솔루션 개요

Fortinet으로 OT 보안 통합 및 단순화

종합 요약

운영 기술(OT)과 정보 기술(IT) 환경은 모두 사이버 보안이 필요하지만 OT 환경은 IT와는 다른 사이버 보안에 대한 고려가 필요하다는 독특한 특징이 있습니다. Fortinet 보안 패브릭은 이런 독특한 OT의 특징을 반영하면서도 OT와 IT 사이버 보안을 단일 대시보드에서 관리할 수 있게 지원합니다. 또한, 보안 패브릭은 조직의 보안 인프라 전체에 진정한 통합과 자동화를 제공하며, 가상 환경, 클라우드, 온프레미스를 포함한 모든 네트워크 세그먼트, 기기, 어플라이언스에 타의 추종을 불허하는 보호와 가시성을 보장합니다. 특히, 여러 가지 서로 호환되지 않는 보안 솔루션을 사용하는 모델에 비해 복잡성이 적습니다.

사이버 보안을 어렵게 하는 OT만의 고유한 특징

조직에서 OT 환경을 보안하려면 여러 가지 고유한 문제를 해결해야 합니다. 예를 들어 다음과 같은 문제가 있습니다.

- 보안 사고로 인해 OT의 운영이 중단되면 생산과 수익에서 수만 달러, 경우에 따라서는 수백만 달러의 손실이 발생할 수 있습니다.
- 패치를 위해 특정 OT 시스템을 정지하는 것은 매출 손실 위험으로 인해 불가능한 것이나 마찬가지입니다.
- OT 환경에서 새로운 사물 인터넷(IoT) 기기가 도입되면서 새로운 위험이 생겨났고, 추적과 보고가 반드시 필요한 새로운 규정 준수 요구 사항이 나타났습니다.
- OT 환경에 인공 지능(AI), 머신 러닝(ML) 또는 디지털 혁신(DX)의 다른 IP 기반 요소를 통합할 경우에도 새로운 위험이 생겨납니다.

OT 보안은 IT 보안과 비교하면 다른 사고방식과 접근법이 필요한데, 효율, 안전성, 가용성의 관점에서 살펴봐야 합니다. 공장을 운영하고 제조업에 있는 리더들은 이 점을 염두에 두고 다음과 같은 특징을 따르는 보안 방식을 찾아야 합니다.

관리하기 쉬운 통합 솔루션

많은 조직이 서로 다른 OT 보안 문제를 해결하는 포인트 보안 솔루션을 적용해 통합되지 않은 보안 아키텍처를 구현합니다. 제품은 많이 나와 있지만 대부분 서로 호환되지 않습니다. 미국 에너지부 국립 연구소(U.S. Department of Energy National Laboratories)의 연구 결과에 따르면, 7개 부문에 57개 OT 보안 솔루션이 있습니다.[1] 얼마 지나지 않아 조직들은 여러 콘솔에서 여러 도구를 관리하고, 보안 데이터를 수작업으로 수정해서 조정, 분석을 거쳐야 합니다. 이렇게 되면 보안에 구멍이 생기고 사람의 실수가 늘어납니다.

Fortinet 보안 패브릭은 서로 분리된 포인트 보안 제품을 사용하는 아키텍처에 비하면 평균 비용과 생산성이 11.5% 절약됩니다.

Fortinet 보안 패브릭은 서로 조정되는 개방적 보안 플랫폼에 보안 솔루션을 통합하여 단순화된 사이버 보안을 제공합니다(그림 1 참조). 보안 패브릭은 IT와 OT 환경에 모두 적용되고, 각 보안 요소가 호환되도록 지원하며, 지능형 위협을 탐지하여 예방하기 위한 위협 인텔리전스를 공유합니다. 보안 패브릭에는 FortiGuard Labs에서 새로 탐지된 제로데이 공격, 지능형 위협, 봇넷, 보안 침해 지표(IOC) 등에 관한 통합 위협 인텔리전스가 포함됩니다.[2] 또한, 완전히 통합하여 동작하는 샌드박스(FortiSandbox)가 포함되어 있어서 알려지지 않은 위협과 제로데이 위협을 탐지하여 예방할 수 있습니다.

