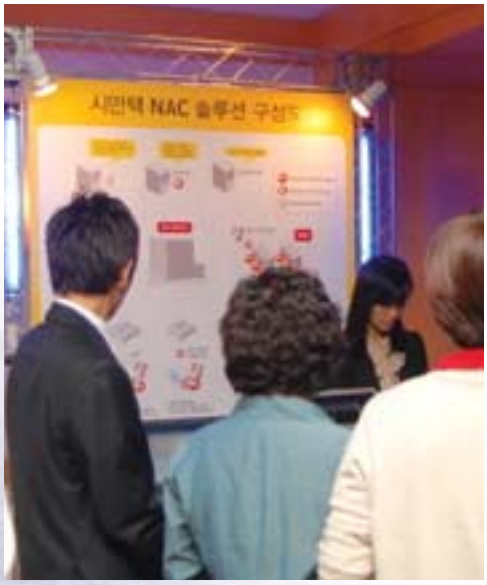
이제는 '포스트 ESM'의 시대
(통합보안관리)

NAC · RMS 등 차세대 통합보안관리 기술에 관심 집중



지난 9월 6일 열린 차세대 보안세미나인 'NES 2007'에서 참석자들이 전시된 다양한 통합보안관리 신제품을 관심있게 살펴보고 있다.

차세대 통합보안관리(ESM: Enterprise Security Management) 기술로 꼽히는 네트워크접근제어(NAC), 위험관리시스템(RMS), 통합보안정보관리(SIEM) 솔루션을 도입하려는 움직임이 두드러지고 있다.

꾸준히 확장되고 발전하는 IT환경과 새로운 공격방식에 걸맞게 한층 진보된 보안기술과 새로운 접근방식으로 기업 경쟁력 창출에서 중요한 요소로 부각된 정보보안체계를 구현하기 위한 보안관리 기술 투자에 관심을 나타내고 있는 것이다.

대부분 기존의 바이러스 · 웜 등 외부에서 내부로 유입되는 위협을 차단하기 위해 네트워크 방화벽과 침입방지시스템(IPS), 안티바이러스를 설치하던 수준에서 중요정보 유출을 방지하기 위한 내부보안 대책을 수립하는 방향으로 선회하는 흐름을 보이고 있다.

또 내부 네트워크에 접속하는 사용자를 사전에 검증하고 사내 보안정책을 일괄적으로 적용해 보안수준을 적절히 관리할 수 있는 시스템을 구현하고, IT자산 전체의 취약성과 위험수준을 미리 예상 · 분석하고 대응할 수 있는 방안을 강구하려는 시도도 두드러진다.

이를 구현하기 위한 보안 기술로 'NAC'와 '통합보안/위험관리' 기술이 주목받고 있다.

업계에서는 이러한 '통합보안관리' 관점의 차세대 기술이 각광을 받기 시작한 이유로 "보안전담조직과 기존 솔루션의 현실적인 대응관리 한계점을 보완해 보안사고의 위험을 줄일 수 있는 가장 현실적이고 효과적인 대안이 되기 때문"으로 풀이하고 있다.

보안시장의 화두, NAC

'네트워크접근제어(NAC)' 기술은 네트워크 보안관리의 새로운 패러다임으로 각광 받으며 단숨에 보안시장 화두로 떠올랐다.

'NAC'는 적절한 권한을 가진 사용자가 내부 네트워크에 접근하기 전에 보안정책을 준수했는지 여부를 검사해 네트워크 접속을 통제하는 것이 핵심으로, 몇 년 동안 개념수준에서만 소개돼오다가 작년부터 국내 주요 기업들에 본격적으로 상용화되기 시작했다.

네트워크 장비 업체와 보안 솔루션 업체들은 지난해부터 앞다퉈 NAC 제품과 기술을 선보이면서 경쟁적으로 시장에 진출했다.

지난해까지 NAC 제품을 선보인 10개 업체 외에도 올 들어 컨센트리네트웍스와 포티넷이 NAC 기능이 포함된 네트워킹 · 보안 통합 제품을 각각 출시하면서 NAC 시장 진출을 선언했다.

