SECURITY REPORT

클라우드 AI 시대 시만텍 전략

By 바이라인네트워크

시만텍,
사이버 보안 새역사 쓴다

'통합 사이버보안 플랫폼'으로 클라우드 시대 복잡한 기업보안 문제 해결

시만텍코리아가 블루코트와 합병으로 탄생한 '뉴(New)시만텍' 출범 후 첫 대규모 고객 행사를 열었다.

시만텍은 지난 8월30일 서울 코엑스 인터컨티넨탈 호텔에서 '시만텍 시큐리티 포럼'을 열고 최근 보안위협 트렌드와 엔드포인트, 네트워크, 클라우드 등 기업 인프라 전반을 보호할 수 있는 뉴시만텍의 통합 사이버보안 플랫폼(Integrated Cyber Defense Platform)을 소개했다.

이석호 시만텍코리아 대표는 이날 행사에서 "1년 전이던 작년 8월 시만텍과 블루코트 합병이 마무리되면서 엔드포인트, 네트워크, 클라우드를 아우르는 보안의 강자가 새롭게 탄생했다"라면서 "세계가 전례없는 사이버위협에 직면하고 있고 기업의 보안관리자와 IT관리자들이 지켜야할 보안위협의 반경이 점점 넓어지는 상황에서 뉴시만텍이 사이버보안의 새로운 미래를 열어나가며 새로운 역사를 쓰겠다"고 강조했다.

이어진 기조연설에서는 뉴시만텍이 만들어가고 있는 혁신을 소개했다. 쉐리프 엘 나바위(Sherif El Nabawi) 시만텍 아시아태평양지역 시스템 엔지니어링 수석이사는 먼저 시만텍이 추진한 변화(Transformation)의 과정을 세 단계로 나눠 제시했다.

"첫 단계는 스토리지 비즈니스를 분리해 보안 사업에 집중하기로 결정한 것이다. 두 번째는 블루코트와의 인수합병으로 웹과 엔드포인트 전문성을 바탕으로 엔터프라이즈 고객 지원을 더욱 강화할 수 있게 됐다. 세 번째 단계는 소비자 보호 역량을 강화하기 위해 라이프로그를 인수한 것이다."

사이버보안의 새로운 미래를 열겠다는
이석호 시만텍코리아 대표

혁신 :
글로벌 위협
인텔리전스 강화

나바위 수석이사는 시만텍과 블루코트가 통합하면서 얻은 가장 큰 이점으로 위협 인텔리전스 범위가 더욱 방대해졌다는 점을 꼽으면서 "시만텍은 업계 최대규모인 1억 7500만개의 엔드포인트 사용자를 보호하고 있다. 엔드포인트와 웹에서 수집된 데이터와 텔레메트리를 합쳐 즉각적으로 전세계에서 발생하는 모든 위협에 대한 가시성을 확보할 수 있고 최신 위협에 보다 빠르게 대응하고 보호한다"고 강조했다.

또한 "시만텍은 3500명 이상의 연구개발(R&D) 인력을 바탕으로 인수합병 1년 만에 '통합 사이버보안 플랫폼'을 발표하면서 새로운 혁신을 이끌고 있다"고 덧붙였다.

시만텍의 통합 사이버보안 플랫폼은 클라우드 세대(Cloud Generation)가 본격 열리면서 나타나는 위협 동향과 기업 업무 환경 변화에 맞춰 기업이 최적화된 사이버보안을 구현할 수 있도록 지원한다.

클라우드·IoT 시대,
'스택형 보안'은 한계

나바위 수석이사는 시만텍과 블루코트가 통합하면서 얻은 가장 큰 이점으로 위협 인텔리전스 범위가 더욱 방대해졌다는 점을 꼽으면서 "시만텍은 업계 최대규모인 1억 7500만개의 엔드포인트 사용자를 보호하고 있다. 엔드포인트와 웹에서 수집된 데이터와 텔레메트리를 합쳐 즉각적으로 전세계에서 발생하는 모든 위협에 대한 가시성을 확보할 수 있고 최신 위협에 보다 빠르게 대응하고 보호한다"고 강조했다.