단일 대시보드를 통해 모든 환경을 관리하며 전체를 아우르는 보안 방식을 사용하면 직원 교육이 간단해지고 총소유 비용(TCO)이 감소합니다. 이러한 효과는 객관적으로도 입증되어 있습니다. Fortinet 보안 패브릭을 타사에서 분석한 결과, 6년간 여러 벤더가 제공하는 각 분야 최고의 포인트 보안 솔루션을 별도로 관리한 것에 비해 비용 및 생산성 절감 효과가 평균 11.5%나 발생했습니다.[3]

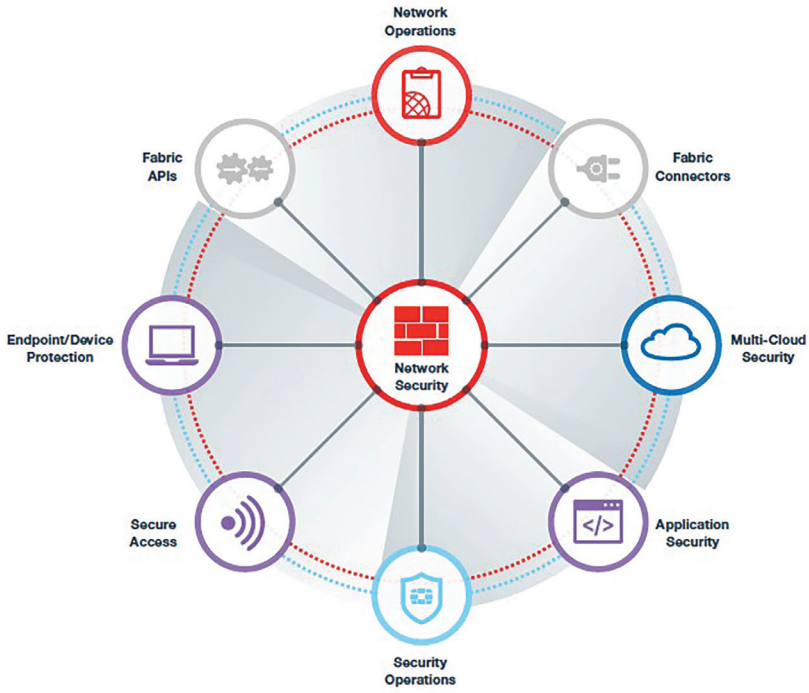

그림 1: Fortinet 보안 패브릭은 모든 환경에서 여러 보안 기술이 서로 매끄럽게 작동하도록 돕고, 위협 인텔리전스라는 단일 소스를 통해 이를 지원합니다. 따라서 네트워크상에서 보안의 빈틈이 사라지고 공격과 보안 침해에 신속히 대응할 수 있게 됩니다.

OT의 한계를 반영한 구조

"버추얼 패칭"은 다른 방식으로 패치 작업을 할 수 없는 OT 기기를 보호합니다.

OT 네트워크는 오랜 경험을 통해 검증된 프로그래밍 가능한 로직 컨트롤러(PLC)와 같이, 신뢰할 수 있는 구형 기기가 많이 포함되어 있습니다. 그러나 이런 기기를 보안할 때는 이들의 독특한 특징을 고려해야 합니다.

예를 들어 PLC와 다른 OT 요소는 IT 네트워크 보안에서 사용하는 기술로 능동적인 스캔이 불가능합니다. 보안 패브릭의 경우에는 네트워크 트래픽을 수동 스캔하여 관찰된 특징과 동작에 따라 각 OT 네트워크 요소 및 상태를 프로파일링합니다. 또한, 취약성을 보완하는 소프트웨어 업데이트의 필요성도 고려합니다.