마이크로소프트(MS), 맥아피, 시만텍, 시스코시스템즈, 쓰리콤/티핑포인트, 유넷시스템, 주니퍼네트웍스, 지니네트웍스, 체크포인트, 트렌드마이크로 등은 이미 지난 2년 동안 제품을 경쟁

적으로 선보이며 활발한 영업을 펼치고 있다.

네트워크 기반 솔루션 업체들은 기업 내부 네트워크를 보호할 수 있는 대책으로, 사용자단 소프트웨어 기반 업체들은 탁월한 엔드포인트 보호 솔루션으로 NAC 제품을 선보였다.

직접 NAC 솔루션을 내놓지는 않지만 다양한 벤더의 NAC 솔루션과 연동하는 안티바이러스, 패치관리시스템(PMS), IPS 등 보안 솔루션 업체들까지 합치면, 이제 국·외산을 막론하고 어지간한 네트워크 장비와 보안 솔루션은 모두 NAC를 지원하는 형태로 확장되는 과정에 있다.

NAC 솔루션은 현재 통합 PC보안 솔루션의 형태로 사용자 PC에 설치돼 동작하는 호스트 기반 제품과 네트워크단의 장비를 이용해 사용자단까지 관리하는 네트워크 기반 제품 형태로 시장에 출시돼 있다.

특히, 최근 등장하는 NAC 신제품은 다양한 사용자 환경을 수용할 수 있는 사용자 인증 및 보안 제품 연동지원 '기능 강화'와 기존 네트워크 장비나 네트워크 보안 솔루션, PC 통합보안 솔루션의 '통합형'이라는 점이 특징이다.

이러한 NAC 기술의 진화와 관련해 박진성 쓰리콤/티핑포인트 이사는 "올 연말이면 하나의 벤더 솔루션으로 기업이 원하는 NAC시스템을 구현할 수 있는 수준에 오를 것"이라면서, "내년에는 시장이 본격화 궤도에 오를 뿐만 아니라 선점 여부가 갈릴 수 있는 시기가 도래할 것"으로 예상했다.

진화하는 NAC 기술, 신제품 출시 경쟁

'자가방어형 네트워크(Self-Defending Network)' 실현을 위한 핵심 보안전략으로 'NAC(네트워크허가통제)' 보안 기술을 선보인 후 현재까지 2단계(Phase 2) 솔루션을 선보인 시스코시스템즈는 올 하반기 중 범용성과 확장성이 강화된 3단계 기술(NAC 3)을 발표한다.

NAC 3는 현재 지원하고 있는 사용자 인증 방식인 802.1X를 사용하지 않은 이른바 'Non-802.1X' 기반의 통합인증을 유·무선 스위치와 라우터단에서 모두 지원할 수 있도록 확장된다는 점이 핵심이다.

시스코의 NAC 2의 핵심은 기존 라우터단 지원에서 나아가 스위치와 무선랜 장비까지 지원이 확대된 데다, 802.1X 사용자 인증을 제공하고 인증 및 정책관리 장비인 ACS(Access Control Server)와 연동되는 보안 솔루션 간의 상호연동을 강화해 자동 업데이트를 제공한다는 점이다. 또 맥아피, 시만텍, 퀄리스 등 취약성 분석 및 감사 기술을 제공하는 솔루션 업체들과 협력해 에이전트가 없는 사용자 단말기(게스트 노트북, 프린터, PDA, IP 전화기)의 위험을 평가할 수 있도록 향상시켰다.

올 연말에 국내 시장에 선보일 NAC 3는 사용자 인터페이스를 모두 한글로 지원하고, 국내 대표적인 PC보안 제품인 안철수연구소의 V3 안티바이러스 외에 스파이웨어(스파이제로)까지 지원, 국내 사용자 환경에 폭넓게 적용할 수

있을 전망이다.