또한 "시만텍은 3500명 이상의 연구개발(R&D) 인력을 바탕으로 인수합병 1년 만에 '통합 사이버보안 플랫폼'을 발표하면서 새로운 혁신을 이끌고 있다"고 덧붙였다.

시만텍의 통합 사이버보안 플랫폼은 클라우드 세대(Cloud Generation)가 본격 열리면서 나타나는 위협 동향과 기업 업무 환경 변화에 맞춰 기업이 최적화된 사이버보안을 구현할 수 있도록 지원한다.

혁신 :
모든 환경, 모든 요소
포괄 지원하는
'통합 사이버보안 플랫폼'

나바위 수석이사는 "시만텍은 엔드포인트, 웹, 클라우드 등 모든 요소를 관리 가능하게 만든다. 통합 사이버보안 플랫폼은 온프레미스, 오프프레미스·클라우드 서비스 모두 똑같은 수준에서 원하는 대로 지원한다"고 밝혔다.

시만텍 통합 사이버보안 플랫폼은 정보(Information), 사용자(User), 웹(Web), 메시징(Messaging)을 보호할 수 있는 온프레미스, 클라우드 솔루션과 서비스를 제공하며, 사이버보안서비스(CSS)도 지원하고 있다.

나바위 수석이사는 "모든 솔루션과 서비스는 글로벌 인텔리전스 네트워크(GIN)와 통합돼 엔드포인트와 웹에서 수집되는 데이터와 텔레메트리 기반 위협 인텔리전스를 공유한다. 바로 실행가능한(Actionabl) 인텔리전스를 제공할 수 있다는 것"이라며 "통합 플랫폼상에서 모든 것을 제공해 일부 의사결정은 자동화할 수 있도록 지원한다"고 설명했다.

혁신은 계속
…파이어글래스·스카이큐어 인수

그는 "시만텍은 여기서 멈추지 않고 계속 전진하고 있다"라면서 최근 시만텍이 사이버보안 솔루션과 서비스 경쟁력을 더욱 강화하기 위해 최근 파이어글래스(FireGlass)와 스카이큐어(Skycure)를 인수한 사례를 소개하기도 했다.

파이어글래스는 웹 브라우저 아이솔레이션(격리) 기술을 보유한 이스라엘 기업이다. 스카이큐어는 모바일 위협 방어 기술업체다.

시만텍은 이날 랜섬웨어 위협과 대응 전략, 인공지능 시대 지능형 지속위협(APT) 대응 해법, 클라우드 보안 방안을 제시했으며, 웹 보안 게이트웨이 솔루션 고객사례 발표와 고객들과 함께하는 패널 토크도 진행했다. By

[그림 1] 시만텍 통합 사이버 보안 모델

늘어나는 **랜섬웨어, 어떻게** 방어하나


실시간 다단계 보안의 중요성을 강조하는 서종렬 시만텍코리아 상무

"최근 랜섬웨어의 가장 큰 특징은 '실시간성'이다. 피해를 최소화할 수 있게 얼마나 빨리 대응하느냐가 중요하다. 보안의 '자동화'와 '최신화'가 핵심이다."

서종렬 시만텍코리아 상무는 '시만텍 시큐리티 포럼'에서 실시간 다단계 보안의 중요성을 강조하면서 랜섬웨어에 가장 효과적으로 대응할 수 있는 방안을 발표했다.

사이버보안에서 기업이 최근 가장 신경 쓰는 부분은 역시 랜섬웨어다. 지난해 기준 전반적인 악성코드 증가율은 둔화된 반면, 새로 발견된 랜섬웨어는 36%가 늘었다. 랜섬웨어 패밀리의 증가율은 237%나 된다.

