네트워크 보안, 방화벽 정책관리

안전한 제로 트러스트 위해 차세대 네트워크 보안 필수

제로 트러스트를 강조하다보면 물리적 보안 경계를 지키는 네트워크 보안 솔루션은 필요 없는 것처럼 여겨진다.

이는 제로 트러스트에 대한 매우 심각한 오해 중 하나로, 제로 트러스트 원칙에서도 네트워크 보안은 필요하다. 사용자와 기기를 검증한 후 안전하게 연결하는 통신보안이 필요하며, 업무가 수행되는 중 허가받지 않은 외부 침입을 차단하는 기본 기능을 네트워크 보안에서 수행해야 하기 때문이다.

클라우드로 비즈니스가 이동한다 해도 온프레미스 데이터센터가 사라지는 것은 아니다. 클라우드 환경을 위한 네트워크 보안 솔루션이 필요하다. 클라우드 서비스 사업자(CSP)를 위한 대규모 고성능 네트워크 보안 솔루션 수요가 늘어난다. 네트워크 보안 시장은 그 어느 때보다 높은 매출 성장을 기대할 수 있다.

위협분석 전문성 탑재한 차세대 네트워크 보안

차세대 방화벽 등장 이후 방화벽, IPS, VPN을 구분하는 것이 의미 없어질 정도로 네트워크 보안 제품이 단일 플랫폼으로 통합되고 있다.

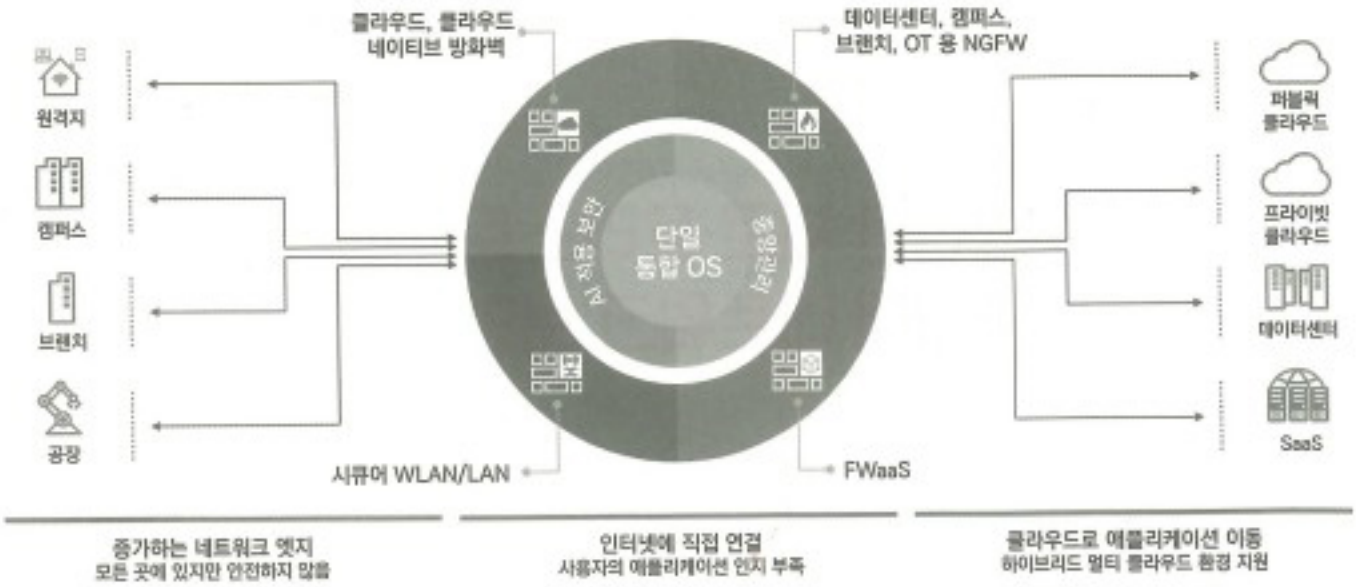
통합의 중심이 되는 차세대 방화벽은 ID 인지, 애플리케이션 제어 기능을 기본으로 탑재하며, IPS, VPN, 안티바이러스, URL 필터링 등 다양한 기능을 단일 어플라이언스에 통합해 네트워크 관문의 역할을 한다.

안랩은 네트워크 보안 시장 변화에 맞춘 완성도 높은 네트워크 보안 포트폴리오를 갖추고 있으며, 위협분석 조직과 인프라를 기반으로 국내 최적화된 위협 대응 능력을 지원한다.

자체 개발한 '어드밴스드 A 팀(Advanced A-TEAM)' 아키텍처를 채택해 패킷 처리 성능을 극대화했다. 이전 제품의 패킷 처리 속도 대비 몇 배 이상의 처리 속도를 보장하며, 멀티 코어 최적 활용 기술과 소프트웨어 가속 처리 기술을 지원한다.

차세대 방화벽 '트러스가드(TrusGuard)'는 안랩 엔드포인트 보안 솔루션과 연동해 엔드포인트부터 네트워크까지 중단 없는 보안을 제공한다. 원격접속 사용자 보안을 위해 SSL VPN 접속 시 보안 점검 검수를 수행하고 디바이스 상태를 확인한 후 접속을

〈그림 1〉 하이브리드 메시 방화벽 개념



(자료: 포티넷)

허용한다.