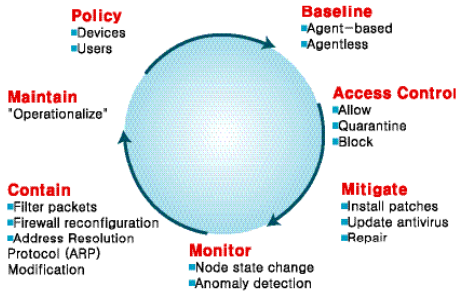
국산 제품으로는 처음으로 802.1X 기반의 무선 네트워크 접속 인증 기반의 NAC 제품을 선보인 유넷시스템도 최근 Non-인증 기반 네트워크 환경에 적용할 수 있는 '애니클릭 NAC 컨트롤러' 신제품을 출시, 다양한 환경에 적용할 수 있는 제품군을 완비한 상태다. 이 회사는 마이크로소프트와도 NAP(네트워크접근보호) 개발 협력을 진행하고 있어, 조만간 '애니클릭 NAP' 신제품을 선보일 예정이다.

주니퍼네트웍스도 지난해 하반기 새롭게 인수한 펑크소프트웨어의 제품을 통합해 유·무선 통합 인증 및 접속제어까지 수행할 수 있는 'UAC(Unified Access Control) 2.0' 신제품을 발표했다. 'UAC 2.0'은 802.1X를 지원하는 L2 스위치와 무선 AP 등으로까지 접속제어 기능이 확장됐으며, L2/3 접속제어 솔루션인 넷스크린 방화벽을 사용하는 고객은 주니퍼의 '인프라넷 콘트롤러'를 추가하는 것만으로 기존 네트워크 환경 변화 없이 구현할 수 있다. 앞으로 IDP(침입탐지/방지) 기능을 제공하는 IDP, ISG 등 방화벽·IDP 통합 제품과 연동 지원을 확대하는 기능을 추가할 예정이다.

쓰리콤/티핑포인트도 올 들어 사전 접속제어뿐만 아니라 네트워크에 사용자가 접속한 이후에도 사용자 트래픽을 지속적으로 점검해 조치할 수 있는 NAC 신제품을 출시했으며, 연말까지 DHCP(Dynamic Host Configuration Protocol) 등 다양한 사용자 인증 환경 확대 지원을 위한 기능을 꾸준히 추가할 예정이다.

시만텍도 10월에 '시만텍 네트워크 액세스콘트롤 11.0' 신제품을 선보인다. 새로운 NAC 제품은 사용자 PC의 상태 확인 및 평가, 네트워크 접근허용 기능뿐만 아니라 보안정책과 컴플라이언스를 준수하도록 보장하는 기능을 구현한다. 특히, 함께 출시할 차기 엔드포인트 통합보안 솔루션인 '시만텍 엔드포인트 프로텍션(SEP) 11.0' 제품에 NAC 제품을 모듈로 통합할 수 있게 해, 강력한 엔드포인트 위협방지 기술을 제공할 수 있도록 할 계획이다.

Gartner NAC 모델



"Gartner's Network Access Control Model", Gartner, Lawrence Orans, 2 August 2005

한편, 최근 국내 시장에 진출해 사업을 본격 개시한 컨센트리네트웍스는 NAC 기능을 통합한 '랜쉴드 스위치' 제품을 출시, 내부 네트워크(LAN)를 보호할 수 있는 '시큐어스위칭' 기술 주도에 나섰다.

컨센트리 측은 '랜쉴드 스위치'가 단일 플랫폼에서 네트워크 접속을 수행하는 L2 스위칭 기능과 함께 NAC, 사용자 기반 보안정책 적용, 레이어 2~7까지 전 계층의 트래픽 분석 및 제어 기능을 모두 제공, 여러 보안 제품이나 서버를 추가하거나 연동하지 않고도 ▲비인가 사용자의 불법적인 네트워크 사용 차단 ▲네트워크에 접속하는 사용자 단말기의 보안수준 관리

▲사용자별 네트워크 사용권한 관리 ▲이상트래픽 관리 · 차단 등 기업 내부 네트워크 보안 관리에서 나서는 문제를 모두 해결할 수 있다고 소개했다.

포티넷도 지난 2월 고성능 스위치와 다중위협 보호, 세분화된 NAC 기능을 모두 제공하는 보안 · 네트워킹 통합 제품인 '포티게이트-224B'를 출시했다.

