솔루션 브리프

위협 탐지, 조사 및 대응의 완전 자동화 - FortiXDR

종합 요약

여러 해 동안, 기업들은 새로운 사이버 보안 위협에 대항하기 위해 새로운 사이버 보안 제품을 추가해 왔습니다. 사이버 보안 제품은 대개 개별적으로는 효과적이지만, 전체적으로 너무 많아짐에 따라 이를 관리, 모니터링, 처리해야 하는 보안 팀이 과중한 업무에 시달리고 있습니다. 따라서 기업은 틈새로 빠져나가거나 노이즈 속에 숨어 있는 잠재적 사이버 공격에 노출될 위험이 커집니다. 오늘날, 대부분의 기업은 보안 및 운영 효율성을 개선하기 위해 공급업체 통합을 시도하고 있거나 시도할 계획을 수립하고 있습니다. 그러나 성공적인 결과를 얻기 위해서는 통합이 단지 단일 공급업체의 독립형 제품을 모아 놓는 것에 그치는 것이 아니라 통합되고 효과적이며 효율적인 전체 보안 솔루션으로 이어져야 합니다. FortiXDR은 완전히 자동화된 위협 탐지, 조사 및 대응을 통해 방대하고 통합되고 자동화된 포티넷 보안 패브릭을 구축할 수 있게 도와줍니다. 덕분에 기업은 보안 태세 및 운영 효율성을 향상함으로써 보안 팀의 부담을 덜어줄 수 있습니다.

확장된 탐지 및 대응(XDR) 기반의 통합

Gartner에 따르면 80%의 기업들이 현재 또는 향후 2~3년 내에 보안 공급업체를 통합할 계획이라고 합니다.[1] 많은 기업은 조달 편의를 기준으로 통합(제품군 또는 엔터프라이즈 라이선스 구매를 통해)하는 것보다는 XDR과 같은 보안 아키텍처를 기준으로 통합하기를 선호합니다. FortiXDR은 포티넷 보안 패브릭을 XDR 솔루션으로 변환합니다. 기업 전체에 배포된 광범위한 포티넷 보안 컨트롤이 중앙 집중식 표준화 레이어에 정보를 제공합니다. 여기서부터, 잠재적인 고위험 인시던트를 탐지하고 조사/분류를 시작할 수 있도록 분석이 적용됩니다. 마지막으로, 적절한 수정 및 대응을 처리하기 위해 대응 작업을 미리 정의할 수 있습니다. 이 프로세스는 완전히 자동화되어 수많은 알림 사이에서 놓칠 수 있는 공격을 탐지하고 완화함으로써 보안 직원의 부담을 덜어줍니다.

광범위한 보안 컨트롤

포티넷 보안 패브릭은 다음을 포함하는 전체 디지털 기업을 다룹니다.

- **엔드포인트 및 사용자** - 엔드포인트 보호(EPP)와 ID 및 액세스 관리(IAM)를 통해
- **네트워크 및 액세스 계층** - 유선 스위치, 무선 액세스 포인트, 엔터프라이즈 방화벽을 통해
- **클라우드** - 클라우드 액세스 보안 브로커(CASB), 웹 애플리케이션 방화벽(WAF), 보안 이메일 게이트웨이(SEG)를 통해.

모든 제품이 통합되어 단일 중앙 분석 플랫폼으로 텔레메트리를 전송합니다.

탐지 분석

잠재적 사이버 공격의 조기 지표를 식별하도록 설계된 고급 분석 세트가 점점 확장되고 있습니다. 이 분석 세트는 FortiGuard Labs 전문가들이 개발한 것이며, 중앙 집중식이고 표준화되었으며 상관관계가 있는 텔레메트리에 적용됩니다. 이러한 탐지는 인시던트 조사의 다음 단계를 시작합니다.

인공 지능(AI) 기반 조사

초기 탐지 유형에 따라 자동 조사 프로세스가 진행되고, 뒤이어 곧바로 AI 기반 결정 엔진이 조사하면서 기존의 보안 분석가가 통상적으로 취할 전문적 조치를 그대로 모방합니다. 이 엔진은 보강과 추가적 분석을 제공하는 다양한 서비스를 호출할 수 있습니다. 대표적인 예로는 FortiGuard Labs와 타사의 위협 인텔리전스, 파일 분석(예: 통계적 Yara 규칙), 동적 샌드박스 평가, 커뮤니티 평판, 사용자 행동 기준을 들 수 있습니다. 하지만 최종 분류로 이어지는 더 많은 것들이 있습니다.

사전 정의된 대응 프레임워크

기업은 분류, 사용자 그룹, 위험 노출 등의 기준에 따라 취할 조치를 미리 지정하는 정책을 설정할 수 있습니다. 그러면 궁극적인 문제 해결 및 대응 속도가 빨라집니다.

