.9 최신판에서 발췌했습니다. 이 가이드에서는 IIoT 에코시스템을 5가지 기능 영역으로 나눕니다.

- 제어 영역
- 운영 영역
- 정보 영역
- 애플리케이션 영역
- 비즈니스 영역

제어 영역은 주로 산업 또는 기계적 측면(즉, 물리적 시스템)을 다룹니다. 예를 들어, 제어, 감지, 구동 기술이 해당합니다.



녹색 화살표: 데이터/정보 흐름, 회색 화살표: 결정 흐름, 빨간색 화살표: 명령/요청 흐름

그림 4: IIoT 에코시스템 기능 영역.

예를 들어 산업 자동화 및 제어 시스템(IACS/ICS)이 여기에 포함됩니다. 제어 영역과 운영 영역을 합쳐서 OT 부분이 되고, 나머지 영역이 IT 부분이 됩니다.

IIoT 기술 아키텍처

IIRA 가이드에서는 IIoT 시스템 아키텍처도 제시합니다. 이 기술 아키텍처는 그림 5와 같이 3단계 구조를 사용합니다.

- **엣지 계층**, OT 관련
- **플랫폼 계층**, OT 및 IT 통합 관련
- **엔터프라이즈 계층**, IT 관련

그림 5: 3단계 IIoT 시스템 아키텍처.

또한, IIRA는 5가지 기능 영역을 3단계 기술 아키텍처에 매핑하고 3가지 네트워크(**근접성 네트워크**, **액세스 네트워크**, **서비스 네트워크**)를 겹쳤습니다. 네트워크는 각 영역과 기술 계층 사이의 통신과 연결을 지원하는 역할을 합니다. 그림 6에서 이 매핑을 확인할 수 있습니다. 통신 네트워크는 유선 또는 무선 기술을 기반으로 할 수 있습니다. 여기에는 로컬 이더넷이나 Bluetooth/Zigbee(근접성 네트워크의 경우) 또는 광역 네트워크(WAN) 대역, 다중 프로토콜 레이블 스위칭(MPLS), 5G 기술(액세스 및/또는 서비스 네트워크의 경우) 등이 포함될 수 있습니다.

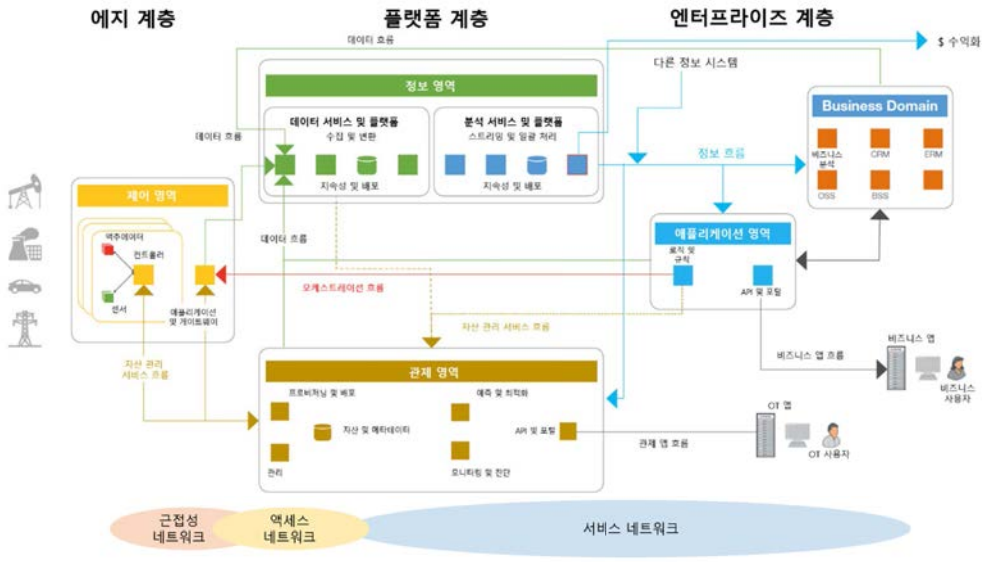


그림 6: IIoT 기능 영역을 3단계 기술 아키텍처에 매핑.

IIoT 보안 아키텍처

보안 구현 과정에서는 상세한 보안 아키텍처를 개발하는 작업이 중요합니다. 보안 아키텍처는 기술과 솔루션을 구현하는 지침이 될 뿐만 아니라, 보안 기술과 솔루션이 다양한 아키텍처 부분에 적용되는 특정 보안 목표와 요구 사항을 충족하는지 평가하는 데도 도움이 됩니다.

OT 보안 배포의 지침이 되는 표준은 ISA/IEC 62443입니다.[2] 그림 7에서는 PERA를 활용한 아키텍처를 활용하여 IIoT 기능 영역, 기술 계층, 보안 요구 사항을 퍼듀 모델에 매핑했습니다. 또한, IIoT 에코시스템에서 사용하는 다양한 통신 네트워크도 표시했습니다.

