1. 네트워크 보안

대부분의 공격은 네트워크를 통해 발생하며, 네트워크 보안 솔루션은 이러한 공격을 식별하고 차단하도록 설계되었습니다. 이러한 솔루션에는 데이터 손실 방지(DLP), IAM(Identity Access Management), NAC(Network Access Control) 및 차세대 방화벽(NGFW) 애플리케이션 제어와 같은 데이터 및 액세스 제어가 포함되어 안전한 웹 사용 정책을 시행합니다.

첨단·다층 네트워크 위협 방지 기술로는 IPS(Intrusion Prevention System), 차세대 안티바이러스(NGAV), 샌드박스링(Sandboxing), CDR(Content Unrarm and Reconstruction) 등이 있다. 또한 네트워크 분석, 위협 헌팅 및 자동화된 보안 조정 및 대응 기술도 중요합니다.

2. 엔드포인트 보안

제로 트러스트 보안 모델은 데이터가 어디에 있든 데이터를 중심으로 마이크로 세그먼트를 생성하도록 규정합니다. 모바일 인력으로 이를 실현하는 한 가지 방법은 엔드포인트 보안을 사용하는 것입니다. 엔드포인트 보안을 통해 기업은 데이터 및 네트워크 보안 제어 기능이 있는 데스크톱 및 랩톱과 같은 최종 사용자 장치, 피싱 방지 및 안티랜섬웨어와 같은 고급 위협 방지, EDR(Endpoint Detection and Response) 솔루션과 같은 포렌식을 제공하는 기술을 안전하게 보호할 수 있습니다.

3. 모바일 보안

태블릿과 스마트폰과 같은 모바일 기기는 기업 데이터에 액세스할 수 있어 기업이 악의적인 앱, 제로데이, 피싱, 메신저(IM) 공격 등의 위협에 노출되는 경우가 많습니다. 모바일 보안은 이러한 공

격을 방지하고 운영 체제 및 장치가 뿌리를 내리고 탈옥하는 것을 방지합니다. MDM(Mobile Device Management) 솔루션에 포함된 경우, 이를 통해 기업은 규정을 준수하는 모바일 장치만 기업 자산에 액세스할 수 있습니다.

4. IoT 보안

사물인터넷(IoT) 장치를 사용하면 생산성 이점을 얻을 수 있지만 조직을 새로운 사이버 위협에 노출시킬 수도 있습니다. 위협 행위자들은 기업 네트워크로의 경로나 글로벌 봇 네트워크의 다른 봇과 같은 악의적인 용도로 인터넷에 무심코 연결된 취약한 장치를 찾는다.

IoT 보안은 연결된 장치의 검색 및 분류, 네트워크 활동을 제어하기 위한 자동 세분화, 취약한 IoT 장치에 대한 악용을 방지하기 위한 가상 패치로 IPS를 사용하여 이러한 장치를 보호합니다. 경우에 따라 장치의 펌웨어를 소규모 에이전트로 확장하여 악용 및 런타임 공격을 방지할 수도 있습니다.

5. 애플리케이션 보안

인터넷에 직접 연결된 다른 모든 것과 마찬가지로 웹 애플리케이션은 위협 행위자들의 대상이다. 2007년부터 OWASP는 인젝션, 인증 끊김, 잘못된 구성, 사이트 간 스크립팅과 같은 중요한 웹 애플리케이션 보안 결함에 대한 상위 10개 위협을 추적해 왔다.

애플리케이션 보안을 통해 OWASP 상위 10개 공격을 중지할 수 있습니다. 애플리케이션 보안은 또한 봇 공격을 방지하고 애플리케이션 및 API와의 악의적인 상호 작용을 차단합니다. 지속적인 학습을 통해 데브옵스가 새로운 콘텐츠를 출시하더라도 앱은

계속 보호될 것이다.