이 제품은 여러 단일 솔루션을 사용하지 않고서도 내 · 외부의 네트워크 위협으로부터 안전하게 보호해 주며, 네트워크 액세스단에서 내부 보안정책을 강화해 바이러스, 웜, DoS(서비스거부) 공격과 침입 시도, 실시간의 복합적인 보안위협을 차단한다.

특히, 클라이언트리스 방식으로 사용자 접근 제어 기능을 수행해 사용자단에 특정 소프트웨어 에이전트를 설치할 필요 없이 네트워크 정책을 강화하도록 지원하며, 안티바이러스, 방화벽, 가상사설망(VPN), IPS, 안티스팸, 안티스파이웨어, 웹 필터링 등 8개의 주요 보안 기능도 통합적으로 제공한다.

기술 검증과 제품 안정화는 필수

NAC 솔루션은 내부 네트워크에 접속하는 사용자 신원을 확인하는 '인증'과 단말기에 설치된 운영체제 보안패치나 안티바이러스 등 적절한 보안조치가 돼 있는지 '무결성'을 검사하는 두 기능이 핵심이지만, 초기에는 대부분 사용자 인증 방식을 지원하지 못했다. 또 단말기에 설치된 운영체제와 보안 제품과의 연동뿐만 아니라 인증 지원 방식에도 한계를 드러내고 있어 실제로 이를 구현하는 데에는 여전히 기능이나 안정성 면에서 부족한 점이 많다.

그럼에도 불구하고 'NAC' 기술은 내부 네트워크 끝단에 있는 사용자를 직접 관리할 수 있어 사전방어적인 내부 네트워크 보안체계를 갖추는 동시에 일관성 있게 사용자 보안정책을 강제할 수 있는 새로운 대안이라는 인식이 자리 잡힌 상태다.

때문에 업체들은 사용자 기대효과에 맞춰 꾸준히 기능을 추가하고 있으며, 다양한 네트워크 장비 및 보안 솔루션 업체와의 연동지원 협력도 넓히면서 편리성과 기능성을 확보해 나가고 있다.

대표적으로 가장 먼저 NAC의 개념을 소개했던 시스코시스템즈는 NAC 전략 발표 후 지난 3년 동안 단계별로 기능을 추가하면서 확장된 버전을 꾸준히 출시하고 있다.

마이크로소프트도 3년 전 처음 발표한 NAP 기능을 올해 출시된 윈도 비스타 외에 내년 출시할 윈도 서버 2008, 윈도 XP 서비스팩3에서 구현할 예정이다.

쓰리콤/티핑포인트도 지난해에는 IPS에서 제공해온 NAC 기능이 무결성 검사와 쿼런틴(격리) 보호 기능 수준이었던 반면, 올해 상반기에는 새로운 전방위 NAC 제품을 출시하고 네트워크에 사용자가 접속한 이후에도 사용자 트래픽을 지속적으로 점검하는 기능을 추가했다.

주니퍼네트웍스도 지난해 하반기 새롭게 인수한 펑크소프트웨어의 제품을 통합해 'UAC(Unified Access Control) 2.0'을 선보이면서, 사용자 인증 기능을 제공하고 있다.

시만텍 또한 올 10월에 기능을 대폭 확장한 '시만텍 네트워크 액세스콘트롤 11.0' 신제품

을 출시할 예정이다.

국산업체로 NAC 시장에서 두각을 나타내고 있는 유넷시스템도 지난해 802.1X 인증 기반의 NAC 솔루션뿐만 아니라 NON-인증기반 네트워크 환경에 적용할 수 있는 '애니클릭 NAC 컨트롤러' 신제품을 출시, 다양한 환경에 적용할 수 있는 제품군을 완비했다. 또한 마이크로소프트와도 NAP 개발 협력을 진행하고 있어, 조만간 국내 시장에 '애니클릭 NAP' 신제품을 선보일 예정이다.

국내에서는 지난해 서울대학교와 전북대병원이 최초로 NAC 솔루션을 도입하면서 NAC 솔루션에 대한 관심이 부쩍 높아졌으며, 올 들어 신한은행과 SK텔레콤, 한국석유공사, 서강대학교, 송파구청, 고려대학교 등도 잇달아 구축을 추진하면서 이제는 전 산업군으로 적용이 확산되고 있는 상황이다.