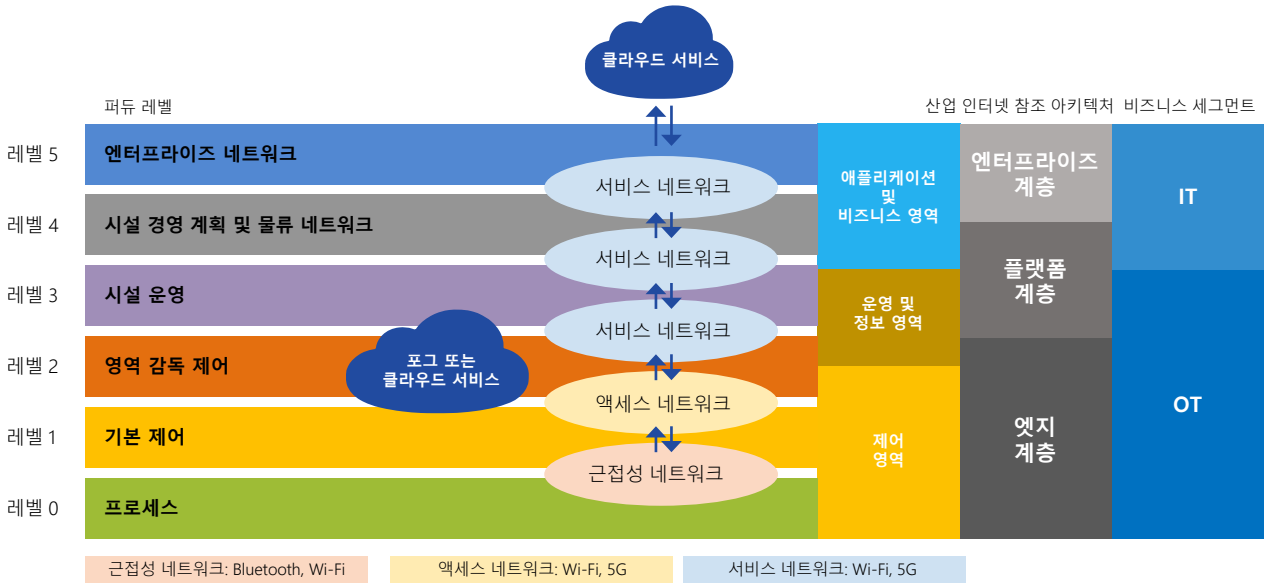


그림 7: IIoT 기능 영역, 기술 계층, 보안 요구 사항을 퍼듀 레벨에 매핑.

그림 7에서 확인할 수 있듯이, IIoT 에코시스템에는 다양한 통신 네트워크가 각 레벨에 통신 채널을 제공할 수 있습니다. 이러한 통신 채널은 보안이 필요합니다. 일반적으로 서비스 네트워크는 전용 사설 통신 네트워크나 임대한 사설 네트워크(이른바 모바일 사설 네트워크(MPN)), 또는 셀룰러 네트워크(예: 4G/LTE, 5G)를 포함한 비공개 액세스 포인트 이름(APN)을 사용합니다. 네트워크의 모든 출입 지점은 사전에 모니터링하고 보호해야 합니다.

엣지 계층(레벨 0, 1, 2로 구성)은 대개 멀티 액세스 엣지 컴퓨팅(MEC) 기반 기술을 통해 IIoT 에코시스템에 컴퓨팅, 스토리지, 분석 기능을 제공합니다. MEC 플랫폼은 레벨 1에 있는 센서, 컨트롤러, 장비(IIoT의 "사물")와 연결한 뒤, 이런 "사물"을 플랫폼 및 엔터프라이즈 계층과 연결합니다. MEC 플랫폼은 주로 가상 운영 체제, 소프트웨어 애플리케이션, 도구를 실행합니다. 모든 MEC 기반 구현은 아래와 같은 필수적인 보안 조치로 보호해야 합니다.

IIoT 보안을 위한 포티넷 솔루션

IIoT 환경을 보호하려면 IT에서 사용하는 것과 동일한 사이버 보안 전략을 IIoT 아키텍처와 사용 사례에 적용해야 합니다. 그러나 OT 환경과 IIoT에는 뚜렷한 특징이 있기 때문에 이를 고려해야 합니다. OT 보안 표준인 ISA/IEC 62443을 기본으로 삼고 NIST 사이버 보안 프레임워크(CSF)[3]를 추가로 참고하여 작성한 아래의 목록은 연결된 IIoT 인프라의 보안 목표를 나타냅니다.

1. 자산 관리
2. 애플리케이션 가시성 및 제어
3. 침입 탐지 및 예방
4. 네트워크 액세스 제어(NAC)
5. 세그멘테이션 및 마이크로 세그멘테이션
6. 신호 보호
7. IoT 플랫폼 보호
8. 로깅 및 모니터링

이 섹션에서는 각 보안 목표를 설명하고 관련 포티넷 솔루션을 간략히 살펴봅니다. 포티넷은 특정 아키텍처가 아니라 조직의 보안 요구사항에 맞는 솔루션을 제공합니다. 그 이유는 자산 소유자가 어떤 아키텍처를 선택하든 보안을 지원하기 위함입니다.

자산 관리

자산 관리는 퍼듀 모델의 모든 레벨에 적용할 수 있습니다. 그러나 네트워크에 연결된 자산의 경우, 네트워크에서 탐색과 식별이 가능한 레벨 1~5의 자산에 적용됩니다. 자산 관리는 광범위한 주제이고, 자산 관리 전략과 구현을 설계할 수 있는 산업 표준과 모범 사례(예: ISO 55001:2014 또는 NIST SP 1800-5)가 공개되어 있습니다.

IIoT 에코시스템에서 자산을 관리할 경우, 포티넷 보안 패브릭 AI에 속하는 여러 가지 솔루션이 도움이 됩니다. 예를 들어, FortiGate 차세대 방화벽(NGFW)과 FortiNAC 네트워크 액세스 제어에 FortiAnalyzer 중앙 로그 관리 및 분석 플랫폼을 결합할 수 있습니다.

포티넷은 오픈 패브릭 에코시스템이라는 광범위한 파트너 네트워크가 있습니다. 이 네트워크의 업계 솔루션 공급업체는 포티넷 보안 패브릭 애플리케이션 프로그래밍 인터페이스(API)를 사용하여 상호 통합합니다. 보안 패브릭 API 통합을 사용하여 파트너 솔루션에서 "패브릭을 지원"하고 솔루션의 기능을 제공할 수 있습니다.[4] 패브릭을 지원하는 파트너 포트폴리오에는 유명한 ICS/OT 자산 관리 솔루션이 다수 포함되었으며, 이들은 포티넷 솔루션(예: FortiGate, FortiSIEM 보안 정보 및 이벤트 관리 시스템)과 매끄럽게 통합되어 전체적인 자산 정보를 제공하고 자산 관리를 지원합니다. 따라서 타사 솔루션에서 수집한 자산 식별 정보를 포티넷 보안 패브릭 플랫폼에서 공유하고 통합할 수 있습니다.

산업 센서와 액추에이터는 수없이 많고 잘 보이지 않는 곳에 흩어져 있습니다. 그래서 인벤토리를 자동으로 구축하고 이런 기기의 실시간 상태를 추적하여 다음과 같은 지표를 수집할 수 있는 시스템을 사용하는 것이 더더욱 중요합니다.

- 기기 유형, 하드웨어 버전, 소프트웨어 버전(해당할 경우)
- 위치
- 네트워크 트래픽 패턴(프로토콜, 패킷/바이트 수, 세션 수)
- 주소 지정 정보 및 자격 증명
- 위협 레벨

OT 환경 구성 요소는 전문화되어 있기 때문에 많은 공급업체가 다양한 환경에서 이런 구성 요소를 검색하고 식별하는 도구를 개발했습니다. 개방적 API를 통해 포티넷 솔루션을 다양한 공급업체의 유명한 NIDS(자산 가시성 및 네트워크 침입 탐지 시스템) 솔루션을 함께 사용할 수 있습니다.