공격량만 늘어난 것이 아니다. 랜섬웨어 자체도 기술적으로 진화하고 있다. 최근 빈번하게 등장하는 크립토 계열 랜섬웨어는 고도화된 암호화 기법을 사용해 기업이나 사용자가 가장 중요하게 여기는 데이터를 인질로 잡는다. 개인이 쓰는 모바일, 사물인터넷(IoT) 기기도 공격 대상이 된다. 공격 범위도 리눅스는 물론, iOS나 안드로이드, 유닉스 등으로 확장됐다.

이 과정에서 해커들이 노리는 타깃도 '기업 내 중요 데이터'로 좁혀지고 있다. 다시 말해 해커들이 어느 것이 돈이 되는지 정확히 짚어내고 있다는 말이다.

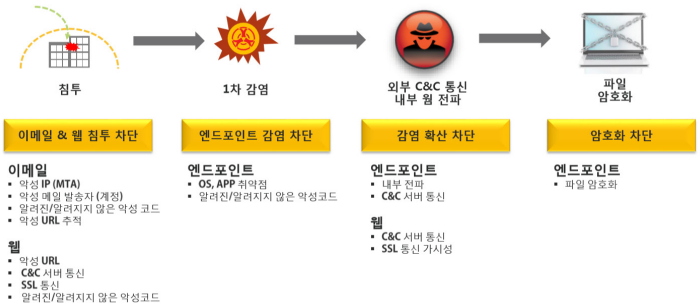
서 상무는 "지난 2015년 랜섬웨어 공격자가 피해자에 요구한 평균 금액이 300달러 수준이었다면 1년만인 2016년에는 1000달러로 세 배나 뛰었다"며 "최근에는 현금대신 비트코인이나 다양한 은닉 트랜잭션 거래를 피해자에게 요청하는 등 해커들이 경제적 이익에 집중하고 있다"고 말했다.

그렇다면 중요 데이터를 지키기 위해서 기업과 개인은 어떤 점에 유의해야 할까.?서 상무는 랜섬웨어가 유입되과 확산되는 각 단계의 '킬링 파트'별 보안에 중점을 둬야 한다고 강조했다. 랜섬웨어가 알려진 취약점을 찾아서 사용자 간섭 없이 스스로 전파하는 형태로 발전하고 있는 만큼, 각 유입 단계에서 실시간으로 철저한 차단이 필요하다.

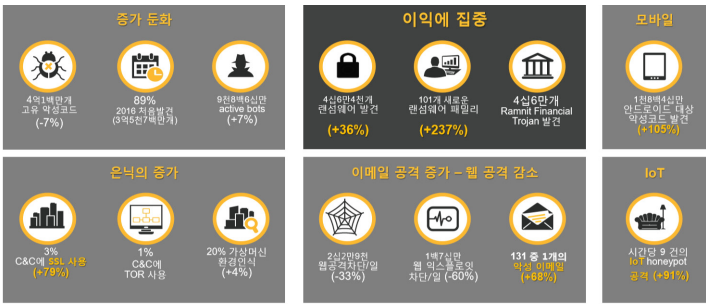
첫 단계는 이메일이다. 지난해 기준, 전체 이메일 131통 중 1통이 악성 이메일이었다. 이메일에 의해 최초 감염자가 생기는 경우가 많은데, 이 단계에서 막지 못하면 랜섬웨어가 자가 증식을 통해 취약점을 찾아 공격한다. 최초 감염자를 방어할 수 있는 실시간 경호 방어체계가 구축되어 있느냐를 점검해야 한다.

웹을 통한 감염도 마찬가지다. 하루에도 1억개 이상의 웹사이트가 생기는데, 수동 필터링 만으로는 모든 위험을 통제할 수 없다. 이 때문에 사용자가 웹에 접속함으로써 랜섬웨어에 감염되는 사태를 막을 수 있는 인프라가 만들어져야 한다. 패치 관리와 이를 유지하는 자동화 포인트를 만들어야 한다. 자동화와 최신화를 통한 실시간 다단계 방어 시스템이 필요하다는 뜻이다.