올해까지는 시장 검증기, 내년 본격 확산 단계 진입 예상

선도적으로 도입에 나선 이들 기업은 적잖은 시행착오와 어려움을 겪고 있다. 현재 국내 시장에만도 10개가 넘는 NAC 관련 제품이 출시돼 있지만 초창기라는 특성상 구축과 사용에 한계가 있기 때문이다.

하지만 업계에서는 올 하반기부터 내년까지 다양한 환경에 구축되는 사례가 많아지고 제품 기능도 대폭 개선되면서 기술 검증과 안정기를 거쳐, 내년에는 본격 확산될만한 수준에 오를 것이라는 희망적인 전망이 우세하다.

도입 작업 중인 기업들도 대부분 방화벽이나 안티바이러스처럼 단번에 설치해 운영할 수 있을 것으로 보기 보다는 장기간 단계적인 과정을 밟아야 NAC 기능을 제대로 구현할 수 있을 것으로 예상하고 있다.

네트워크에 접속하는 사용자를 인증하고 적정한 보안정책을 준수하고 있는지 확인해 강제하는 NAC 솔루션은 단품 형태가 아니라 기업 내 '보안인프라' 기능을 수행하기 때문에 구축이 쉽지 않다.

NAC 기술을 도입하려면 먼저 현실적으로 기업의 사용자 보안정책 수준과 절차를 적절히 정의해야 한다. 또한 기존 네트워크 및 보안 장비뿐만 아니라 사용자단과 직접 연계돼 있어 PC 운영체제상에서 동작하는 보안 솔루션과의 연동 등 고려해야할 사항도 많다.

아직까지 많은 제품이 사용자 인증을 지원하지 않은 채 PC의 무결성만을 검사해 네트워크 접속을 차단 · 격리시키고 있으며, 그 기능도 완벽하다고 할 단계는 아니다. 사용자 인증의 경우에도 DHCP, IPSec(Internet Protocol Security), 무선랜 보안 표준인 802.1X, 사용자 디렉토리 서버 등 다양한 사용자 환경을 수용하지 못하고 있다. 또한 개방형 표준을 지원하지 않아 특정 제품만을 지원하는 경우도 많다.

외국계 회사의 제품은 국내에서 많이 사용하는

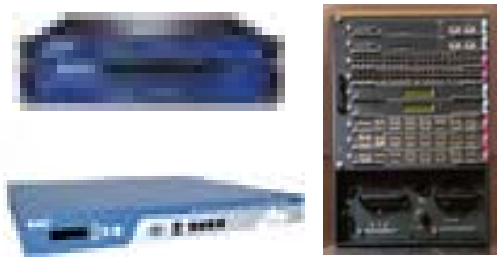
안티바이러스와 호스트 기반 IPS, 패치관리시스템(PMS) 등을 지원하지 않는 경우도 있다.

솔루션 업체들은 이러한 문제가 올 말이나 내년 초쯤이면 상당부분 개선될 것으로 전망하고 있다. 따라서 도입에 나선 기업 대부분은 1차 파일럿 형태로 구축한 후 사용자 적용 숫자와 기능을 단계적으로 확장하는 형태로 진행하는 상황이다. NAC 솔루션을 구축중인 한 업체 관계자는 "원하는 보안수준을 충족하기 위한 기능을 다양하게 구현하려면 내년 후반까지는 가야 할 것으로 보여, 단계적으로 서서히 구축을 확장해 나갈 계획"이라고 말했다.

현재 도입을 추진 중인 한 대학의 담당자는 "방화벽이나 IPS 등 기존 보안제품과는 달리 실 환경에 적용했을 때 예상할 수 있는 사전 테스트를 수행하기에도 제한적이며, 사용자 무결성 검사의 수준(depth)을 설정하는 것도 어렵다"고 토로했다.