애플리케이션 가시성 및 제어

기기 식별은 자산 가시성의 한 부분에 불과합니다. 프로토콜과 애플리케이션 유형도 제어가 필요합니다. FortiGate 애플리케이션 제어 기능은 기기에서 사용 가능한 프로토콜이나 통신 가능한 애플리케이션을 모니터링하거나 제한할 수 있습니다. 허용되지 않은 통신 프로토콜이나 기능을 사용하면 알림이 생성되고, 필요에 따라 차단할 수도 있습니다. 애플리케이션과 프로토콜의 정의에는 24개 카테고리에서 4,000개 이상의 규칙이 포함됩니다. 모든 일반적으로 사용되는 IoT 프로토콜(예: MQTT, AMQP, HTTP, CoAP)에 적용되고 적절한 구성으로 TLS(Transport Layer Security) 검사를 실행할 수 있습니다. 하이브리드 IIoT 솔루션에는 다양한 산업 프로토콜이 제공됩니다.

FortiAnalyzer는 보안 관제 센터(SOC)가 수집된 정보를 간략히 확인하는 기능과 특정 이벤트의 자세한 정보를 확인하는 기능을 제공합니다. 정기적으로 보고서를 생성해 자산과 통신 네트워크의 정보를 지속해서 받을 수도 있습니다. 또한, FortiAnalyzer는 등록된 보안 구성 요소의 로그 이벤트에 따라 조치를 하는 지능적 이벤트 관리 도구도 내장되었습니다. FortiSIEM은 다양한 타사 제품과 바로 통합하고 더욱 지능적인 상관관계와 사용자 설정을 제공합니다.

침입 탐지 및 예방

IIoT 기기는 가장 먼저 공격을 받는 표적입니다. 주로 퍼듀 모델의 여러 계층을 "정지"시킬 수 있고 외부 세계에서 가장 낮은 계층의 기기로 바로 액세스할 수 있기 때문입니다. 일반적으로 IIoT 기기는 연결이 제한되고 소수의 대상과만 통신합니다(예: IoT 플랫폼, 다른 서버를 제공하는 애플리케이션 서버 정도(펌웨어 업그레이드, 데이터 스토리지)).. 즉, 제대로 설계된 네트워크에서는 해킹된 기기에서 공격을 시작하기가 어렵습니다. 하지만 IoT 플랫폼이나 애플리케이션 서버가 언제든 해킹되어서 로컬 OT 네트워크 내부에서 공격이 시작될 수 있다고 전제해야 합니다.

대부분 IIoT 기기는 기능이 제한적입니다. 취약점이 발생할 가능성은 작지만 다른 문제가 있습니다. IIoT 기능은 직접 개발되는 경우가 많아서 일반적으로 필드 강화된 범용 구성 요소에서는 나타나지 않는 버그가 생길 수도 있습니다. 게다가 IIoT나 IoT를 붙인 기기는 그 종류가 매우 다양하다는 것도 잊지 말아야 합니다. 농토 모니터는 자율 주행 자동차와는 완전히 다른 환경에서 작동합니다. 어떤 기기든 익스플로잇의 가능성을 염두에 두고 보호 조치를 취해야 합니다.

IoT 플랫폼도 다른 소프트웨어와 마찬가지로 취약점이 있을 수 있습니다. 버퍼 오버플로나 다른 메모리 손상을 일으키는 코딩 버그가 대부분입니다. 또한, 대부분 IoT 플랫폼 신호는 일종의 API를 통해 발생하기 때문에 전형적 API 공격을 받을 가능성도 고려해야 합니다. 마지막으로 플랫폼에서 수신한 데이터는 데이터베이스를 읽거나 쓰는 경우가 많습니다. 따라서 SQL 공격도 고려해야 합니다.

다른 서비스 플랫폼과 마찬가지로, 노출을 최소화하고 사용하지 않는 서비스를 남겨 두지 않도록 주의를 기울여야 합니다. (사용하지 않는 서비스가 주로 공격의 원인이 됩니다.) 예를 들어 SMB(Server Message Block) 서비스는 기본적으로 활성화되어 있는 경우가 많은데, 일반적인 공격 벡터이기도 합니다. 열린 포트는 반드시 점검하고 불필요한 서비스는 비활성화하거나 시스템에서 제거해야 합니다.

통신을 처음부터 끝까지 TLS로 보호할 경우, 트래픽을 복호화하는 보안 기기를 적어도 하나 이상 두고 트래픽이 정상인지 확인해야 합니다. 그렇지 않으면 해킹된 IoT 기기가 암호화된 연결을 사용하여 악성 트래픽을 숨길 수 있습니다. 보안 기기가 IoT 플랫폼과 같은 곳에 있다면 TLS 처리와 복호화된 트래픽을 플랫폼에 바로 전달할 수 있습니다.

그렇지 않을 때에는 트래픽을 다시 암호화하여 감청을 차단해야 합니다.

침입 방지

FortiGate 침입 방지 시스템(IPS)은 다양한 유형의 공격에 대응하기 위해 IIoT 및 IoT에 대한 여러 가지 공격을 탐지하고 차단하도록 설계되었습니다.

- **익스플로잇**: 모든 취약점 공격을 포함하며, 주로 서비스 거부(DoS)(소프트웨어 내에서 충돌을 일으키거나 추가 작업 발생)나 로컬 코드를 실행하는 데 사용합니다. 이는 2차 공격(예: 악성 실행 파일 전송)으로 이어지는 경우가 많습니다.
- **정찰**: 열린 TCP나 사용자 데이터그램 프로토콜(UDP) 포트를 찾거나 알려진 소프트웨어나 프로토콜 버전을 찾는 스캔 공격입니다. 정찰 공격의 목표는 대개 취약점이나 중요한 표적을 찾는 것입니다.
- **퍼징 공격**: 취약점을 찾는 방법 중 하나입니다. 일반적으로 통제된 로컬 환경에서 실행하지만, 라이브 네트워크에서 무차별 대입 공격으로 사용할 수도 있습니다. 예를 들어, 의도적인 프로토콜 오류, 극단적으로 긴 필드 사용, 잘못된/비정상적인 날짜 사용 등이 있습니다. 이런 기술은 모두 프로그래밍 오류를 일으키도록 설계되었으며, 취약점을 찾거나 작동을 중단시키는 것이 목적입니다.