IPS 솔루션 '안랩 AIPS'는 알려진 공격뿐 아니라 다양한 취약점 공격까지 대응할 수 있는 진화한 보안 기능을 제공한다. 국내 네트워크에 최적화된 안랩의 6000여개 네트워크 공격 대응 시그니처를 제공하며, 암호화 트래픽의 가시성을 제공한다.

고성능 보장하는 네트워크 보안

국내 네트워크 보안 시장의 강자인 시큐아이는 클라우드, OT 환경에도 최적화된 솔루션과 서비스를 제공하면서 경쟁력을 입증하고 있다.

차세대 방화벽 '블루맥스 NGF(BLUEMAX NGF)', IPS '블루맥스 IPS', 무선 침입방지 시스템 '블루맥스 WIPS', 통합관리 시스템 '블루맥스 TAMS', 디도스 방어 '시큐아이 MFD', 네트워크 취약점 방어 '스캔 용 블루맥스 클라이언트' 등으로 구성된 네트워크 보안 포트폴리오를 갖고 있다.

클라우드 환경을 위한 차세대 방화벽 '블루맥스 NGF VE'도 지원해 다양한 가상화 클라우드 플랫폼 환경에서도 내외부 위협을 효과적으로 차단한다. Rest API 연동으로 보안 오케스트레이션을 지원해 보안조직의 탐지·대응을 효율화한다.

'블루맥스 NGF'는 PQC 알고리즘, 머신러닝이 추가돼 차세대 보안 요구에 최적의 대안을 제시한다. 더불어 SD-WAN 기능도 탑재해 시큐어 액세스 서비스 엣지(SASE) 플랫폼으로 진화하기 위한 기반을 마련했다. 더불어 통합 보안 플랫폼 '에스스퀘어오픈(S2OPEN)'과 연계해 클라우드 보안과 매니지드 서비스까지 지원하고 있다.

뛰어난 성능의 차세대 방화벽으로 인정받는 엑스게이트(AXGATE)의 차세대 방화벽은 논리적 가상화 기술을 적용해 방화벽 한 대로 여러 대의 방화벽과 VPN을 사용하는 것과 같은 독립적인 보안 서비스를 제공한다.

저가의 인터넷 회선을 묶어 고대역폭 VPN 채널을 제공하는 '디큐브 본딩(dCube Bonding)' 기술로

비용 효율적인 고성능 보안을 보장한다.

지능적인 로드밸런싱 기술을 적용해 네트워크 성능을 극대화하며, 멀티코어에 최적화된 설계로 안정적인 성능을 구현하며, 존 기반 정책으로 보안 정책 효율성을 높인다.

가상머신의 엑스게이트 OS를 포팅해 클라우드 망 내에서도 차세대 방화벽 기능을 이용할 수 있게 한다

글로벌 서비스 사업자부터 SOHO까지 지원

국내 네트워크 보안 시장에서 포티넷이 1, 2위를 다투는 강력한 경쟁력을 보이고 있다. 비용 효율적이고 관리가 편하며 다른 솔루션과 통합이 유연한 포티넷 차세대 방화벽 '포티게이트(FortiGate)'는 소규모 사무소부터 글로벌 서비스 사업자, 운영기술(OT) 환경까지 지원하는 다양한 제품군을 갖추고 있다.

포티게이트는 맞춤형 ASIC 아키텍처를 통해 업계 최고의 성능과 안정성, 트래픽 복호화 기능을 제공한다. 경쟁사 동급 방화벽보다 36배 우수한 성능, 사이버 레이팅 평가 보안 효율성 99.88% 획득 등의 검증된 기술을 기록하고 있다.

포티게이트는 포티매니저(FortiManager)를 통해 하이브리드 메시 방화벽을 구성할 수 있다. 포티매니저는 포티게이트, 시큐어 SD-WAN, 시큐어 WLAN/LAN, 유니버설 ZTNA 등 엔터프라이즈 네트워크를 모두 포괄하는 포티넷의 중앙 집중식 관리 솔루션이다.

단일 벤더 SASE 솔루션 '포티SASE'와 통합돼 하이브리드 네트워크 전반에서 일관된 보안, 관리, 분석을 제공한다.

'차세대 방화벽'이라는 용어를 처음 만들고 시장을 개척해 온 팔로알토 네트웍스는 방화벽에 인라인 머신러닝 기능을 탑재해 지능형 우회 공격까지 효과적으로 차단한다. 시그니처에 없는 공격도 10초 이내에 시그니처로 만들어 배포함으로써 실시간에 가까운 선제방어가 가능하다.

고성능 어플라이언스 'PA 시리즈'부터 클라우드 NGFW, 클라우드·가상환경을 위한 'VM 시리즈', 클라우드 네이티브를 위한 'CN 시리즈'까지 다양한 포트폴리오를 갖추고 있다.

이를 통해 엔터프라이즈 네트워크는 물론이고 클라우드, IoT, 커넥티드 디바이스 전반에서 머신러닝 기반 가시성을 보장하며, AIOps를 구현할 수 있게 하고 높은 ROI를 실현한다.

방화벽의 대명사라고 할 수 있는 체크포인트는 방화벽 성능을 선형적으로 높이는 '퀀텀(Quantum)' 솔루션으로 투자를 보호하면서 고성능 보안 요구에 대응할 수 있게 한다. 퀀텀은 사용자, 클라우드 앱, 클라우드 자산, 데이터, 게이트웨이, 퍼블릭·프라이빗 클라우드까지 통합 관리해 보안운영센터(SOC) 업무를 줄인다.