사용자단 통제가 어려운 대학은 PC단의 보안제품만도 수십 개가 깔려있는 경우도 있어, 모든 솔루션을 연동 지원하기에도 난감한 문제가 나타나기도 한다. 이러한 여러 문제로 NAC시스템을 구축하려면 먼저 NAC의 기능을 어디까지 구현할 것인지 정확히 설정하고, 네트워크 인프라와 사용자 환경을 면밀히 파악해 구축 절차를 수립하는 것이 중요하다는 게 업계 전문가들의 조언이다. 그렇지 않으면 예정에 없던 네트워크 인프라를 전면 교체해야 하는 등 과도한 투자와 불필요한 작업에 시달릴 수 있고, 사용자들의 불편만을 초래한 채 심각한 관리부담에 직면할 수도 있다는 지적이다.

이미 1차 시스템 구축을 완료한 한 대기업의 보안담당자는 "NAC시스템을 구현하려면 먼저 사용자 인증체계를 제대로 갖추고, 사용자가 지켜야 하는 보안절차 지도(MAP)를 생성해 그에 맞게 구축하는 것이 중요하다"고 강조했다. 이어 "사용자에 대한 설득력을 높이고 구축 실행력을 담보하기 위해 IT보안팀 만이 아니라 IT기획 · 인프라 · 경영지원팀까지 협력해야 하며, 원하는 기능과 현재 사용하는 보안 솔루션과의 연동 지원 문제도 사전에 해결할 수 있는 방안을 제시하도록 솔루션 개발 업체에 적극적으로 요구할 필요가 있다"고 덧붙였다.



이렇게 NAC를 구현하는데 많은 어려움이 있음에도 불구하고 기업 담당자들은 "NAC 기술은 비인가자의 내부 네트워크 접속을 차단하고 사용자들이 사내 보안정책을 준수하도록 강제해 보안 사고를 예방할 뿐 아니라 무분별한 전산자원 낭비까지도 막을 수 있는 효과를 거둘 수 있다"는 데 동의하고 있다.

특히 "제대로 구축하면 사용자들에게 기존 네트워크 사용 환경을 동일하게 제공하면서 안전한 사용 환경을 보장할 수 있어 효과적"이라는 데 이견이 없다.

'통합보안위험관리', 차세대 보안투자의 화두로 급부상

수준 높은 내부 보안관리체계를 수립하기 위한 시장 관심은 총체적인 IT자산의 위험수준을 능동적으로 파악하고 대응할 수 있는 진보된 '통합보안/위험관리' 기술로도 집중되고 있다.

기업들이 보안관리 정책과 중앙집중적인 관리체계가 미흡하고 보안관리 인력도 부족한 상황에서 강화되는 외부 규제(컴플라이언스)와 늘어나는 IT운영상의 취약점 및 위험도를 적절히 대응하고 관리할 수 있는 효과적인 방안을 모색하려는 데서 이와 같은 기술을 필요로 하고 있기 때문이다.

각종 위험과 위협에 지능적으로 대처하기 위해서는 개별 보안제품에 의존할 것이 아니라 다양한 보안기술을 통합적으로 활용하고 중앙집중적으로 관리해야 한다는 인식이 자리하면서, '통합'과 '관리' 기능을 제공하는 보안기술에 대한 관심이 부쩍 높아진 것과도 무관하지 않다.

업계에 따르면, 최근 시장에서는 기업의 보안정책에 맞게 프로세스 상에서 통제할 수 있는 폭넓고도 한층 고도화된 통합보안관리 솔루션에 대한 요구가 높아지고 있다. 공공기관과 금융기관, 제조·통신사업자 등이 ESM(통합보안관리솔루션)이나 TMS(위협관리시스템) 외에 RMS(위험관리시스템), SIEM(통합보안정보관리) 등 새로운 기술 투자에 적극 나서고 있다는 점이 이를 반증한다.

보안관리 솔루션이 기업 전체의 IT 및 보안시스템과 연관돼 있다는 점에서 기업들의 차세대 보안관리 기술의 적용은 곧 보안정책과 프로세스를 혁신해 총체적인 위험관리체계와 보안사고관리체계를 구현하는 작업이 될 것이라는 게 업계의 분석이다. 특히, 진보된 통합보안위험관리 기술은 기존의 보안시스템에 한정됐던 보안관리 범위와 대상이 IT정보자산과 내부 조직의 업무프로세스 전반으로 확대, 비즈니스와의 연관성을 높일 것으로 기대되고 있다. 또 기존의 보안시스템과 유기적으로 운영되면서 정보자산의 취약점을 파악해 지속적인 모니터링과 조치과정을 거쳐, 잠재된 보안위험을 제거해 기업의 손실을 능동적으로 예방할 수 있는 체계를 유지하도록 만드는 효과도 거둘 것이라는 예상이다.