FortiGate IPS 기능은 이런 유형을 비롯한 모든 공격을 식별하여 차단합니다. ICS/OT를 위한 선택적 산업 보안 서비스 패키지를 포함해 30,000개 이상의 규칙이 포함되어 있습니다. 규칙 패키지는 **FortiGuard Labs**(포티넷의 연구 분석 기관)에서 매일 자동 업데이트하여 보호를 최신 상태로 유지합니다.

가상 패칭

IIoT 기기, 컨트롤러, 인프라 구성 요소에서 취약점이 발견되었을 때 가장 효과적인 해결 방법은 공급업체에서 제공한 펌웨어 업데이트로 해당 기기를 패치합니다. 하지만 그러지 못할 경우가 있습니다. 오래된 기기는 보안 업데이트가 중단되었을 수도 있습니다. 보안 업데이트가 제공되더라도 업데이트를 설치하는 데도 위험이 따르며, 대부분은 일정 기간 테스트를 거쳐 새 릴리스를 생산에 배포합니다. 펌웨어 업데이트를 지원하지 않는 기기도 있습니다.

포티넷의 정식 패치가 적용되는 동안 가상 패칭(또는 취약점 보호)을 제공하는 기능으로 이런 문제를 해결할 수 있습니다. 업스트림 침입 방지 기기(예: FortiGate NGFW)를 사용하면 취약점이 있는 표적에 공격이 도달하기 전에 탐지해 차단할 수 있습니다. 이는 확실한 패치를 설치하거나 패칭이 불가능할 경우 영구적 보호 조치를 취할 때까지 일시적으로 보호해주는 역할을 합니다.

보안 침해 탐지

IT나 OT 모두 사이버 보안의 일반적 목표는 기기에 침입하기 전에 공격을 차단하는 것이 되어야 합니다. 하지만 공격이 방어를 뚫고 침투하면 IIoT 보안 솔루션이 감염의 징후를 탐지하고 신속하게 조치를 해야 합니다.

공격자가 기기의 제어권을 획득하면 여러 가지 위협이 발생할 수 있습니다. 공격이 기기를 비활성화하는 데 그칠 수도 있습니다. 악성 펌웨어(봇)을 설치할 필요가 없기 때문에 대체로 가장 손쉬운 유형의 공격입니다. 이와 같은 공격은 대가를 요구하는 랜섬 모델을 사용하여 이익을 취하기도 합니다. 경우에 따라서 공격자가 기기를 영구적으로 파괴하기도 합니다. 예를 들어 기기 수명이 끝날 때까지 배터리 수명이 유지되어야 하는 배포에서 배터리 사용량을 서서히 늘리다가 완전히 방전시킬 수 있습니다.

더욱 일반적인 공격(공격자에게 가장 유연성을 많이 제공하는 공격)은 봇넷입니다. IoT 봇넷이 얼마나 효과적인지는 지난 2017년에 Mirai 공격으로 입증되었습니다. 수십만 개의 IoT 기기(주로 카메라와 DVR)가 역사상 최대 규모의 분산형 서비스 거부(DDoS) 공격에 악용되었습니다.[5] 봇넷은 IIoT 기기도 같은 방식으로 악용할 수 있습니다.

FortiOS 봇넷 보호를 사용하면 대상 주소, 도메인, 프로토콜에서 봇넷 활동이 탐지될 때마다 알림이 생성되고 봇넷이 차단됩니다. FortiGuard Labs는 유명한 봇넷 대상 주소와 포트 조합 목록을 가지고 있으며, 모든 FortiOS 기기에 수시로 업데이트합니다. 모든 외부로 나가는 세션은 이 목록을 적용하여 검사합니다. 또한, FortiGuard 보안 침해 지표(IOC) 서비스에서 다른 알려진 악성 대상과 연결된 것이 탐지되면 보안 침해 알림이 생성됩니다. 고속 도메인(IP 주소 매핑을 지속해서 변경하는 도메인)을 사용하는 봇넷은 DNS 요청을 가로채서 검사하면 도메인 자체를 검사할 수 있습니다. 마지막으로 대상 주소와 도메인을 모르더라도 C&C 프로토콜로 대부분 봇넷을 탐지할 수 있습니다. 포티넷은 이 세 가지 방법을 함께 사용하여 봇넷에 감염된 기기를 최대한 많이 찾아냅니다.

네트워크 액세스 제어(NAC)

NAC는 모든 통신 네트워크 경계에 적용할 수 있습니다. 그러나 통신 네트워크 유형(예: 레이어 2 vs. 레이어 3)에 따라 배포 방식이 달라집니다. 가장 간단하게 NAC를 구현하고 싶다면 지원되는 IIoT 자산에서 802.1X 네트워크 인증 프로토콜을 활성화하면 됩니다. FortiGate, FortiNAC, FortiAuthenticator 솔루션을 조합한 포티넷 기술을 사용하면 통합 인증 및 승인 기능을 갖춘 NAC를 간단히 구현할 수 있습니다. 무선 네트워크의 경우, FortiAP 보안 무선 액세스 포인트를 FortiGate와 통합하고 무선 기기를 제어할 수 있습니다. FortiSwitch 솔루션은 액세스 네트워크 내에 구현하면 IIoT 컨트롤러의 액세스 권한을 세부적으로 제어할 수 있습니다.

일반적으로 IIoT 네트워크는 정기 또는 임시 유지관리나 문제 해결을 위해 타사 원격 액세스를 흔히 사용합니다. 여기에는 원격 자산 구성이나 원격 공장/시설 승인 검사(FAT/SAT)가 포함됩니다. NAC 기능으로 타사 연결 요청에 허가 전/후의 네트워크 정책을 적용할 수 있습니다. 원격 액세스는 FortiToken 솔루션을 통합해 다단계 인증(MFA)으로 보강할 수 있습니다.

세그멘테이션 및 마이크로 세그멘테이션

세그먼테이션과 마이크로 세그멘테이션은 산업 네트워크를 물리적 또는 가상 보안 세그먼트(영역)로 나눌 때 주로 사용하는 방법입니다. 일반적으로 로컬 영역 네트워크(LAN)나 광역 네트워크(WAN) 사이를 분리합니다. 때로는 노스-사우스(north-south) 통신이라고도 합니다. 마이크로 세그멘테이션은 LAN 내부에서 실행하고 이스트-웨스트(east-west) 통신을 제어하는 데 사용합니다. 산업 네트워크의 경우, 네트워크 세그먼트에는 다양한 산업용 LAN 또는 WAN이 포함되고 네트워크 마이크로세그먼트에는 여러 가지 산업 컨트롤러와 호스트(예: RTU, HMI)가 포함될 수 있습니다.