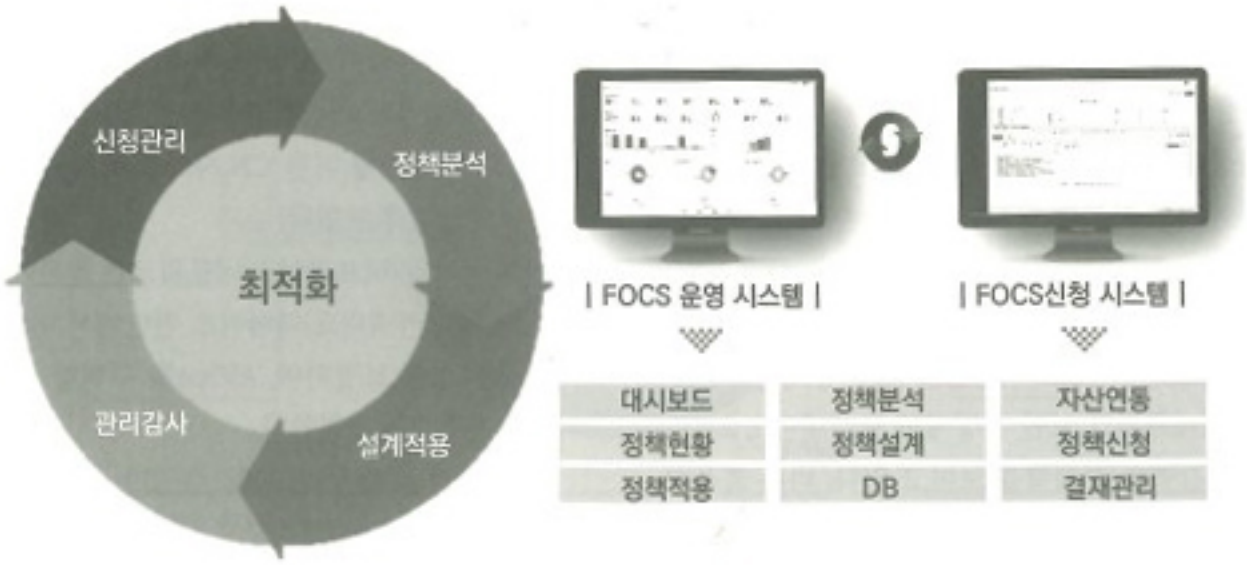
글로벌 위협 인텔리전스와 뛰어난 샌드박스 기능으로 위협의 선제방어부터 감염 후 피해 확산까지 막을 수 있다. 제로데이 공격 방어를 위해 콘텐츠 무해화(CDR) 기능을 적용, 악성코드 없는 안전한 파일만 사용자에게 전달한다.

자동화된 방화벽 정책관리 필수

방화벽의 활용도가 무한 확장되면서 방화벽 관리 문제가 크게 불거지게 됐다. 특히 방화벽 정책 문제로 비즈니스가 중단되는 사고까지 발생하면서 방화벽 정책관리 자동화 솔루션이 필수가 됐다.

방화벽 정책관리 솔루션은 다양한 이종 방화벽을 연동해야 하는데, 비표준 기반으로 설계된 오래된 방화벽이나 일부 국산 방화벽은 연동이 쉽지 않다. 그래서 방화벽 정책관리 솔루션 시장에서는 토종 솔루션이 점유율을 높이고 있다.

<그림 2> 벨로크 FOCS 정책 최적화 프로세스



유넷시스템즈가 제공하는 '에니몬에프엠(AnymonFM)'은 특허받은 정책분석 기술 '피밸리데이터(Pvaildator)' 검증모듈을 사용해 방화벽 정책 이관 시에도 중단이나 장애 없이 최적화된 정책을 유지할 수 있게 한다.

방화벽 추가 혹은 업그레이드 시 정책 이관이 자유롭지 않아 비즈니스 중단 우려로부터 자유롭지 못했는데, 에니몬에프엠의 피밸리데이터를 이용하면 원본과 이관된 방화벽의 정책과 객체 정보를 비교하고 안전하게 운영할 수 있다. 더불어 AI를 적용해 중복정책을 최적화한다.

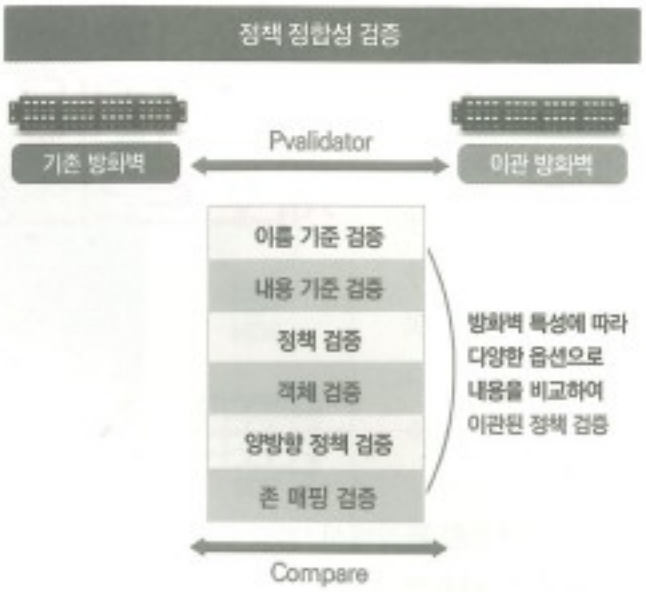
벨로크의 '팍스(FOCS)'는 금융·공공기관 등에 공급되면서 기술력과 안정성을 인정받고 있다. 팍스는 보안관리 동향을 고려해 고객이 필요로 하는 방화벽 정책을 통합 관리한다. 방화벽 관리자 업무 부담을 줄이면서 대규모 방화벽을 효율적으로 관리할 수 있게 한다.

