아이뉴스24

EDR 보안기업, XDR로 보폭 넓힌다 [IT돋보기]

입력 2022.06.20. 오전 9:42

국내는 아직 걸음마 단계…"EDR 시장 규모부터 확대돼야"

디지털 전환 가속화로 보안의 경계가 흐려지면서 '다계층 위협 탐지·대응(XDR)' 솔루션이 부상하고 있다. XDR은 '엔드포인트 위협 탐지·대응(EDR)'을 확장·통합한 개념이다. 글로벌 기업들은 XDR 사업 확장에 본격 나서고 있지만 국내에서는 EDR 시장 규모부터 늘려야 한다는 분석이 나온다.

디지털 전환 가속화로 '다계층 위협 탐지·대응(XDR)' 솔루션이 부상하고 있다. [사진=조은수 기자]

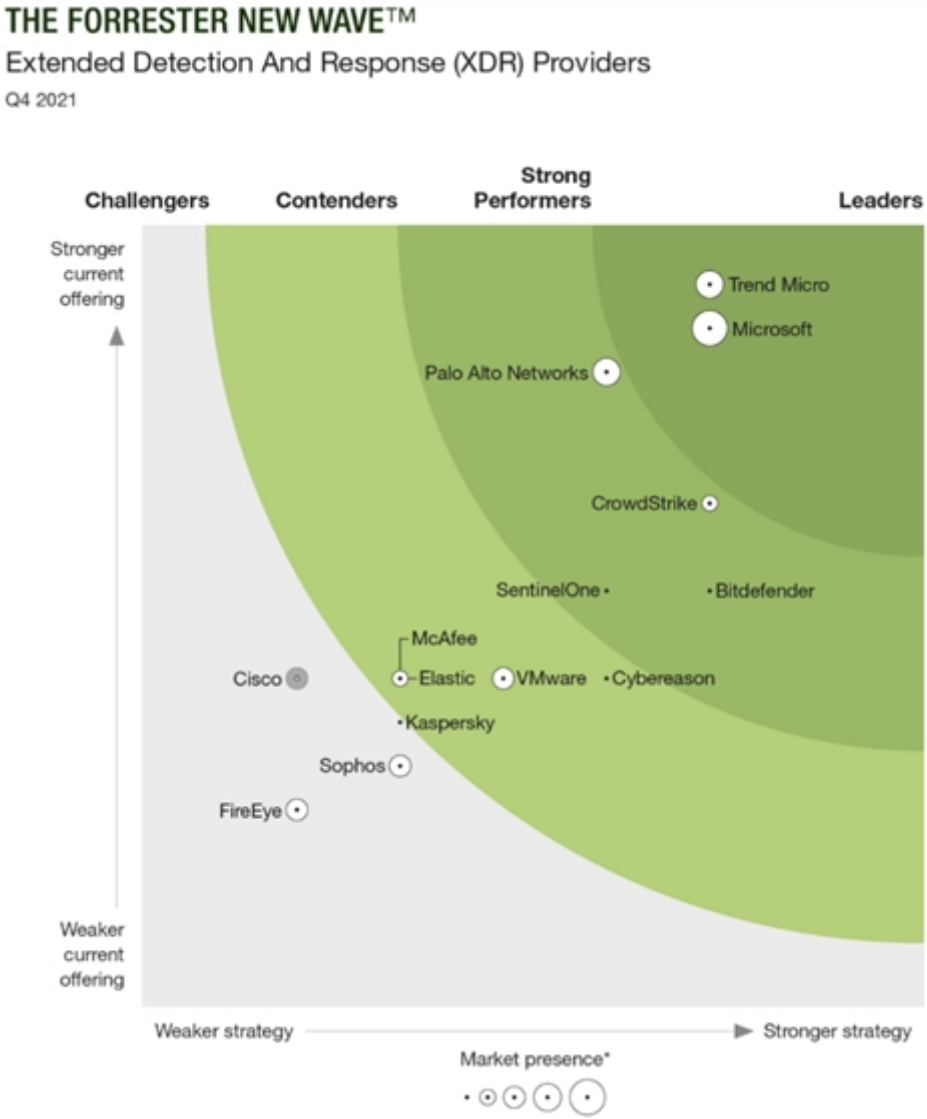
20일 보안업계에 따르면 올해 RSA 컨퍼런스에서 글로벌 EDR·통합보안관제(SIEM) 업체들은 XDR 전환을 강조했다. 크라우드스트라이크(CrowdStrike)는 '팔콘(Falcon) XDR'에 신규 기능을 도입했으며, '크라우드 XDR 얼라이언스(Alliance)' 회원사를 늘리면서 자사 솔루션의 개방성을 확대하고 있다. 현재 구글 클라우드

와 옥타(Okta), 서비스나우(ServiceNow) 등이 가입돼 있다. RSA는 기존 SIEM과 네트워크 분석, 엔드포인트 등을 '넷위트니스(NetWitness) XDR'로 통합해 공개했다.

XDR은 정보 수집의 대상을 엔드포인트를 비롯해 클라우드, 네트워크까지 확장한 개념이다. 다양한 환경에서 수집한 데이터를 분석해 기업이 통합적인 측면에서 위협을 탐지·대응할 수 있도록 돕는다. 가트너(Gartner)는 '여러 보안 제품의 데이터를 자동으로 수집하고 상호 연결하는 탐지·대응 플랫폼'으로 정의한 바 있다.

XDR이 대두된 배경은 '제로 트러스트(Zero-Trust)' 보안 패러다임, 클라우드 보안 등의 중요성이 커지면서 기존 보안관제의 한계점을 보완하기 위해서다. 위협 탐지 범위를 확대하고 대응 수준을 고도화한다는 전략이다.

EDR 제공업체들은 기존 SIEM 기반 보안관제에 네트워크 트래픽, 엔드포인트 심층 분석 기능을 추가한 XDR 솔루션을 출시하고 있다. 포레스터(Forrester) 보고서에 따르면 지난해 4분기 기준 14개의 글로벌 기업이 XDR 사업에서 선두를 달리고 있거나 관련 솔루션을 출시한 상태다.



글로벌 XDR 공급업체 현황. [사진=포레스터 보고서 발췌]

해외에서는 XDR 주도권을 둘러싼 각축전이 벌어지고 있지만 국내에서는 아직 걸음마 수준이다. 한 국내 보안업계 관계자는 "국내에서도 EDR 기업을 중심으로 안티바이러스, 네크워크 접근제어(NAC) 등 주력 분야를 강화해 XDR로 확대하겠다는 움직임은 감지되고 있다"며 "다만 아직까지 기업 고객들이 EDR 도입에 부담을 느끼고 있어 EDR 시장 규모 자체도 크지 않은 상황"이라고 전했다.

또 다른 업계 관계자는 "올해 RSA에서 부각된 XDR은 단순히 EDR을 확장한 개념이 아닌 네트워크와 클라우드 등 모든 보안 위협에 대응하는 통합 솔루션이라는 개념으로 강조된 것"이라며 "국내에서는 EDR 시장 규모부터 커져야 하는데 내년 상반기쯤 어느 정도 확대될 것으로 보고 있다"고 말했다.

김혜경 기자 hkmind9000@inews24.com

이 기사 주소 https://n.news.naver.com/mnews/article/031/0000679850