그는 "랜섬웨어가 기업 내 네트워크에 확산될 때, 공격 단계 중 하나의 체인만 끊어져도 기업 보안에 큰 영향을 미치지 못할 것"이라며 "이메일로 인한 1차 감염, 랜섬웨어가 스스로 취약점 찾아 전파



[그림 1] 랜섬웨어 대응 방안-킬 체인 전략



[그림 2] 악성 코드 동향

되는 시점에서의 차단, 그리고 암호화를 통해 가장 중요한 데이터를 보호하는 것 등 각 단계별로 랜섬웨어 확산을 끊어주는 킬체인 전략이 중요하다"고 강조했다.

마지막으로 '최신 랜섬웨어에 대한 정보' 역시 보안의 한 축이라고서 상무는 설명했다. 지금처럼 매일 새로운 랜섬웨어가 등장하는 때는 문제가 일어났을 때 관련정보를 얼마나 확보하고 있고, 또 얼마나 믿을 수 있게 실행할 수 있느냐가 매우 중요하다는 것이다.

그는 "워너크라이가 발발했을 때 시만텍은 2200만 건의 공격을 차단했다"며 "시만텍은 방대한 위협 인텔리전스 DB를 통해 최신 정보를 공유, 정품 서비스에서 활용할 수 있도록 제공한다"고 말했다. By

보안 위협 패러다임 변화를 설명하는 최장락 시만텍코리아 이사

인공지능 시대, 보안 패러다임도 변한다

사이버보안 기술이 나날이 발전하고 있지만 보안사고는 끊이지 않는다. 오히려 '랜섬웨어'같은 더욱 진화된 사이버보안 범죄가 증가하고 있다. 기존의 시각으로 보안사고를 바라봐서는 안 된다. 보안 위협 패러다임 역시 바뀌고 있기 때문이다.

최장락 시만텍코리아 이사가 말하는 지능형지속위협(APT)을 비롯한 보안 패러다임 변화를 요약하자면, 인공지능으로 이뤄진 창과 방패다. 그는 '시만텍 시큐리티 포럼'에서 지능형위협 침투 탐지부터 사후 대응을 모두 아우르는 APT 관련 해법을 논했다.

먼저 보안 패러다임은 어떻게 바뀌었을까. 카네기멜론대학 연구팀이 만든 인공지능 시스템 '메이헴(MayHem)'이 그 방향성을 시사한다. 메이헴은 인공지능 시스템 간 해킹대회에서 우승한, 매우 똑똑한 슈퍼컴퓨터다. 그 결과 지난해에는 인간과의 해킹 대결(세계 최대 해킹 방어대회 '데프콘 CTF') 참여권을 얻었다. 다만 성적은 최하위에 머물렀다. 하지만 메이헴은 폴란드의 유명 해킹팀을 이긴 것으로 나타나 눈길을 끌었다.

메이헴은 원하는 대상의 취약점을 학습을 통해 자동으로 찾아가고 공격한다. 이 모든 과정이 전부 머신러닝을 통해 이뤄졌다. 여기서 향후 해킹의 방향을 엿볼 수 있다. 최 이사는 "우리가 말하는 기존의 지능화된 정교한 공격을 사람이 아닌 인공지능 시스템이 수행하는 형태가 실제로 발생하고 있다"며 "방어하는 사람 입장에서도 인공지능 기술을 이용해야 한다는 것이 분명해진 것"이라고 말했다.

결국, 앞으로는 머신러닝을 잘 하는 기업이 보안도 잘 한다는 논리다. 10년 전만 해도 보안 공격 패턴이 복잡하지 않았다. 수동으로 패턴을 일일히 업데이트 할 수도 있었다. 아니면 특정 규칙을 만들어 시스템에 적용하기만 해도 웬만한 보안 사고를 막을 수 있었다. 그런데 이제는 그런 방법으로는 더 이상 안심하기 어렵다. 데이터도 많아지고, 기존 패턴으로는 이해하기 어려운 공격형태들이 나오고 있기 때문이다.