원래 세그멘테이션은 자산 분리를 목적으로 산업 네트워크에서 사용되었습니다. 공격자가 다수의 기기에 액세스하기가 어려워지고 사이버 공격이 네트워크 전체로 확산되지 못하게 차단하는 효과가 있었습니다. 그 외에도 보안 적용과 컨트롤이 개선되고 네트워크 가시성이 향상된다는 장점이 있습니다. 일반적으로, 모든 네트워크 경계와 각 퍼듀 레벨에 적용됩니다. 앞서 설명했듯이, 세그먼테이션은 각 레벨에서 자산에 원하는 보호 수준에 따라 물리적일 수도 있고 논리적일 수도 있습니다. 자산은 함께 묶고(퍼듀 용어로는 "영역을 나누고") 다른 자산과 분리해야 합니다. "도관"이라고 하는 특수한 세그먼트(영역)를 영역과 네트워크 경계 사이, 또는 영역이 만나는 곳에 구현해야 합니다. 이를 위해서는 네트워크 통신이나 정보 교환을 모니터링하고 필터링하는 등, 다양한 보안 컨트롤을 구현해야 합니다.

일반적으로 세그멘테이션은 네트워크 스위치와 가상 LAN(VLAN)으로 구현합니다. 네트워크 라우터나 방화벽은 각 VLAN 사이의 통신, 즉 VLAN 간 통신을 허용하는 데 사용합니다.침 VLAN은 네트워크 스위치 수준에서 LAN을 가상으로 분할하고 네트워크 자산을 가상 영역으로 그룹화하는 데 유용한 메커니즘을 제공합니다. 그러나 네트워크 트래픽을 검사하고 악성 통신(페이로드)가 통신 채널을 통과하는지 확인하는 데는 효과적이지 못합니다. VLAN 간 통신을 위한 차세대 침입 방지(NGIPS) 기능이 내장된 NGFW를 사용하면 VLAN 사이의 네트워크 트래픽을 검사하는 문제를 해결하고 VLAN 통신에 결정 기반 보안 정책을 효과적으로 구현할 수 있습니다. 그러나 한 가지 문제는 남아 있습니다. VLAN 내부의 호스트 간 통신, 즉 VLAN 내부 통신이 틈새가 됩니다. 검사를 위해 트래픽을 보내지 않는 한, NGFW에서 VLAN 내부 통신을 검사하지 않습니다. 이를 마이크로 세그멘테이션이라고 합니다.

산업 네트워크 내의 마이크로 세그멘테이션은 각 산업용 VLAN 또는 LAN을 개별 자산 수준으로 보안 세그먼트를 나누고 보안 컨트롤을 정의한 다음, 각 고유한 마이크로세그먼트에 서비스를 전달하는 방법으로 세그멘테이션을 더욱 완벽하게 실행합니다. 오늘날 산업 IoT 환경은 인터넷이 지원되는 복잡한 개방적 표준 통신 프로토콜을 사용하는데, 생산 제어 환경의 민감한 정보가 전송되는 경우가 많습니다. 통신 프로토콜이 개방적이고 복잡하기 때문에 이를 통과하는 정보를 조작하면 환경에 혼란을 생기고 사이버 공격의 여지가 생길 수 있습니다.

산업 프로토콜과 통신을 인식하는 NGIPS가 내장된 NGFW는 마이크로 세그멘테이션에 매우 효과적일 수 있습니다. 자산 간의 통신을 보안 정책에 따라 평가하고, 자산의 인그레스 및 이그레스 지점에서 IIoT 프로토콜과 통신을 검사할 수 있습니다.