하지만 그 외에도 다른 문제가 있습니다. 바로 대부분의 OT 요소는 패치가 불가능하다는 것입니다. FortiGate 차세대 방화벽(NGFW)은 이러한 문제를 독특한 방식으로 해결합니다. FortiGate NGFW은 FortiGuard 산업보안 서비스[4]를 이용하여(FortiGate 엔터프라이즈 번들[5] 이나 360 번들[6]에 포함) 대부분의 OT 프로토콜을 식별하고 단속할 수 있는 시그니처를 업데이트 받습니다. NGFW는 이 시그니처를 사용하여 알려진 OT 취약성을 익스플로잇하려는 시도를 탐지해 차단할 수 있습니다(표 1 참조). 이를 구형 OT 장비를 보호하는 "버추얼 패칭"이라고 합니다.

그 외에도 OT는 대부분 OT 기기에서 보안 클라이언트 소프트웨어를 설치할 수 없다는 한계가 있습니다. FortiGate NGFW는 중요한 데이터와 애플리케이션을 분할하는 작업을 통해 보안 클라이언트 소프트웨어 없이 이러한 요소를 보호합니다. 또한, 분할은 악성 익스플로잇이 횡적으로 확산되지 못하게 막고, 보안이 침해된 기기를 신속히 격리하도록 도와줍니다. 게다가 기기에 대한 액세스를 관리하는 기능으로 미국의 국립 표준 기술 연구소(National Institute of Standards and Technology, NIST) 사이버 보안 프레임워크나 유럽 연합의 네트워크 및 정보 시스템(NIS) 지침 등의 규정을 더욱 잘 준수할 수 있게 됩니다.

개방적 보안 플랫폼을 통해 여러 가지 기존 솔루션 통합

Fortinet 보안 패브릭에는 보안 패브릭을 지원하는 파트너 70개 이상에 제공되는 애플리케이션 프로그래밍 인터페이스(API) 연결 기능이 사전 구축되어 있습니다. 따라서 모든 보안 패브릭 요소에서 여러 가지 타사 솔루션과 완벽하게 통합할 수 있습니다.[7]

그뿐만 아니라 패브릭 지원 파트너 에코시스템에 포함되지 않는 보안 제품의 경우, REST API 및 DevOps 스크립트를 통해 보안 패브릭에 간편하고 신속하게 추가할 수 있고, 원격 측정 정보를 공유하고, 보안 프로비저닝, 구성, 대응을 자동화하는 기능 등이 제공됩니다.

OT 프로토콜	
BACnet	MMS
DNP3	Modbus
Elcom	OPC
EtherCAT	PROFINET
EtherNet/IP	S7
HART	SafetyNET
IEC 60870-5-104	Synchrophasor
IEC 60870-6 (TASE.2)/ICCP	
IEC 61850	
LonTalk	

OT 애플리케이션 및 벤더		
7-Technologies/ Schneider Electric	Honeywell	RealFlex
ABB	ICONICS	Rockwell Automation
Advantech	InduSoft	RSLogix
Broadwin	Intellicom	Siemens
CitectSCADA	Measuresoft	Sunway
CODESYS	MicroSys	TeeChart
Cogent	Moxa	VxWorks
DATAC	PcVue	Wellintech
Eaton	Progea	Yokogawa
GE	QNX	

표 1: FortiGuard Industrial Security Services.

보안 패브릭은 연결성을 단순화하기 위해 다양한 벤더의 스위치와 무선 AP와 상호작용하고 이를 제어하는 기능이 있습니다. Cisco, HP, Ruckus 등의 170개 이상 벤더에서 제공하는 2,000여 종의 모델이 포함됩니다.[8] 대부분의 경우, 이를 통해 조직의 보안 태세를 강화하고 관리에 걸리는 시간을 절약할 수 있습니다. 또한, 기기 업그레이드나 교체 시기를 늦출 수 있어 기존 투자에 대한 보호도 제공합니다.