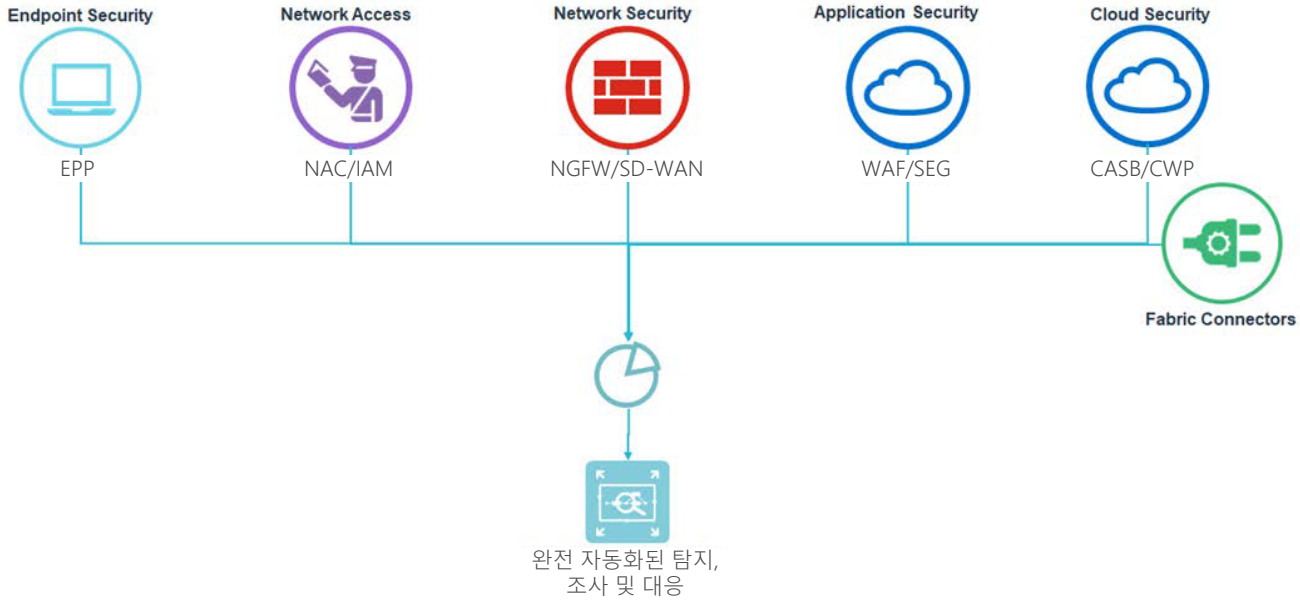

그림 1: FortiXDR 및 포티넷 보안 패브릭.

FortiXDR 차이

XDR은 업계에서 초기 단계 개념이며 핫 이슈입니다. 그러나 기존의 보안 패브릭 비전과 완벽하게 조화를 이루며 여러 가지 자연스러운 장점을 솔루션에 제공합니다. 폭넓은 범위, 개별 구성 요소의 효과, 자동화 수준 등이 장점입니다. 따라서 기업들이 공급업체 통합의 이점을 실현할 가능성이 더 높습니다.

평균적으로, FortiXDR은 추가적인 조사 및 대응을 위해 100개의 high-value 개별 알림을 10개의 high-fi 인시던트 탐지로 변환합니다.

폭넓은 범위

XDR 솔루션을 더 넓게 "확장"할수록 더 많은 정보를 분석, 강화하고 궁극적으로 분류에 사용할 수 있습니다. FortiXDR은 네트워크 및 엔드포인트 구성 요소는 기본이며 액세스, 이메일, 웹 애플리케이션 및 클라우드도 다룰 수 있어 차별화됩니다. 마찬가지로, 사이버 공격 전달의 중요한 중간 사이버 킬 체인 단계에 분석을 적용하는 동안에는 익스플로잇, 설치 및 통신이 중요합니다. 초반에 그리고 후반에 텔레메트리를 확장함으로써 전체 사이버 킬 체인을 다룰 수 있다는 것은 상당한 장점입니다. 물론 위장 기술로부터 얻은 통찰력은 정찰 탐지에 도움이 되며, 에이전트 기반 사용자 및 엔터티 동작 분석(UEBA)에 의한 후반 단계 데이터 모니터링을 통해 보완됩니다.

구성 요소의 효과

기업들은 공급업체를 통합하기 위해 포티넷 보안 컨트롤 및 XDR을 구축하는 것이 표준 이하의 성과로 이어질까 걱정할 필요가 없습니다. FortiXDR에 포함된 모든 포티넷 보안 제품은 독립 테스트에서 계속 높은 점수를 받고 있습니다. 이들은 AV-Comparatives, ICSA Labs, NSS Labs, Virus Bulletin 등 제3자가 실시한 테스트에서 업계 최고의 성능을 보여줍니다. 실제로, 포티넷 포트폴리오는 업계에서 독립업체로부터 가장 많은 인증을 받았습니다.