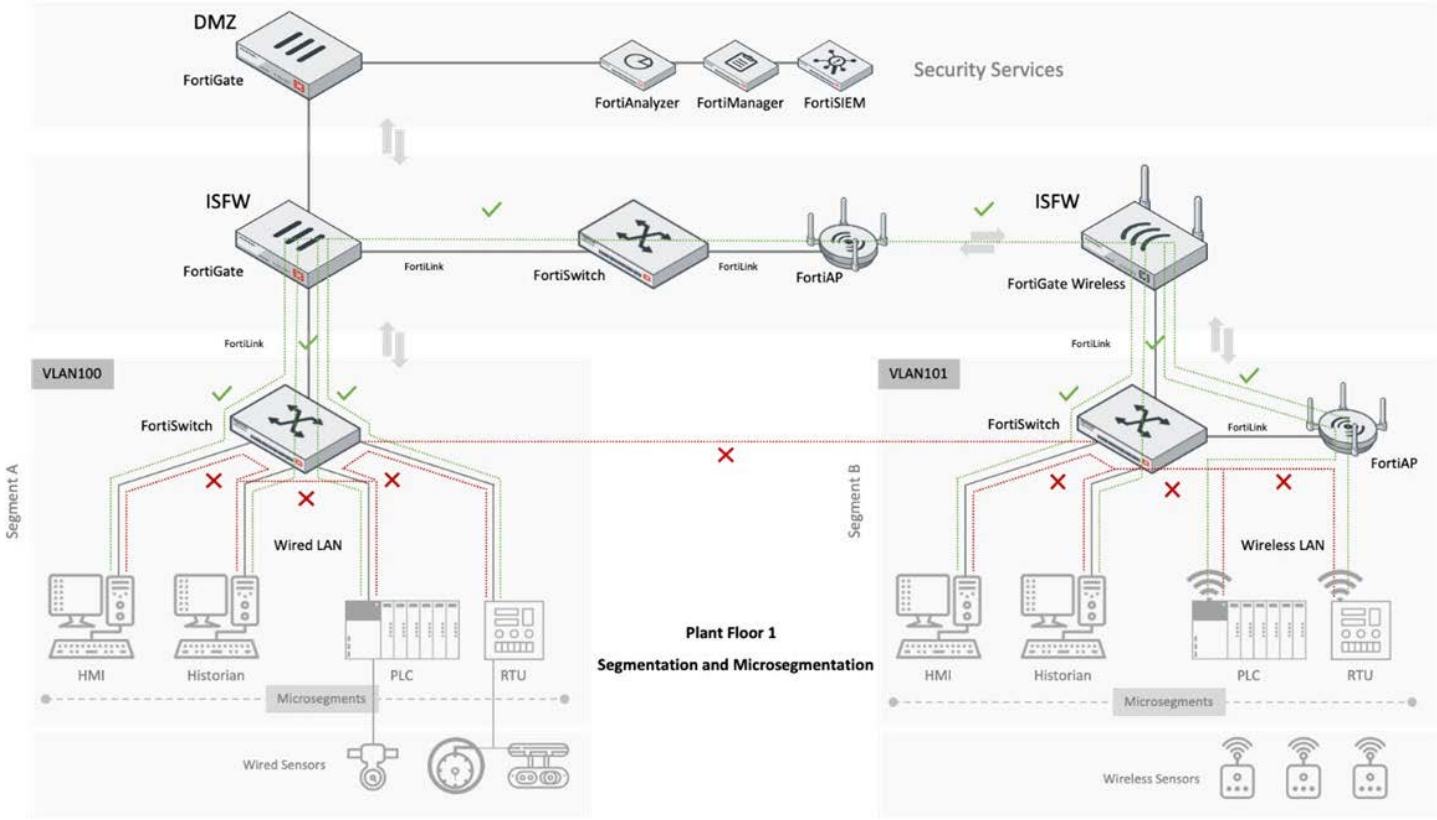


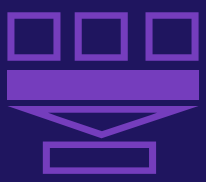
그림 8: 유무선 산업 네트워크의 세그멘테이션과 마이크로 세그멘테이션.

예를 들어 그림 8은 여러 가지 생산 LAN으로 구성된 산업 환경을 나타냅니다. 각 생산 LAN에는 여러 VLAN이 있고, 각 VLAN에는 여러 호스트(예: RTU, HMI)가 있습니다.. LAN은 FortiSwitch를 통한 유선 네트워크나 FortiAP를 사용한 무선 연결로 통신합니다. FortiGate NGFW는 내부 세그멘테이션 방화벽(ISFW) 역할을 하며 LAN을 세그먼트 A와 B로 나누고 두 네트워크 세그먼트를 오가는 모든 네트워크 통신에 VLAN 간 라우팅, 가시성, 검사를 제공합니다.

또한, 각 VLAN(VLAN 100 및 101)은 동일한 ISFW를 사용하여 마이크로 세그멘테이션을 실행하고 세그먼트 내의 각 호스트를 분리합니다. FortiGate NGFW가 NGIPS와 딥 패킷 검사(DPI) 기능을 산업 프로토콜에 실행하면 프로토콜 페이로드까지 가시성과 제어 기능이 제공되고, 나아가서는 각 호스트를 오가는 모든 네트워크 통신 정보를 제공하고 이를 제어할 수 있게 됩니다. 마찬가지로 동일한 ISFW를 VLAN 내부 통신에도 적용합니다.

가상 도메인(VDOM)은 마이크로 세그멘테이션을 적용한 산업 IoT 환경에 매우 유용합니다. 일부 IIoT 기기가 IP 기반 라우팅을 지원하지 않을 수도 있기 때문입니다. FortiGate는 IP 기반이 아닌 모드(레이어 2)와 IP 기반 모드(레이어 3)에서 동시에 실행하도록 구성할 수 있습니다. 이를 각각 투명한 VDOM과 NAT/라우팅 VDOM이라고 합니다. 그리고 포티넷 FortiLink는 FortiGate 내에서 FortiSwitch와 FortiAP를 검사합니다. FortiGate 내에 통합된 FortiSwitch와 FortiAP를 구성하고 관리하는 데 도움을 제공합니다. 기본적으로 FortiLink, 통합 FortiSwitch, FortiAP는 FortiGate NGFW에서 확장된 네트워크 포트 역할을 합니다.

포티넷의 OT 보안 제품을 사용하는 가장 큰 장점은 산업 프로토콜에 대한 가시성을 포함한 산업 환경 분리와 마이크로 세그멘테이션 기능입니다. FortiGate, FortiSwitch, FortiAP 등을 비롯한 포티넷 제품은 포티넷 보안 패브릭에 통합되어 산업 환경과 엔터프라이즈 디지털 환경을 전체적으로 보호합니다.



FortiGate의 가상 도메인 (VDOM) 기능은 하나의 FortiGate를 여러 가상 방화벽 인스턴스로 나누어 유연성을 제공합니다. 동일한 FortiGate 내에 있는 각 가상 방화벽 인스턴스는 독립적으로 보안 기능을 수행합니다.

신호 보호

5G 기술이 안정화되면 산업 네트워크에서 셀룰러 액세스 네트워크의 사용이 일반화됩니다. 이런 네트워크는 신호 오버헤드가 높습니다. 전송되는 데이터 용량보다 IIoT 엔드포인트 수가 많을 경우, 의도적이든(사이버 공격) 의도적이 아니든(기기 오작동) 신호가 폭증할 위험이 있습니다.

의도치 않은 신호 폭증이 특히 위험한데, 그 이유는 임베디드 기기에서 오류를 처리하기가 매우 어렵기 때문입니다. 기기를 정상 상태로 되돌리는 가장 신뢰할 만한 방법은 재시작입니다. 이론적으로는 그렇습니다. 하지만 실제 운영 환경에서는 기기를 다시 시작하기 어려울 수 있습니다. 게다가 외부 요소(예: 고온, 정전, 지진)로 인해 오류가 발생했을 수도 있습니다. 외부 요소가 다수의 비슷한 기기에 영향을 미친다면 모든 기기를 동시에 네트워크에 다시 연결해야 합니다. 이로 인해 신호 인프라에서 오버헤드가 발생하면 해당 기기뿐만 아니라 네트워크를 공유하는 다른 서비스까지도 정지될 수 있습니다.

FortiOS는 신호 폭증은 물론이고 통신 네트워크를 보호하는 다양한 기능을 제공합니다. 또한, 포티넷 IPS는 특정 네트워크 동작에 대한 규칙(예: 속도 기준 규칙)을 정의하는 기능이 있습니다. 많은 IoT 기기가 패킷 속도를 예측 가능합니다. 이 사실을 이용하면 (오작동이나 해킹으로 발생할 만한) 비정상적인 활동을 찾아내서 네트워크에서 기기를 제거하고, 신호 인프라를 보호할 수 있습니다.