자동화된 침입 방지, 탐지 및 사고 대응 프로세스

Fortinet 보안 패브릭의 여러 가지 요소는 서로 함께 작동합니다. 예를 들어, 방화벽, 이메일, 엔드포인트 보안, 샌드박스, 스위치, 무선 AP 등이 멀웨어를 자동 탐지하거나, 위협 예방을 위한 시그니처를 생성하여 공유하거나, 위협을 격리하거나, 알림을 전송합니다. 오늘날의 위협은 인공지능과 머신 러닝에 힘입어 기계의 속도로 발전하기 때문에 보안 솔루션도 그에 맞는 속도로 발전해야 위협을 막을 수 있습니다.

보안 패브릭은 위협이 탐지되면 정책 기반 이벤트 트리거, 대응 조치, 승인을 결합한 워크플로를 자동화해서 위협을 신속히 차단합니다. 보안 사고는 정보 기술 서비스 관리(ITSM) 솔루션에 자동으로 전달될 수 있습니다. 보안 분석 전문가는 중앙에서 자동으로 구현할 수 있는 대응 카탈로그를 선택할 수 있습니다. 이러한 기능을 내장한 덕분에 대응 시간이 며칠에서 몇 시간으로 단축되었고, 한정적인 보안 인력이 모니터링과 정보 라우팅보다는 전문적인 의사 결정에 집중할 수 있게 되었습니다.[9]

자동화된 규정 준수 및 감사 추적, 보고

일반적으로 감사를 준비할 때는 다양한 보안 솔루션에서 데이터를 수집해서 이를 수작업으로 보정하고 분석했습니다. 이 작업은 힘들 뿐만 아니라, 보안팀의 여러 인원이 더욱 중요한 작업을 하지 못하게 방해하는 경우가 많습니다. FortiManager와 FortiAnalyzer는 업계 규정 및 보안 표준에서 요구하는 규정 준수 추적과 보고를 자동화해서 귀중한 인력의 시간을 절약해줍니다.

보안 패브릭은 며칠, 심하면 몇 주까지 걸리던 대응 시간을 몇 분 이내로 단축합니다.

보안 평가 서비스는 전체적인 보안 태세와 복구 업데이트가 필요한 특정 영역을 평가하여 종합한 점수를 제공합니다.

고급 규정 준수 기능에는 사전 구축되어 쉽게 예약하고 바로 사용할 수 있는 보고서 수백 개가 있고 보고서 맞춤 설정을 위한 차트 400개, 템플릿 35개 이상이 준비되어 있습니다. 또한, FortiAnalyzer는 보안 작업에 자동화된 심층 분석을 제공해 공격면에서 위험 범위를 파악한 다음, 즉각적으로 필요한 영역을 찾아냅니다. 또한, 이 기능은 Fortinet 보안 평가 서비스에 알림을 제공합니다. Fortinet 보안 평가 서비스는 조직의 전체적인 보안 태세를 동종 업계 조직 및 널리 인정되는 보안 표준과 비교해 한눈에 볼 수 있는 대시보드를 제공합니다. FortiGate Enterprise 번들[10] 및 360 번들 구독 서비스[11]에 포함된 Fortinet 보안 평가 서비스를 사용하면 경영진과 이사진에게 쉽게 알아볼 수 있는 형식으로 간략한 트렌드를 제공할 수 있습니다(그림 2 참조).[12]