에스에스앤씨가 국내에 공급하는 'FPMS'는 국내 여러 글로벌 제조사에서 안정적으로 운영하고 있는 솔루션으로, 방화벽 운영 효율성을 높인다. 방화벽 정책에서 컴플라이언스 등을 확인해 보안성을 강화하며, 퍼블릭 클라우드와 이기종 방화벽 지원 기능을 제공한다.

통합보안관리 시스템(OASIS)와 함께 사용하면 보다 원활한 정책관리가 가능하다. OASIS는 운영 중인 모든 보안 솔루션의 효율적인 보안관리, 결재를 자동화한다. 이 시스템은 향후 보안 포털의 기반이 될 수 있다.

자동화된 정책 분석·정합성 기술로 방화벽 정책 최적화

유넷시스템즈의 방화벽 정책 관리 자동화 솔루션 '애니몬에프엠(AnymonFM)'은 이기종 방화벽 정책 분석과 최적화를 통한 통합관리를 제공하며, 신규정책 입력 시에 정책결재와 푸시를 자동으로 해준다. 특허받은 정책 분석 기술을 탑재했으며, 2팩터인증(2FA) 기능을 통해 원격·재택근무 시에도 안전하게 솔루션에 접근할 수 있다.



자체 개발 정책 검증 모듈로 정책 이관·검증 최적화

방화벽 정책 관리는 네트워크 보안을 유지하고 규정을 준수하며, 효율적인 트래픽 관리를 위해 필수적인 솔루션이다. ISMS-P 인증심사 시에도 '최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립 이행하고 정책적용 현황을 관리해야 한다'라고 명시하고 있다.

방화벽 정책 관리를 제대로 하지 못하면 치명적인 보안 사고를 겪을 수 있지만, 관리자의 수작업으로는 복잡한 정책 관리를 제대로 수행하지 못한다. 방화벽 관리자는 단순 반복적인 신규 정책을 적용하는 것 만으로도 일과의 대부분을 사용하고 있으며, 정책 중복, 충돌, 만료된 정책 관리, 침해대응 등 중요한 업무에는 거의 시간을 할애하지 못한다.

최신 정책 업데이트, 새로운 방화벽 교체 등으로 인한 방화벽 정책 이관 문제도 심각하다. 방화벽 정책 이관 시 누락이나 변경 없이 방화벽 정책이 안전하게 이관됐다는 사실을 확인하기 쉽지 않다.

애니몬에프엠은 자체 개발한 정책 정합성 검증 기술 '피밸리데이터(Pvaildator)'를 이용해 원래 정책과 이관된 정책, 객체정보 비교할 수 있게 한다. 정책이나 객체 비교 시 이름 기준 또는 내용 기준으로 옵션화해 검증할 수 있으며, 인터페이스나 존의 명칭이 다를 경우에도 매핑정보를 이용해 검증할 수 있다.

유넷은 정책 정합성 검증 기능을 별도 모듈화해 공급, 활용 사례를 다양하게 만들 계획이다. 방화벽 제조사와 협력해 고객 방화벽 업그레이드와 교체 시 활용하며, 기존 솔루션 영업도 지역이나 산업군 특화 채널사 등을 활용해 마케팅을 강화할 계획이다.

정책 푸시 디바이스팩으로 활용 사례 다각화

애니몬에프엠은 기존 기술을 고도화하면서 정책 관리 업무를 개선했다. 정책신청 푸시 모듈을 방화벽 제조사와 제품별 디바이스팩 형태로 바꿔 기존 운영환경을 변경하지 않고 디바이스팩 추가 장착만으로 이기종 방화벽에 대한 추가 연동할 수 있게 했다. 또한 디바이스별로 프로세스가 동작하기 때문에 시스템 안정성 향상은 물론 부하분산, 동시 처리 성능 향상 등 솔루션의 성능을 높여 운영효율화를 기할 수 있다는 장점이 있다.

또한 AI 기술을 방화벽 정책 관리에 접목해 데이터 분석, 머신러닝 학습 기능을 활용할 수 있게 하며, 중복정책 최적화 추천 등의 기능을 이용할 수 있다.

유넷시스템즈 02-2088-3030 www.unet.kr

데이터 암호화

사용 환경 자동 최적화하는 암호화·키관리 기술 필수

데이터 보호 전략을 수립할 때 중요하게 고려해야 하는 점이 '데이터 주권'이다. 데이터 주체가 데이터 라이프사이클 전반을 직접 통제하고 관리할 수 있도록 보장하는 것이다.

그런데 데이터 경제로 접어들면서 데이터 주권을 행사하는 것이 어려워지고 있다. 자신의 데이터를 기업에 제공하면 데이터 보호 책임이 기업으로 넘어가며, 데이터 주체는 자신의 데이터가 어떻게 활용되는지 알 수 없다.