이 과정에서 최 이사가 강조한 것은 '양질의 데이터'다. 알파고의 예를 들어보자. 최 이사는 "알파고가 아마추어 기보 데이터로 연습했다면 이세돌을 이기기 어려웠을 것"이라며 "시만텍이 머신러닝을 활용한 보안과 탐지를 잘 할 수밖에 없는 이유는 (보안과 관련한) 양질의 모 데이터가 지금 이순간에도 세계에서 모아지고 있기 때문"이라고 강조했다.

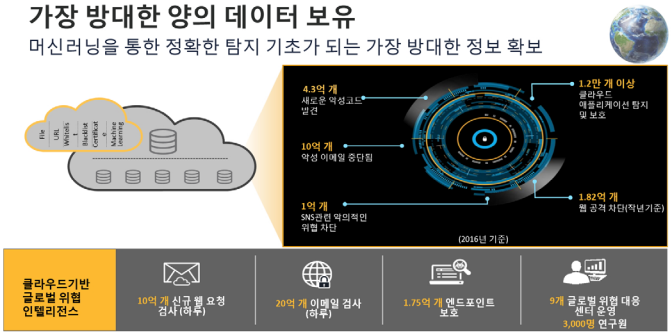
특히 시만텍에서 인공지능을 연구하는 수백명의 연구진이 보안 상품의 설계부터 참여, 머신러닝 기술을 어떻게 적용시킬 것인지를 논의하는 것을 자사 상품의 강점 중 하나로 꼽았다. 머신러닝이 적용된 대표 사례 중 하나가 이 회사 대표 보안 솔루션인 '시만텍 엔드포인트 프로텍션(SEP) 14'다. 악성 여부 판단을 위해 4억개 이상의 샘플을 돌리고, 그 결과 값을 그룹으로 나눠 분류해 악성 여부의 유사성을 계속해 찾아가는 방식으로 보안 위험을 찾아가는 방식이 SEP 14에 적용됐다. 이 경우, 새로운 샘플이 들어오게 되면 인공지능 시스템이 자동으로 해당 샘플을 어느 그룹에 포함시킬지 결정하게 된다.

최 이사는 "어디에도 알려지지 않은 데이터를 100개씩 테스트 해보면, 한 번도 알려지지 않은 악성코드임에도 90개 이상을 탐지하는 결과를 보인다"며 "어드밴스드 머신러닝을 다른 시스템과 비교하면 획기적으로 탐지율이 높은 것을 알 수 있다"고 설명했다.

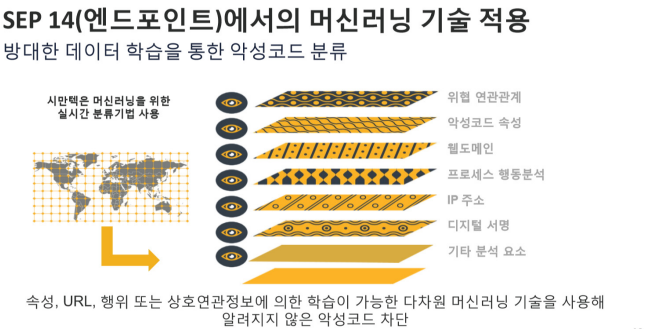
아울러 사용자의 평상시 통신 습관(IP, 접속 국가, 프로토콜, 파일 사이즈 등)을 학습해 놓고, 이와 다른 형태의 접속이 들어올 경우엔 그 차이 정도에 따라 알람을 울리는 방식 등을 통해 해킹 위험에 대비하게 하는 것이나, 평소 사용치 않던 프로토콜이나 애플리케이션을 누군가 내부 공격을 위해서 접속할 경우 이를 잡아내게 하는 것 등도 인공지능을 도입하면서 얻게 되는 성과다.

이밖에 시만텍 데이터유출방지(DLP) 솔루션은 회사 내부에서 기밀로 분류되는 패턴을 미리 지정해 놓고 보안 시스템에 학습시킬 경우 새로 생성되는 문서의 중요도(기밀) 여부를 판단, 이를 잡아내고 차단하는 역할로도 활용 가능하다.