이러한 기대효과는 당연

히 기업의 비즈니스 업무절차와 조직구성원의 행위를 체계적으로 통제하고 가장 우선적인 보안투자에 효과적인 의사결정을 지원할 수 있는 장점까지 반영될 수 있다. 그런 점에서 기존의 보안관리시스템은 기능과 역할의 범위가 한계에 다다랐다는 진단이 나오고 있다.

먼저 ESM은 보안솔루션의 로그를 취합해 한눈에 보여주는 수준으로, 당초 목표로 했던 고도의 상관관계 분석을 통한 능동적인 통합보안관리 기능을 수립하지 못했다는 평가가 지배적이다.

방대한 양의 로그 중에서 실제로 기업이 필요한 로그를 분별해내기도 어렵고 분석기능 부족으로 보안위협과 위험에 대한 대응수준을 적절히 관리할 수 있도록 이용하는데 한계가 있다는 지적이다.

TMS도 네트워크상의 위협을 실시간으로 식별할 수 있어 사고 발생 시 즉각적인 조치를 수행할 수 있도록 하지만, 원래의 예보 기능은 제대로 수행하지 못했다는 평가다. 때문에 기존 ESM · TMS의 한계를 보완할 수 있는 다른 영역의 보안관리 제품이나, IT자산의 취약점과 네트워크상의 이상트래픽, 보안이벤트 등을 한꺼번에 포괄할 수 있는 통합적인 시스템이 요구되고 있는 것이다.

이에 따라 ESM과 TMS로 대표돼온 기존의 보안관리 시장은 RMS · SIEM 등으로 저변이 확대되는 동시에 모든 형태의 보안관리 기술을 수용하는 '통합보안위험관리시스템' 으로 빠르게 진화하기 시작했다.

SK텔레콤이 최근 ESM과 TMS, RMS 등 각각의 보안관리솔루션을 모두 포괄한 차세대 통합 보안관리시스템 개발에 들어간 것도 같은 맥락이다. SK텔레콤은 이번 사업에서 정보보호관리체계(ISMS)와 보안포털, RMS, SIEM을 통합적으로 구현, 기존의 ESM, TMS, NMS(네트워크관리시스템), 방화벽 로그분석시스템 등 보안/네트워크관리시스템까지도 모두 연동할 계획이다. 이를 통해 IT자산과 네트워크의 보안 및 위험관리를 수행할 수 있는 차세대 통합 보안정보관리솔루션체계를 갖출 것으로 기대하고 있다.

RMS, 차세대 보안관리 분야 핵심기술로 주목

국내에서는 포스트 ESM 솔루션 중에서도 '위험관리시스템(RMS)' 이 가장 많은 관심을 끌고 있어 이 제품이 차세대 통합보안관리 시장을 이끄는 데 톡톡히 역할을 할 것으로 기대되고 있는 상황이다. 이미 지난해 초부터 업체들은 전문 RMS 제품을 잇달아 시장에 활발히 소개해 왔고, 기존 보안관리 분야 전문업체들도 ESM · 위협관리시스템(TMS) 제품에 위험관리 기능을 추가하기 위한 작업에 나서고 있다.

'RMS' 의 핵심 기능은 IT자산 전체를 대상으로 취약점과 위협을 미리 파악해 대응함으로써 사전에 보안사고를 예방하고 보안수준을 상시적으로 관리하는 데 있다.

내부에서 새롭게 발생하는 취약점과 위협이 발생하고 있는 지점을 즉각적으로 찾아 우선순위별로 대응 조치할 수 있도록 제공하기 때문에 보안투자와 운영관리 효율성을 높일 수 있다는 점에서 높게 평가받는다. 기존 보안의 개념을 확장시켰다고 정의할 수 있다.