개인정보의 예를 들어 보면, 개인정보 소유주는 자신의 정보를 기업에게 제공하고 그 기업의 서비스를 이용한다. 기업은 개인의 정보를 이용해 영리활동을 하지만, 개인은 정보제공에 대한 대가를 받지 않는다.

또 개인은 기업에 제공한 자신의 데이터가 어떻게 활용되는지 알지 못한다. 기업이 정보관리에 소홀해 유출 사고를 당했을 때 개인이 피해를 입지만, 그에 합당한 보상을 받기 어렵다.

개인정보와 관련된 컴플라이언스도 데이터 보호 전략의 중요한 리스크가 된다. 만일 우리나라 기업에서 정직원으로 근무하는 EU 시민권자가 있을 때, 우리나라 기업이 해당 직원의 민감한 의료 데이터에 접근했다면 EU 시민 데이터의 무단접근으로 GDPR 위반이 될 수 있다. 자사 소속 직원이라고 해도 동의받지 않은 개인 데이터 접근은 규제사항이다.

클라우드로 데이터 주권 보장 어려워

기업이 소유한 데이터라 해도 데이터 주권을 보장받기 어렵다. 클라우드 스토리지에 데이터를 저장한 경우를 가정해 보면, 클라우드 스토리지 사업자는 자사 인프라의 안전성과 복원력 향상을 위해 자체 백업 센터를 운영하면서 만일의 사고에 대응한다. 이 백업센터는 클라우드 서비스 사업자(CSP)가 자사 서비스 연속성을 위해 운영하는 것이기 때문에 CSP의 책임 하에 있다.

CSP가 운영하는 백업센터에 침해가 발생하고 데이터가 유출됐다면, CSP가 그 책임을 져야 한다. 그런데 실제로 피해를 보는 것은 해당 스토리지 서비스를 이용한 기업이다.

CSP가 피해보상을 한다 해도 2차, 3차 공격을 막

데이터 보호 솔루션 선택 시 고려 사항

지속적으로 운영 부담을 줄일 것

대부분의 조직이 데이터 보호 전담 조직이나 인력을 충분히 두지 못한다. 대부분의 경우 3~5명의 전담인력으로 조직을 구성하거나 다른 업무와 병행하도록 한다. 따라서 데이터 보호 플랫폼은 운영 인력의 업무 복잡성을 높이지 않으면서 편리하게 정책을 생성하고 미리 정의된 템플릿과 워크플로우를 쉽게 사용할 수 있어야 한다.

데이터 사용 중 데이터 보안 통제를 적용할 것

데이터 보호를 위해 데이터 사용을 지나치게 제한해서는 안 된다. 데이터 접근제어, 데이터 유출방지(DLP), 데이터 마스킹과 익명화, 암호화, 권한관리와 토큰화 등을 적절하게 사용해 데이터의 원활한 사용을 보장하면서 적절하게 보호한다.

보안 수준이 보장된 공급업체를 선택할 것

최근 보안 솔루션 기업이 해킹당해 고객들까지 연쇄적으로 피해를 입는 일이 늘어나고 있다. 따라서 보안 수준을 입증할 수 있는 솔루션 공급업체를 찾는 것이 중요하다. SBOM·SCA 보고서를 제공하거나 제품 취약점 대응을 위한 사고대응팀을 운영하는 공급업체를 선택하는 것이 좋다.

(자료: 포레스터)

지 못한다. 후속 공격이 CSP의 침해사고로 인해 발생했다는 사실을 입증하기 어렵다.

CSP 혹은 CSP가 관리하는 다른 고객의 법적 문제로 인한 피해도 발생할 수 있다. 해외 클라우드 리전에 데이터를 저장하고 운영하는 중, CSP가 법적인 문제에 걸려 클라우드 저장 데이터가 수사대상이 됐을 때, 사건과 상관없는 조직의 데이터까지 수사 당국에 넘어갈 가능성이 있다.

클라우드 리전이 위치한 국가와 고객의 국가가 다르며, 정보보호 및 개인정보보호 관련 규제가 충돌할 경우 컴플라이언스로 인한 갈등도 발생할 수 있다.

암호화의 핵심, 키관리

암호화 데이터를 안전하게 보호하면서 데이터 주권을 지키기 위해 강력한 키관리가 필요하다. 암호화 데이터는 키가 있어야 접근할 수 있으며, 키에 대한 접근권한을 가진 사람만이 키를 이용해 암호화 데이터를 풀 수 있다.

공격자가 데이터를 유출한 후 이를 공개하려 할 때 암호화 키가 없거나, 키가 있어도 권한을 훔치지 못했다면 유출한 데이터를 공개할 수 없다. 랜섬웨어 악성코드가 데이터를 암호화하려 해도 암호화된 데이터는 정상 권한과 키가 없으면 변경할 수 없기 때문에 데이터를 보호할 수 있다.

수사기관이 수사할 때 암호화 데이터와 키를 가져가지 않으면 데이터에 접근할 수 없다. 데이터의 키를 데이터 소유주가 직접 관리하면 CSP가 수사대상이 됐을 때 해당 사건과 관련 없는 데이터를 보호할 수 있다.

