S 리포트 | APT 보안-3부

‘엔드포인트’ 중요성 부각, ‘차세대 솔루션 관심 증폭

[디지털데일리 이유지기자]

사이버 위협은 지속적으로 변화한다. 더구나 기업의 업무 환경은 모바일, 클라우드 확산으로 하이브리드 형태로 더욱 복잡해지고 있다. 기업에서 제어하고 보호해야 할 자산과 데이터는 점점 더 많아지고 복잡해졌을 뿐만 아니라 여기저기 산발적으로 흩어지고 있는 것이다.

이같은 기업 IT자원의 ‘복잡화’는 지능화된 사이버위협에 대한 대응을 더욱 어렵게 만드는 요소로 꼽힌다. 방어자. 즉 기업이나 공공기관, 금융회사들은 모바일 기기에서부터 데이터센터 IT 인프라까지 보호해야 할 대상이 너무 많다. 반면 공격자 입장에선 여러 채널중 취약한 엔드포인트 하나만 파고들면 된다. 엔드포인트 솔루션에서 일단 중요한 보안대응 전략의 해법을 찾아야하는 이유다.

지난 2월, 미국 샌프란시스코에서 개최됐던 세계 최대 연례 보안 컨퍼런스인 ‘RSA2016’에서

기조연설자로 나온 보안전문가들은 이같은 '복잡성'을 해소하고 동시에 보안효과를 높이는 기술적 지향점을 집중적으로 제기해 주목을 끌었다.

마틴 로쉬 시스코 부사장(보안사업담당)은 효과적인 보안의 3요소로 '인티그레이션(Integration), 콘솔리데이션(Consolidation), 자동화(Automation)'를 제시했다. 고성능의 확장성 있는 플랫폼을 활용해 '간소화(Simplicity at Scale)'된 환경을 구현해야 한다는 주장이다. 그는 현재 기업의 보안 관리와 분석 측면의 복잡성이 크게 증가하면서 보안 제품을 많이 구비했음에도 보안 역량은 오히려 약화되고 있다는 진단에 따른 해결책이다.

로쉬 부사장은 "조직들이 너무 많은 보안 제품을 구축하고 있다. 이로 인해 많은 인력이 이를 관리하고 쌓이는 데이터를 분석하느라 오히려 공격에 대한 방어능력을 약화시킨다"며 "결국 보안에 악영향을 미치고 있는 것이 현실"이라고 지적했다. 그는 이같은 상황을 그래프로 나타내면서 "기업의 복잡성은 기하급수적으로 급등하지만 보안 솔루션의 능력은 수평을 이루는 모습이 된다"며 "위협이 발생할 때마다 새로운 보안 제품을 단순히 추가 구매해 문제를 해결하려는 접근방식은 잘못됐으며, 복잡성만 증가시키는 것"이라고 단언했다.

〈그림〉시스템의 복잡성과 보안대응의 효과

이를 위해 제품 간 통합, 중앙집중식 관리, 고성능의 서비스 플랫폼으로 보안 제품의 수를 줄일 수 있는 '인티그레이션'과 '콘솔리데이션', 관리 · 분석 '자동화'로 이같은 문제를 해결할 수 있다는 주장이다.

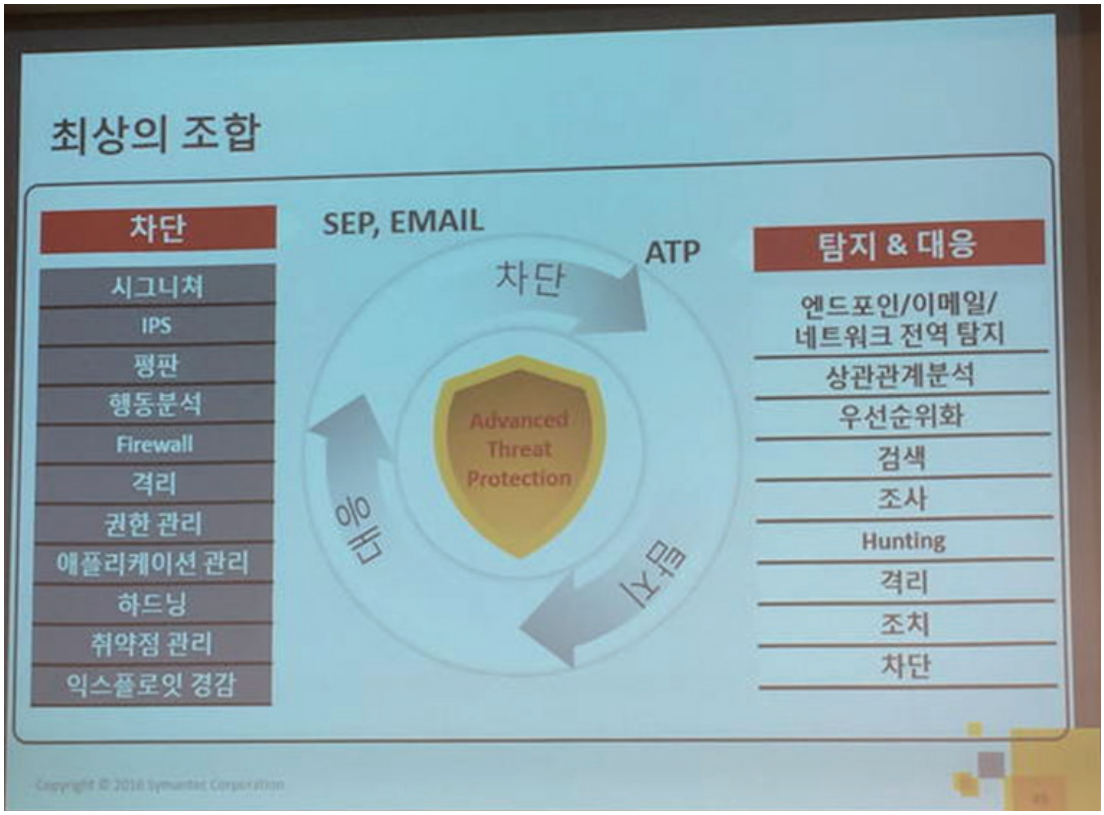
팻 겔싱어 VM웨어 CEO도 IT보안의 복잡성으로 인한 문제 해결방안으로 '가상화'를 핵심으로한 공통의 조직화된 프레임워크를 활용할 것을 제시했다. 가상화가 인프라에 보안을 내장시킬 수 있는 포괄적인 아키텍처를 만들어낼