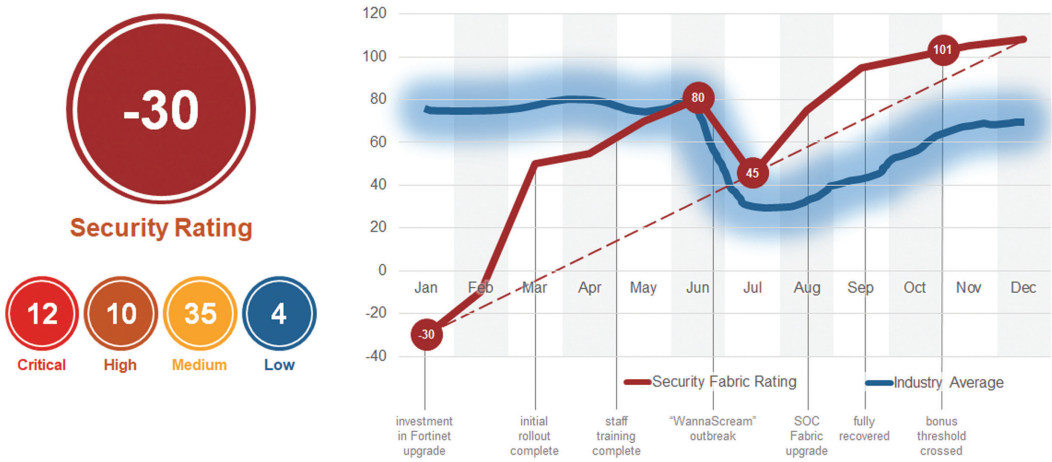

그림 2: Fortinet 보안 평가 서비스 Fortinet 보안 평가 서비스를 사용하여
자사 환경의 보안 태세를 특정 시점에서 추적하고 추세를 분석해 업계 평균과 비교합니다.

사이버 보안 통합을 통해 복잡성과 위험 최소화

Fortinet 보안 패브릭을 사용하면 OT 및 IT 사이버 보안에 OT 네트워크의 고유한 문제를 해결할 방법을 통합할 수 있습니다. 통합 OS와 개방형 API 중심적 아키텍처, 단일 창 관리에 기초한 보안 패브릭을 사용하면 중요한 위협 인텔리전스를 더욱 효과적으로 수집하여 관계성을 파악하고, 공유 및 대응할 수 있습니다. 이러한 보안 방식은 보안팀의 효율성을 향상하면서도 위험을 낮추는 효과가 있습니다.

또한, 보안 요소가 하나의 통합적인 에코시스템으로 작동할 경우, 각 조직은 네트워크상 어디서나 보안이 침해된 기기를 즉시 찾아내어 분리하고, 복구 업데이트할 수 있으며 멀웨어를 자동으로 찾아서 제거하고, OT, IT, IoT 기기, 클라우드에 이르기까지 어디서나 보안 정책 업데이트를 오케스트레이션 할 수 있습니다. 그와 동시에 복잡성이 감소하고 보안과 규제 준수 능력은 강화됩니다. OT 조직이 IoT 센서, AI, ML, 빅데이터 등의 디지털 혁신을 받아들이게 되면서 이러한 자산을 보호해야 할 필요성이 생겼기 때문에 이러한 요소가 중요합니다.

1 Carl M. Hurd and Michael V. McCarty, "A Survey of Security Tools for the Industrial Control System Environment," Idaho National Laboratory, U.S. Department of Energy, 2017년 6월 12일.
2 "FortiGuard Labs," Fortinet, 2019년 3월 22일
3 Zeus Kerravala, "How to Enable Digital Transformation and Improve ROI with Fortinet Security Fabric," ZK Research, 2018년 2월.
4 "Industrial Control Systems," Fortinet, 2019년 3월 25일
5 "Comprehensive Security with the FortiGate Enterprise Protection Bundle," Fortinet, 2019년 1월 21일.
6 "360 보호 번들: Delivering Real-Time Network Management, Comprehensive Security and Operational Services, and Advanced Support," Fortinet, 2019년 3월 26일
7 "Technology Alliances," 2019년 4월 21일
8 "FortiNAC: Network Access Control," Fortinet, 2019년 4월 27일.
9 "Purpose-built Integrated NOC-SOC Management and Analytics," Fortinet, 2018년 9월 11일.
10 "Comprehensive Security with the FortiGate Enterprise Protection Bundle," Fortinet, 2019년 1월 21일.
11 "360 보호 번들: Delivering Real-Time Network Management, Comprehensive Security and Operational Services, and Advanced Support," Fortinet, 2019년 3월 26일.
12 "Proactive, Actionable Risk Management with the Fortinet Security Rating Service," Fortinet, 2019년 4월 5일.

2019년 6월 5일 수요일, 오후 3:34 AM
392073-0-0-EN
D:₩Fortinet₩Work₩2019₩June₩060519₩Task 2₩sb-plant-operations-ot-security-selection-complexity