특히 클라우드에 암호화해 저장된 데이터는 강력한 키관리를 적용해야 한다. 클라우드 인프라 어느 곳에 데이터가 저장돼 있는지 파악하지 못해도 키가 있으면 자유롭게 접근할 수 있다. 암호화된 상태로 키를 삭제하면 암호화 데이터를 열 수 없어 영구 삭제된 것으로 간주한다.

아태 기업 62%, 키관리 시스템 5개 이상 사용

키관리의 중요성은 기업·기관의 의사결정권자도 충분히 인식하고 있는 것으로 보인다. 탈레스 조사에서 아시아 태평양 조직의 의사결정권자 96%가 디지털 주권을 위해 전체 데이터를 암호화할 의향이 있다고 답했으며, 키관리의 중요성에 대해서도 동의하고 있었다.

조직은 암호화와 키관리의 중요성을 잘 알고 있지만, 이를 완벽하게 통제하지는 못하는 것으로 나타났다. 디지서트 조사에 따르면 전 세계 조직의 의사결정권자 52%만이 소속 기업이 현재 사용 중인

암호화 키 유형과 특성에 대한 목록을 작성하고 있는 중이라고 답했으며, 응답자의 39%만이 암호화 자산에 우선순위를 두고 있다고 답했다.

기업 전반에 일관되게 적용되는 중앙화된 암호 관리 전략을 갖춘 기업도 거의 없는 것으로 확인됐다. 응답자의 61%는 기업이 특정 애플리케이션이나 사용 사례에 적용되는 제한적인 암호 관리 전략만 있거나(36%), 중앙화된 암호 관리 전략이 없다(25%)고 답했다.

특히 키관리 전략의 부재로 인해 데이터 위협이 높은데, 탈레스 조사에서는 아태지역 조직의 14%만이 클라우드 환경의 모든 키를 관리하고 있다고 답했다.

그 이유는 키관리의 복잡성 때문이다. 응답자의 62%가 5개 이상 키관리 시스템을 사용하고 있으며, 57%는 CSP의 키관리 도구와 암호키를 사용하면서 CSP에 전적으로 의존하고 있다고 답했다.

한국 기업의 88%는 클라우드 업체에서 제공하는 키관리 솔루션에 의존하는 경향 때문에 클라우드 환경의 데이터 주권 우려가 높다고 답했다.

암호화·키관리 복잡도 낮춘 단일 플랫폼 필요

데이터 환경이 복잡해진 만큼 키관리 정책 설정도 복잡해지고 있다. 암호화된 데이터마다 부여되는 키를 자동 관리하기 위한 키관리 시스템(KMS)이 사용된다. 온프레미스와 클라우드, 외부 협력사 등 여러 환경에서 각각 다른 키관리 시스템을 사용하면 KMS를 관리하는 데 많은 인력이 필요하다. 키관리 실패로 인한 데이터 유출·유실 문제도 발생한다.

그래서 KMS를 자동 관리하는 또 다른 플랫폼이 필요하다. 여러 환경에 저장된 각각의 데이터를 암호화한 키, 이 키를 관리하는 시스템과 시스템 접근 사용자를 관리하는 키를 함께 운영해야 한다.

데이터 보호를 위해 암호화·키관리를 적용했는데, 관리 복잡성이 극대화되면서 오히려 가시성이 떨어져 보안 문제를 야기할 수 있다.

탈레스의 '사이퍼트러스트 데이터 시큐리티 플랫폼(CDSP)'은 데이터 관리 및 보호에 대한 모든 요구를 충족하는 단일 플랫폼 기반 기술을 제공해 복잡성을 낮추면서 데이터를 보호한다.

CDSP는 모든 환경, 모든 종류의 데이터를 식별하고, 분류하며, 정책에 따라 암호화, 토큰화, 마스킹 등의 조치를 취한다. 개발자를 위한 데이터 보호 솔루션을 제공하며, 국내 개인정보보호법 준수를 위한 민감데이터 검출과 자동 보호를 지원한다.

고객이 어떤 암호화 플랫폼을 운영하든 상관없이 중앙집중적이며 체계적인 키관리를 지원하는 CDSP는 HSM을 이용한 강력한 키 보호 체계까지 갖출 수 있게 한다. 멀티 클라우드를 위한 다양한 키관리 시스템을 지원, 조직 내부에서 자체적으로 운영하는 키와 클라우드 사업자가 제공하는 키, 외부 독립적인 키관리 솔루션을 통한 키관리가 모두 가능하다.

IoT까지 지원하는 키관리 시스템

유넷시스템즈의 '트러스트KMS(Trust KMS)'는 암호키 생성부터 폐기까지 전체 라이프사이클을 관리한다. HSM을 이용해 암호화 키를 외부에 노출시키지 않고 시스템 내부에서 안전하게 암호화 키를 관리할 수 있다. 또한 중앙집중식 관리 형태로 비용을 절감하며 로그 및 감사를 통한 사후 모니터링 및 분석이 가능하다.

트러스트KMS는 암호키 접근에 대한 에이전트별 접근제어 관리와 키관리자 투팩터 인증을 진행한다. 또한 서버 이중화 구성을 지원하며, 키 파일(key file) 생성 기능으로 통신망 두절 등의 재난 상황 대비에도 용이하다.

급변하는 IoT 환경에도 대비해 경량 알고리즘(LEA, LSH) 및 경량 디바이스에 적용 가능한 형태의

소프트캠프 '실디알엠' 작동 예시

암호키 관리를 제공한다.