최 이사는 "머신러닝은 단순한 개념이 아니다"라며 "블루코트와 합쳐진 시만텍이 보유한 방대한 정보를 통해 학습을 열심히 하고 있기 때문에 이메일, 웹, 클라우드 등 전 분야를 연계할 수 있는 것"이라고 말했다. By



[그림 1] 가장 방대한 양의 데이터 보유



[그림 2] SEP 14에서의 머신러닝 기술 적용

섀도우 IT에 대해 설명하는
최재우 시만텍코리아 이사

증가하는 클라우드 보안위협, '섀도우 IT·데이터' 문제 해결방안은

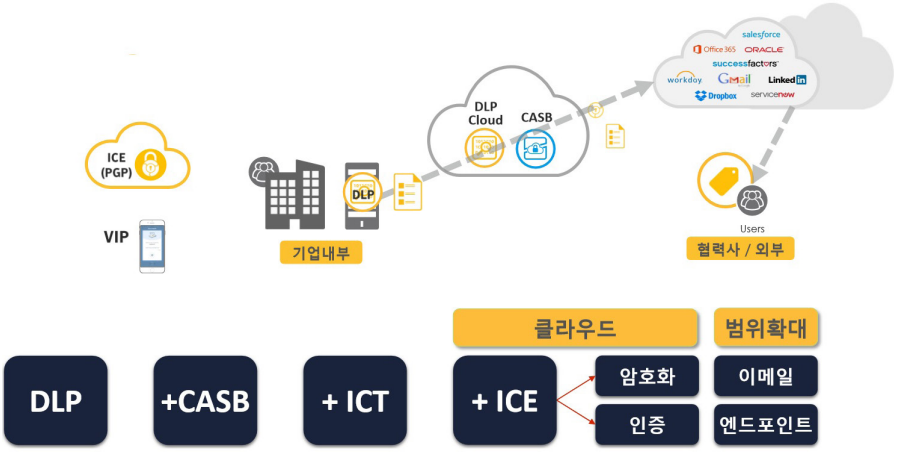
"기업에서는 평균 40여개의 클라우드 애플리케이션(앱)을 사용하고 있는 것으로 인지하고 있지만, 실제로 사용하고 있는 클라우드 앱은 평균 928개에 달한다. 기업 데이터의 26%는 가시성이 확보돼 있지 않은 채 이미 클라우드상에서 다른 사람과 공유되고 있다."

최재우 시만텍코리아 이사는 '시큐리티 포럼' 행사에서 이같은 조사 결과를 소개하면서 기업에서 클라우드 서비스 사용이 늘어나고 있지만 그 사용현황에 대한 가시성이 확보돼지 않는 '섀도우 IT'와 '섀도우 데이터' 문제가 나타나고 있다고 지적했다.

최 이사는 "이제는 클라우드 세대(Cloud Generation)라는 거스를 수 없는 시대가 시작된 만큼 보안방식도 변화가 필요하다"라고 강조하면서 "기존에 DLP(Data Loss Prevention)로 보호되는 기업 내부 정보를 클라우드로 전송할 때 CASB(Cloud Access Security Broker)와 연동해야 하며, 데이터 중요성을 사용자만 알고 있는 경우 문서파일에 태깅을 해야 한다. 이런 파일이 외부로 전송될 때 암호화와 인증 기술로 한 번 더 보호할 필요가 있다"고 말했다.

시만텍은 클라우드 사용 가시성과 통제 기능을 제공하는 CASB 플랫폼인 '클라우드SOC'를 비롯해 ▲정보유출 방지 솔루션인 'DLP' ▲데이터 암호화 솔루션인 'ICE(Information Centric Encryption)' ▲데이터 등급을 사용자가 지정(태깅)·분류하는 'ICT(Information Centric Tagging)' ▲다중요소인증 기능을 지원하는 'VIP(Validation and ID Protection)'를 클라우드 보안을 위한 정보 중심 보안 방안인 'ICS(Information Centric Security)' 솔루션으로 통합 제공하고 있다.

시만텍은 DLP 솔루션이 제공하는 범위를 클라우드까지 확대했다. CASB와 연계해 클라우드 환경에서도 기존 DLP에서 운영돼온 세부 기밀보안 정책을 그대로 클라우드까지 확장해 사용할 수 있게 했다.