IoT 플랫폼 보호

IoT 플랫폼은 모든 IIoT 서비스에서 중추가 되고, 규모가 큰 네트워크에서는 플랫폼 계층으로 구현할 수 있습니다. 모든 신호와 데이터는 대개 하나 이상의 플랫폼 노드를 통과하므로 이런 노드를 공격으로 보호하는 것이 매우 중요합니다. 기존 IoT 모델에서 IoT 플랫폼은 클라우드에 위치합니다. 하지만 IIoT에서 이 방식을 사용하기에는 두 가지 문제가 있습니다.

- 이벤트 로직(예: 센서값에 따른 액추에이터 조정)의 경우, 기기와 클라우드를 오가는 왕복 시간이 너무 길고 클라우드 연결이 불안정할 수 있습니다.
- 데이터를 클라우드로 보낼 때도 공개 인터넷 링크를 타고 비공개 데이터를 전송해야 하기 때문에 보안 위험이 발생할 수 있습니다.

3GPP(The 3rd Generation Partnership Project, 모바일 통신 프로토콜을 개발하는 표준 기관의 컨소시엄)는 이 문제를 해결하기 위해 다음과 같이 다양한 솔루션을 제안했습니다.

- 5G 패킷 코어 인스턴스를 고객 프레미스나 그 근처에 구현하는 MEC 아키텍처. IoT 서비스 플랫폼과 관련 애플리케이션 서버가 온프레미스에 위치하기 때문에 왕복 시간과 데이터 보호 문제가 해결됩니다.
- 비공개 5G 네트워크. 위의 솔루션과 유사하지만 5G 패킷 코어가 최종 사용자에게만 할당된다는 차이가 있습니다. 개인정보 보호 문제가 해결되고 인프라를 완전히 제어할 수 있습니다.

위의 솔루션 중 하나를 선택하거나 두 가지를 모두 사용해서 매우 안정적이고 지연이 낮으면서도 대역폭이 높은 애플리케이션을 제공하고 모든 중요 데이터를 최종 사용자의 영역에 남길 수 있습니다.

보안의 관점에서 보면 고객 프레미스나 그 근처로 프로세싱을 가져오는 것(이른바 "엣지 컴퓨팅")은 장점이 있습니다. 데이터를 WAN 링크나 공개 인터넷을 통해 보내지 않고 로컬에서 트랜잭션을 처리할 수 있습니다. 로컬에서 처리할 수 없는 트랜잭션은 적절한 보안 정책을 적용한 로컬 인터페이스를 통해 더 높은 레이어로 내보냅니다.

신뢰할 수 없는 네트워크를 통해 클라우드로 데이터를 보내야 하는 경우, 암호화와 무결성 보호를 적용하여 감청이나 조작으로부터 보호해야 합니다. FortiOS는 확장성이 높으면서도 매우 안정적인 필드 강화 TLS와 IPsec(Internet Protocol security) 구현을 제공합니다. FortiGate 어플라이언스의 애플리케이션 전용 통합 회로(ASIC)를 사용하거나 가상 인스턴스의 중앙 처리 장치(CPU) 가속 기능을 사용해 하드웨어를 가속하기 때문입니다.

로깅 및 모니터링

중앙 집중형 로깅 및 모니터링으로 한 곳에서 모든 IIoT 에코시스템을 관찰할 수 있습니다. 그 역할은 주로 SOC 또는 네트워크 관제 센터(NOC)가 담당합니다. 기준을 결정하거나 구성하고, 기준에서 벗어나거나 악의적 활동에서 발생한 로그와 이벤트에 대한 액세스를 제공하는 기능이 포함되어야 합니다. 로깅 및 모니터링 기능은 퍼듀 레벨 2와 레벨 3(레벨 2.5) 사이, 또는 레벨 3과 레벨 4(레벨 3.5) 사이, 또는 레벨 5를 연결하는 도관에 설치하는 것이 적절합니다. 위치는 IIoT 조직의 운영 구조에 따라 달라집니다.

포티넷 솔루션(예: FortiAnalyzer, FortiManager, FortiSIEM)은 IIoT 에코시스템과 OT 환경 전체에 배포된 포티넷 기술을 한 곳에 로깅하고 모니터링하는 기능을 지원합니다. 또한, 포티넷 오픈 패브릭 에코시스템에 속한 수백 개의 공급업체 기기에서 정보를 수집할 수도 있습니다.

IIoT 환경을 지원하는 포티넷 솔루션 요약

보안 요구 사항	해당 퍼듀 레벨	통신 네트워크	기능 영역	기술 계층	포티넷 솔루션
자산 관리	모든 레벨	모든 네트워크	모든 영역	모든 계층	FortiGate, FortiSwitch, FortiAP, FortiNAC, 패브릭 지원 파트너 솔루션
애플리케이션 가시성 및 제어	레벨 1~5	모든 네트워크	모든 영역	모든 계층	FortiGate, FortiSwitch, FortiAP
침입 탐지 및 대응	레벨 1~5	모든 네트워크	모든 영역	모든 계층	FortiGate, FortiSwitch, FortiAP, 패브릭 지원 파트너 솔루션
네트워크 액세스 제어	레벨 1~5 내부 및 중간	네트워크 경계 사이	모든 영역	모든 계층	FortiGate, FortiSwitch, FortiAP, FortiAuthenticator, FortiToken, FortiNAC
네트워크 세그멘테이션	레벨 1~5 내부 및 중간	네트워크 경계 사이	모든 영역	모든 계층	FortiGate, FortiSwitch, FortiAP
로깅 및 모니터링	레벨 3.5 내부 또는 레벨 3.5~ 레벨 5 사이	네트워크 경계 사이	모든 영역	모든 계층	FortiGate, FortiSwitch, FortiAP, FortiNAC, FortiAnalyzer, FortiManager, FortiSIEM, 패브릭 지원 파트너 솔루션

그림 9: 포티넷 기술을 보안 요구 사항 및 IIoT 기능 영역, 계층, 네트워크에 매핑.