트러스트KMS와 직접 통신이 불가능한 IoT 디바이스는 IoT 게이트웨이를 통해 암호키를 전달받을 수 있으며, 전달받은 암호키를 통해 암호화 통신도 가능했다. 또한 윈도우, 리눅스, 유닉스, HP, 솔라리스 등 다양한 플랫폼을 지원해 활용성을 높였다.

비밀관리 솔루션으로 클라우드 자산 보호

키관리 기술과 연관된 기술로 비밀자산(Secret Asset) 관리 솔루션이 있다. 비밀자산은 보안과 관련된 다양한 정보, 자료, 암호화키, 패스워드, API 토큰, 인증서, 기밀 문서, 설정 파일 등의 무형 자산과 그 자산을 관리하는 시스템, 서비스, 소프트웨어 등을 말한다.

기업의 다양한 클라우드 환경 변화에 따라 보안의 형태가 변화하고 있어 클라우드 비밀자산 관리가 필요하다.

동훈아이텍의 클라우드 비밀자산 솔루션 '키르케(Keyrke)'는 비밀 자산의 상호 연관성을 시각화하고, 라이프 사이클을 자동화해 관리·보안 편리성, 비용절감 등의 효과를 제공한다.

클라우드 환경의 자산을 시각화 분석하고, 침해 사고 시 신속하게 대응하며, 보안 대상을 자동화로 관리한다.

이 솔루션은 ISMS-P, CSAP, ISO27001 등 주요 컴플라이언스를 충족하며, 국내 환경에 최적화됐다.

멀티 클라우드 아우르는 데이터 보호 정책

데이터 암호화 정책에서 '사용중인 문서'는 제외되는 경우가 많다. 암호화된 상태로는 업무를 할 수 없으며, 특히 여러 조직과 협업하는 도중에는 암호화가 불가능하다. 그런데 협업 과정에서 중요한 정보가 유출되거나 권한 없는 사용자의 무단 개입으로 변경될 수 있다.

우리나라에서는 문서 암호화를 위해 DRM을 사용하는데, DRM은 클라우드나 외부 조직과 공유할 때 암호화 상태를 유지하기 어렵다.

퍼블릭 클라우드 환경에서는 서비스 사업자마다 다른 암호화와 키관리 정책을 운영하고 있으며, 외부 DRM을 지원하지 않아 클라우드 데이터를 암호화 상태로 유지하는 것이 쉽지 않다. DRM 솔루션이 마이크로소프트365, 구글워크스페이스 등 협업용 SaaS와 호환되지 않아 조직 내외의 다양한 협업환경에서 일관된 데이터 보호가 어렵다.

이에 소프트캠프는 '문서 보안 오케스트레이션(Document Security Orchestration)'이라는 새로운 개념을 제안한다. 문서가 사용되는 환경마다 최적화된 암호화 정책을 자동으로 적용하는 기술이다.

문서 보안 오케스트레이션의 핵심 솔루션인 '실디알엠(SHIELDRM)'은 클라우드 DRM 브로커(Cloud DRM Broker)로, 문서의 보안 정책을 유지하면서 데이터 암호화 기술을 적용할 수 있다.

로컬 PC에서는 DRM으로 보호하고, 마이크로소프트 애저에서는 애저 인포메이션 프로텍션(AIP)의 보안 정책이 자동 적용된다. 구글 클라우드, AWS 등 퍼블릭 클라우드나 기타 다른 프라이빗 클라우드 환경에서도 문서 보안 수준에 따른 보호 정책이 중단 없이 이어질 수 있도록 한다.

제로 트러스트 원칙을 지키면서 문서의 종류, 사용자 행위, 대상 스토리지, 암호화 방식에 따라 유연한 정책 설정과 운영이 가능하다. 암호화 키를 조직 내부에서 관리해 데이터 주권을 확보할 수 있도록 한다.

소프트캠프는 구축형 DRM 솔루션 '도큐먼트 시큐리티(DS)'와 클라우드 스토리지 보안 브로커(CSSB) '실드라이브(SHIELDrive)', 데이터 등급관리와 유통 가시성을 제공하는 '실드인포(SHIELDInfo)'와 보안협업을 지원하는 '실드셰어(SHIELDShare)'도 제공해 중단 없는 데이터 보호가 가능하도록 한다.

성큼 다가온 양자 시대 ... 준비는 미흡

양자 컴퓨터 시대가 성큼 다가오면서, 양자기술에 취약한 암호 문제를 해결해야 한다는 시급성도 높아졌다. 과학기술정보통신부는 전 세계 양자시장이 연평균 20% 이상 높은 성장을 이룰 것이며, 양자암호통신은 이미 초기 상용화 단계에 진입, 4-6년 내 확산될 것이라고 예측했다. 양자센서는 7-9년, 양자컴퓨팅은 10-14년 내에 상용화 시장이 열릴 것으로 예상된다.

양자암호를 이용한 다양한 기술이 속속 상용화되면서 시장 성장에 불을 당기고 있다. 엑스게이트는 양자암호 기술을 탑재한 '퀀텀 VPN'을 공개하면서 양자 보안 시장을 선도하고 있다.