기존의 ESM 솔루션은 보안시스템으로부터 로그를 수집해 모니터링하는 기능을 수행하는데 초점이 맞춰졌다. 반면에 RMS는 이들의 기능과는 다른 장점을 갖고 있는 것이다.

이에 따라 기존의 국내 ESM과 TMS 업체들은

모두 기존 제품에 RMS 기능을 추가하거나 연동 가능한 전문 제품을 별도로 출시하고 있다. 관제서비스에 적용하는 ESM 업그레이드 서비스 모델도 나오고 있는 상황이다.

또한 기존 RMS 전용 제품의 경우에도 본래의 기대효과를 높이기 위한 꾸준한 기능 추가 작업도 이뤄지고 있다.

국내 ESM 대표 업체였던 이글루시큐리티가 지난 7월 출시한 '스파이더-X' 는 이기종의 보안시스템과 주요 정보시스템에서 발생하는 여러 종류의 위협 및 취약성 정보를 해당 자산의 중요도와 연계시켜 종합적으로 분석, 전사적 위험도를 관리할 수 있는 웹 기반의 종합위험관리시스템이다.

이글루시큐리티는 정보보호 수준측정을 위해 이 제품에서 제공해온 평가지표 항목을 국가사이버안전메뉴얼과 한국정보보호진흥원(KISA) ISMS뿐만 아니라 국제 표준인 BS7799/ISO27001도 지원할 수 있도록 확장하는 작업 등을 꾸준히 진행하고 있다.

안랩코코넛은 보안관제서비스 툴로 사용해 온 자체 개발 ESM 솔루션인 '세피니티' 를 RMS로 업그레이드, 위협 · 자산관리 기능을 추가한 2.0 버전을 조만간 출시할 예정이다. 연내에 취약점 분석과 컴플라이언스 관리 · 계정관리 솔루션도 추가로 연동해 위험관리서비스 모델을 완성해 나간다는 목표다. 이를 보안관제서비스인 'e트리니티' 서비스에 적용, 위험관리 기반의 새로운 보안관제 모델을 선보일 방침이며, 고객 전용 위험관리 포털인 'e트리니티 온라인 v2.0' 도 함께 준비하고 있다.

유일한 외산 솔루션으로 RMS 개념을 국내에 소개해 초기 시장을 여는데 견인차 역할을 해온 한국맥아피는 기능을 강화한 '파운드스톤 6.0' 신제품을 공급할 예정이다. 이 제품은 맥아피의 보안관리 솔루션인 'ePO' 와 IPS인 '인트루쉴드' 와 통합되며, 위험관리 분석보고서 생성 기능도 강화됐다. 또 기존 BS7799, ISO17799 뿐만 아니라 바젤II 등 컴플라이언스 지원 모듈도 확장할 예정이다.

보안컨설팅과 보안관제서비스를 제공해온 인포섹도 최근 RMS, TMS, ESM에 사이버안전지원(웹포털) 기능을 통합한 종합보안정보관리(ToSIM)시스템을 개발하고, 이 시스템을 주축으로 보안SI 사업에 적극 나섰다.

TMS 시장을 양분하고 있는 윈스테크넷과 정보보호기술도 기존 TMS에 ESM와 RMS 기능을 통합하는 작업을 활발히 진행하고 있다.

윈스테크넷은 현재 유해트래픽 분석 · 제어 솔루션에서 제공하고 있는 TMS인 '스나이퍼 iTMS' 와 비정상트래픽 감지시스템 '스나이퍼 APS' , 종합위협분석 · 처리시스템인 '스나이퍼TSMA' 을 기반으로 대규모 네트워크에서 요구하는 RMS을 추가로 개발하고 있다.

정보보호기술은 연말까지 '테스 TMS' 의 위협관리 기능에 통합관제 기능을 강화하고 위험관리 기능도 추가해 차세대 TMS 신제품을 내놓을 예정이다.

윈스테크넷의 김대연 사장은 "TMS와 ESM, RMS는 시장의 요구에 따라 각각 서로간의 부족한 기능이 자연스럽게 추가 · 보완되고 있다" 면서, "향후에는 세 솔루션이 모두 합쳐지는 형태가 될 것" 이라고 말했다.