포티넷의 강화된 퍼듀 모델

최근 몇 년간 IIC와 같은 여러 표준 기관에서 연구를 진행하기는 했지만, 퍼듀 모델에는 아직 IIoT와 무선 연결 기능이 공식 통합되지 않았습니다. 연구가 진행되고 있더라도 자산 소유자와 보안 전문가는 공식 승인 절차를 기다렸다가 보안 조치를 구현할 시간이 없습니다. 그래서 포티넷에서는 지난 몇 년 동안 향상된 퍼듀 모델을 제공하고 있습니다. 어떤 아키텍처에도 적용할 수 있도록 IIoT 기기와 플랫폼, 무선 기기(IIoT 또는 그 외의 기기)를 OT 보안 경계 내에 물리적으로 존재하는 평평한 "6영역"에 수평으로 배치했습니다. 아래의 그림 10을 참조하세요.

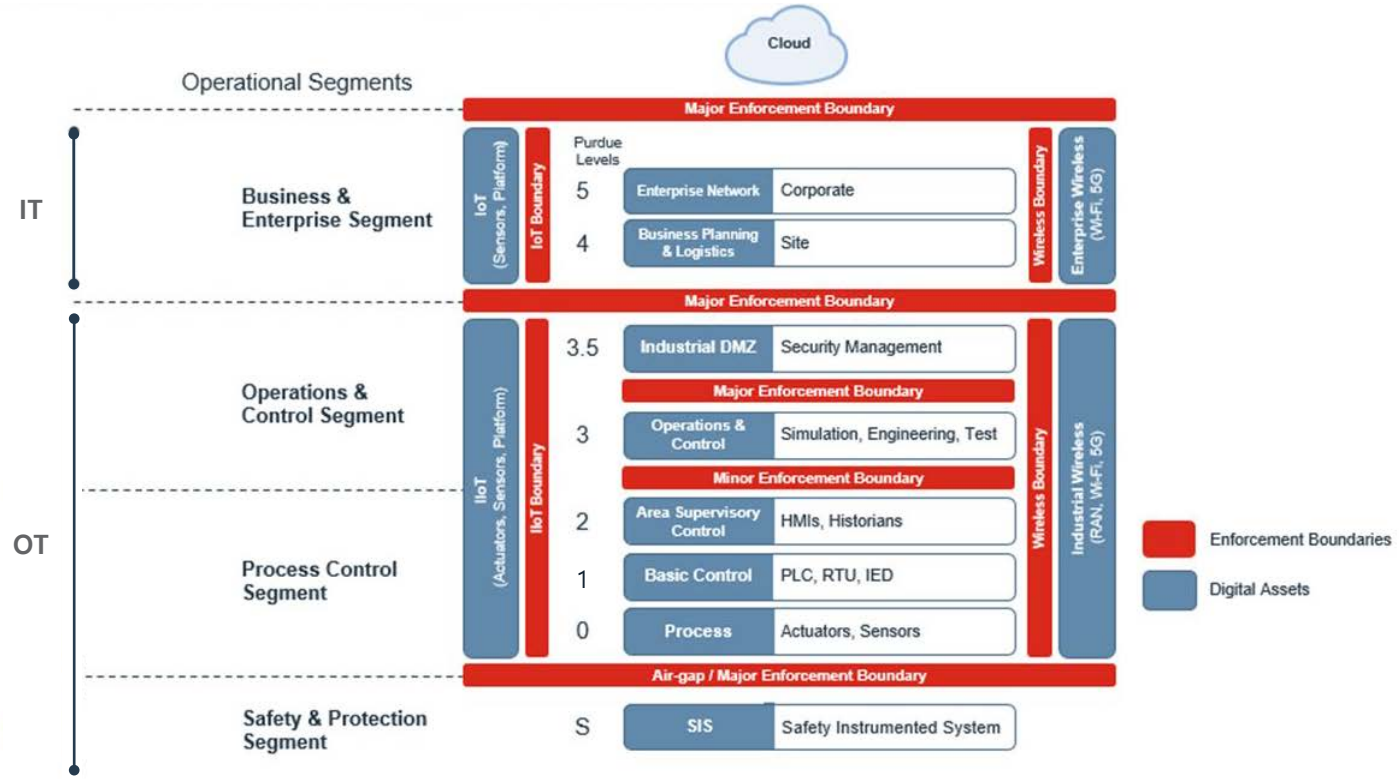


그림 10: IIoT 및 무선을 포함하여 강화한 퍼듀 모델.

결론

생산 환경은 무선, 5G, IIoT 기술의 등장으로 엄청난 변화를 겪고 있습니다. OT 기반 조직의 유연성, 생산성, 제어 역량을 시험하는 새로운 시대를 맞이하게 되었습니다. 그와 동시에 비즈니스와 공개 인프라의 중요한 곳을 노리는 범죄자에게는 새로운 공격 벡터가 열리고 있습니다. 이런 인프라를 설계 및 보호하는 표준이 꾸준히 발전하고 있지만 최종 결과가 나올 때까지 운영과 보안 관리를 미룰 수는 없습니다. 지금 이 순간에도 위협은 실재합니다. 따라서 오늘날의 변화하는 유무선 OT 환경과 함께 발전할 수 있는 요소를 포함하여 유연한 보안 인프라를 구현하는 것이 중요합니다.

포티넷은 사이버 보안에만 전념하는 기업입니다. IT와 OT 환경을 보호한 경력만 20년 이상인 포티넷은 업계 최고의 순수 사이버 보안 기업으로서 상호 호환될 뿐만 아니라 수백 개 공급업체의 제품과도 연결되는 완전한 통합 보안 솔루션 제품군을 제공합니다. 여기에는 모든 주요 ICS 및 감시 제어 및 데이터 수집(SCADA) 솔루션, 자산 및 네트워크 산업 시스템 가시성 제품, 산업 시스템 통합 도구 등이 포함됩니다. 생산과 OT 운영기술이 발전하는 동안, 지금 포티넷이 투자한 보안 기술이 점차 변화하며 미래의 요구 사항에 맞추어 성장하는 모습을 보여드리겠습니다.

[1] "Industrial Internet Reference Architecture," IIC, 2020년 12월 30일 액세스.

[2] "New ISA/IEC 62443 standard specifies security capabilities for control system components," ISA, 2020년 12월 30일 액세스.

[3] "Cybersecurity Framework," NIST, 2020년 12월 30일 액세스.

[4] "Open Fabric Ecosystem," Fortinet, 2020년 12월 30일 액세스.

[5] Josh Fruhlinger, "The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet," CSO, 2018년 3월 9일.

서울특별시 강남구 영동대로 325 에스타워 14 /15층 전화: 080-559-8989 Email: kr-callcenter@fortinet.com

884983-0-0-KO