자동화 수준

기업에 큰 피해를 입힐 수 있는 눈에 띄지 않는 위협을 탐지하는 것이 매우 중요합니다. 그러나 알림이 늘어나는 것은 대부분의 보안 팀에서 가장 원치 않는 일입니다. 일부 공급업체는 더 많은 보안 정보를 한 곳에 상호 연결하여 더욱 보기 좋게 제공하는 방식을 취했지만, 포티넷은 그보다 한발 더 나아갑니다. FortiXDR을 사용하면 데이터 표준화/상관관계 및 탐지 분석뿐 아니라 인시던트 조사, 분류 및 수정 프로세스까지 완벽하게 자동화할 수 있습니다. 따라서 사이버 보안 태세를 강화하는 한편 보안 팀의 업무를 늘리는 것이 아니라 덜어줍니다.

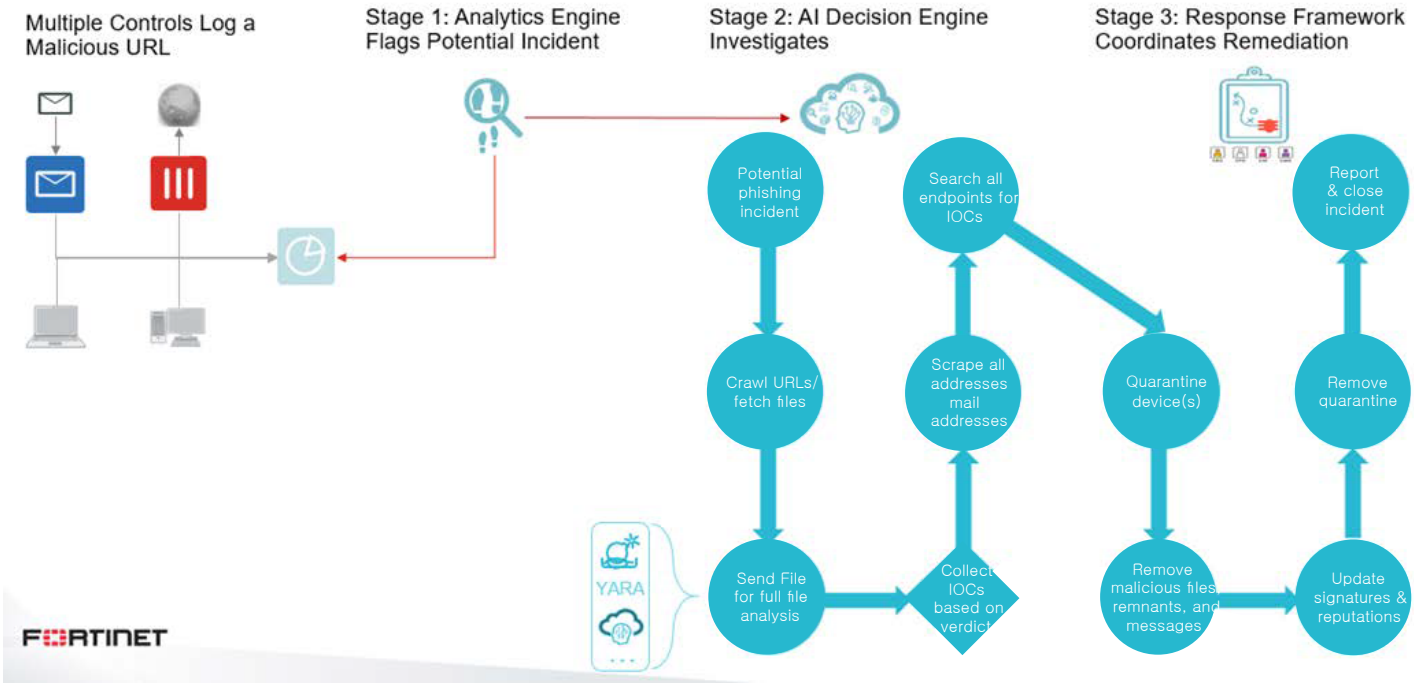

그림 2: 피싱 탐지, 조사 및 대응.

FortiXDR로 보안 태세 및 운영 효율성 향상

오늘날 위협 동향의 횟수, 지능화 수준, 속도가 높아지고 있어 보안 팀은 사이버 보안 인력과 기술 공급이 부족한 시기에 그 어느 때보다 힘든 어려움에 처했습니다. 관리해야 할 개별 보안 제품, 분석할 보안 정보, 조사해야 할 잠재적 인시던트가 너무 많아지면서 엔터프라이즈 보안에 접근하는 방식에 근본적인 변화가 필요합니다. 이것이 바로 많은 기업이 공급업체 통합을 추진하고 있는 이유이며, XDR과 같은 새로운 솔루션이 매우 유망한 이유입니다. FortiXDR은 탐지, 조사, 대응을 완전히 자동화하는 독특한 방식을 취합니다. 현재 진행 중인 사이버 공격을 찾아낼 가능성도 커집니다(데이터 침해나 랜섬웨어 인시던트가 일어나기 전에). 또한 보안 관제팀의 부담을 덜어주고 보다 가치 있는 전략적 활동에 힘을 쏟을 수 있게 해줍니다.

[1] John Watts and Peter Firstbrook, "Security Vendor Consolidation Trends: Should You Pursue a Consolidation Strategy?" Gartner, 2020년 7월 30일.

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

859551-0-0-KO