[그림 1] 시만텍의 클라우드 보안 솔루션

최 이사는 "시만텍 DLP는 CASB와 클라우드상에 있는 'DLP 클라우드 서비스 커넥터'라는 클라우드 탐지서버로 연결돼 바로 전송하기 때문에 대역폭 문제없이 세밀한 정책 그대로 연동해 사용할 수 있으며, 공유된 파일을 취소할 수 있는 유연한 정책도 바로 적용된다"고 장점을 부각했다.

시만텍 '클라우드SOC' CASB 솔루션은 조직에서 사용하는 모든 클라우드 애플리케이션을 찾아 모니터링을 수행하고 감사(Audit) 기능도 제공한다. 클라우드로 데이터가 이동, 저장, 사용 중인 상황에서도 자동 감지, 분류해 보안정책에 따라 실시간 통제 기능을 적용할 수 있다. 세부 트랜잭션 가시성과 사용자행동분석(UBA), 보안위협 탐지, 포렌식 기능도 지원한다.

CASB는 클라우드 앱 기반 애플리케이션 프로그래밍인터페이스(API) 방식과 게이트웨이 방식으로 구성되는데, 시만텍은 두 가지 방식을 모두 제공해 다양한 클라우드 앱과 데이터 사용 환경을 지원하고 있다.

API 방식은 현재 박스, 드롭박스, 오피스365, 세일즈포스닷컴, 구글 앱스 등 11개 앱에서 API 방식을 지원한다. 게이트웨이 방식은 70개 이상의 클라우드 앱을 지원하고 있다.

최 이사는 "API 방식은 손쉬운 구성이 가능하다. 파일을 업로드하거나 수정하는 등의 이벤트가 발생하는 즉시 탐지할 수 있다. 게이트웨이 방식은 클라우드 서비스로 파일이 이동될 때 관문에서 트래픽을 거치게 하는 형태로 부하가 걸릴 수 있지만 더욱 많은 클라우드 앱을 탐지해 대응할 수 있다"고 설명했다.

이어 그는 "시만텍은 클라우드상에서 내가 공유해준 파일이 혹시 제3의 인물에게 공유될 수 있는 문제를 해결하기 위해 정보 중심 보안 기술을 제공한다"라면서 "시만텍 ICE는 파일이 외부 클라우드로 전송될 때 기밀정보나 중요정보가 포함된 경우 정책에 따라 해당파일은 자동 암호화한다. 수신자는 인증 절차를 거쳐 데이터를 열어볼 수 있으며, 파일이 잘못 공유될 경우 관리자가 공유나 업로드를 취소할 수 있다"고 설명했다.

아울러 "ICE는 파일을 열어보고 수정, 저장, 인쇄하는 권한도 세밀하게 제어할 수 있다. ICE 콘솔에서는 누가 어떠한 파일을 언제 열어봤는지 추적할 수 있다"라면서 "그동안 공유되는 파일이 어디로 전달되고 어떻게 사용되는지 몰랐고 세부 권한도 설정할 수 없었지만 모두 가능해졌다"고 덧붙였다.

최 이사는 "중요 데이터나 지적재산 분실·도난을 방지하기 위해 클라우드로 공유되는 문서파일에는 등급을 분류할 필요가 있다"는 점도 강조하면서 "파일 문서에 담긴 데이터 중요도는 키워드 기반 정책 보다는 실제 문서를 작성하고 만든 사람만이 가장 잘 알고 있다. 시만텍은 ICT 태깅 기술을 제공해 문서를 생성·저장하거나 메일 전송시 기밀등급을 설정해 데이터를 분류할 수 있다"고 소개했다. By

클라우드 AI 시대 **시만텍** 전략

바이라인네트워크

발행 | 바이라인네트워크
배포 | https://byline.network/
취재/글 | 이유지 기자 yjlee@byline.network
남혜현 기자 smilla@byline.network
문의 | byline@byline.network