수 있다는 것이다.

마크 맥로린 팔로알토네트웍스 CEO는 정교화돼 있고 자동화돼 있는 사이버공격자들과 싸우기 위한 새로운 보안 패러다임으로 '예방(Prevention) 중심의 차세대 플랫폼' 을 내세웠다. 기존의 수동적(manual)이고 반응적(reactive)인 방식이 아니다. 그는 "고도로 오케스트레이트 돼 있고 커뮤니케이션을 수행하며 자동화돼 있어야 한다"며 특히 "위협을 서로 공유해 알려지지 않은 위협을 알려진 위협으로 매우 빠르게 전환하고, 해당 위협정보를 자동으로 공유해 각자 네트워크에 적용하는 조치가 이뤄져야 한다"고 강조했다.

엔드포인트솔루션 중요성 더욱 부각

보안기술이 아무리 발달됐다고 는 하 지 만 공격자가 방어자보다 더 유리한 위치에 있을 수 밖에 없다. 시스템의 복잡성의 증가로 인해 방어자들은 '비대칭적인(asmmetric) 싸움'을 벌이고 있는 상황인데, 이런 점에서 엔드포인트 솔루션에 대한 중요성은 더욱 강조되고 있다. 실제로도 최근 보안 솔루션 업계에서 두드러진 흐름 가운데 하나는 엔드포인트 중요성이 재부각되고 있다.



초창기에 선보였던 지능형지속위협(APT) 보안 솔루션은 주로 네트워크단 보호에 초점을 맞췄다. 공격자들은 APT 탐지에서 효과를 발휘한 가상화 기반 '샌드박스'를 우회할만큼 발빠르게 움직이고 있다. APT 솔루션에 대한 수요와 공급은 지난 2012년부터 나오긴 했으나, 고객들이 실제 도입을 시작한 단계는 2014년부터로 분석된다.

결국 각종 보안시스템을 뚫고 사내에 침투하는 정교한 사이버위협으로 인한 피해를 막기위해서는 악성코드가 설치되는 엔드포인트단에서 위협을 탐지하고 분석하는 것이 효과적이라는 게 업계의 시각이다. 공격자 침입을 완벽하게 방어할 수 없다는 것을 인정하고 조직 내부에 잠입한 지능형 위협을 신속하게 탐지해 대응하자는 보안 패러다임이 대세가 되고 있다.

올해들어서도 많은 보안업체들은 엔드포인트단에서 정교한 공격을 신속하게 탐지 · 대응하는 솔루션을 속속 선보이고 있다.

이에따라 앞서 언급한 'RSA컨퍼런스2016'에서도 위협 분석 · 인텔리전스 솔루션과 더불어 엔드포인트 탐지 · 대응((Endpoint Detection and Response, EDR) 솔루션이 두드러졌다. EDR은 오랜 기간 안티바이러스가 입지를 구축해온 엔드포인트 보안 분야의 차세대 솔루션으로 인식되고 있다.

차세대 엔드포인트 제품군은 악성코드가 설치되는 엔드포인트단에서 비정상 행위를 분석해 알려지지 않은 위협을 탐지하고 침해흔적을 찾아낸다. 이후 피해 확산을 빠르게 막을 수 있도록 격리하거나 조치해 대응하는데 집중한다.

카본블랙을 비롯해 이미 많은 차세대 엔드포인트 보안 전문 신생업체들이 등장했다. EMC RSA, 파이어아이, 체크포인트 등 유명 보안업체들이 새롭게 선보인 엔드포인트 보안 솔루션도 대부분 EDR 기능을 제공하고 있다.

엔드포인트 보안 강자인 시만텍 역시 엔드포인트와 이메일 게이트웨이, 네트워크 영역까지 포괄하는 통합대응형 '지능형위협보호(ATP)' 솔루션을 지난해 말 선보인 후 EDR 기능을 집중 부각하고 있다.

시만텍은 "보안업계는 최근 정교한 악성코드를 엔드포인트 단에서 쉽고 빠르게 탐지 및 대응할 수 있는 역량을 제공하기 위해 노력을 기울이고 있다"며 "가히 '엔드포인트 르네상스(Endpoint Renaissance)' 시대가 열렸다고 할 수 있으며, ATP 솔루션의 해법은 엔드포인트가 좌우한다"고 강조하고 있다.

〈이유지 기자〉yjlee@ddaily.co.kr