퀀텀 VPN은 IDQ의 양자난수생성기(QRNG)를 탑재해 데이터 송수신 과정에서 암호화와 해독 과정 시 양자난수를 활용해 보안성을 강화한다. 그러면서도 기존 VPN의 고성능을 유지할 수 있어 강력한 보안이 필요한 국가주도 전략사업과 속도가 중요한 금융, 네트워크 인프라와 호환성이 필요한 제로 트러스트 등에 적용될 수 있다. 홈 네트워크 보안을 위한 솔루션으로도 제안된다.

양자시대에 대한 기대와 함께 우려도 크다. 2030년에는 현재 공개키 암호를 해독할 수 있는 양자컴퓨터기술이 상용화될 것으로 예상된다. 그러면 현재 암호체계가 완전히 무력화되며, 암호화로 보호되는 모든 데이터와 통신 체계가 무너진다. 이에 공격자들은 '지금 수집, 나중에 해독(HNDL)'이라는 전략으로 암호화된 상태의 중요 데이터를 수집하고 있다.

디지서트 조사에서 아태지역 IT 리더 19%만이 양자 보안 대비 전략을 갖고 있으며, 대부분은 양자내성암호(PQC) 준비가 거의 돼 있지 않다고 답했다. 응답자의 41%는 PQC 대비 시간이 5년도 남지 않다고 답했는데 30%만이 현재 소속 기업이 PQC 준비 예산을 배정하고 있다고 답했다.

탈레스 조사에서도 경영진은 양자기술에 대한 높은 우려를 보이고 있지만, 양자 시대 준비도는 부족한 편이다. 아태지역 IT·보안 담당 임원 60%가 PQC가 현실 세계에서 실현되고 있다고 답했고, 네트워크 암호 해독을 양자기술 보안 최대 위협 요소로 지목했다.

한편 전 세계에서 PQC 대비를 위한 표준화 준비에 한창인 가운데, 미국 NIST는 2023년 PQC 알고리즘 4종을 공개하고 2024년 최종 확정할 계획이다. 우리나라는 2035년까지 양자내성암호 전환 마스터플랜을 마련한다는 계획을 발표하고, 표준 알고리즘 마련 절차를 진행하고 있다.

강력하고 안전한 키관리 시스템으로 암호 데이터 보호

유넷시스템즈의 '트러스트KMS(Trust Key Management System)'는 하드웨어 보안모듈(HSM)을 이용해 데이터 암호키 생성부터 폐기까지 전체 라이프사이클을 관리한다. 암호 키 관리 보안성을 높이기 위해 국정원 암호모듈검증(KCMVP)을 획득한 암호모듈을 탑재했으며, 독립된 하드웨어 어플라이언스 형태로 제공해 암호키 유출을 원천 차단한다.

IoT에도 최적화된 키관리 제공

데이터 암호화는 키관리가 핵심이다. 암호화의 안정성은 이미 공개된 암호화 알고리즘이 아니라, 암호화 시에 사용하는 암호키가 좌우하기 때문이다. 암호키의 정보가 유출되면 강력한 암호화 알고리즘으로 데이터를 암호화했더라도 복호화 할 수 있어 암호화의 의미가 없어진다. 암호키가 유실되면 암호화된 데이터를 복호화 할 수 없어 데이터가 영구삭제 되는 것과 같다.

이에 암호키관리 시스템(KMS)이 데이터 암호화의 필수다. KMS는 중앙집중식 관리를 통해 모든 키에 대한 강력한 통제를 적용하며, KMS는 HSM 모듈 기능을 겸할 수 있는 보안 솔루션이다.

유넷시스템즈의 '트러스트KMS'는 암호키 보안을 강화하기 위해 암호키 접근에 대한 에이전트별 접근제어 관리와 키 관리자에 대한 2팩터인증(2FA)을 적용한다. 서버 이중화 구성을 지원해 중단 없는 서비스를 지원하며, 키 파일(key file) 생성 기능을 이용해 통신망 두절 등의 재난 상황에도 대비할 수 있게 한다. 안전한 암호키 배포를 위해 암호키 전송구간에 SSL 암호화 통신과 암호키 암호화 전송을 기본으로 한다.

IoT 보안을 위한 경량 알고리즘(LEA, LSH)과 경량 디바이스에 적용 가능한 형태의 암호키 관리를 제공한다. 일반적인 네트워크 환경뿐 아니라 트러스트KMS와 직접 통신이 불가능한 IoT 디바이스에 대해서도 IoT 게이트웨이를 통해 암호키를 전달받을 수 있게 한다. 전달받은 암호키를 통해 암호화 통신도 가능하다. 윈도우, 리눅스, 유닉스, HP, 솔라리스 등 다양한 플랫폼을 지원해 활용성을 높였다.

암호화 보안 컴플라이언스 대응도 완벽

트러스트KMS는 개인정보보호법 제29조(안전조치의무), 전자금융감독규정 제31조(암호프로그램 및 키관리 통제), ISMS-P 2.7.2 암호키 관리부분(암호키의 안전한 생성, 이용, 보관, 배포, 파기를 위한 관리 절차를 수립, 이행하고 필요 시 복구 방안을 마련해야 한다) 등을 사전에 준비할 수 있어 보안컴플라이언스 대응 및 보안감사에도 철저하게 대비할 수 있다.

이외에도 관리의 편리성 제고를 위해 직관적인 웹 UI를 제공하며, 서버의 상태를 한눈에 확인할 수 있는 시스템현황조회, 에이전트 및 키관리, 서비스 및 감사로그 통계 및 분석 기능 등을 제공한다.

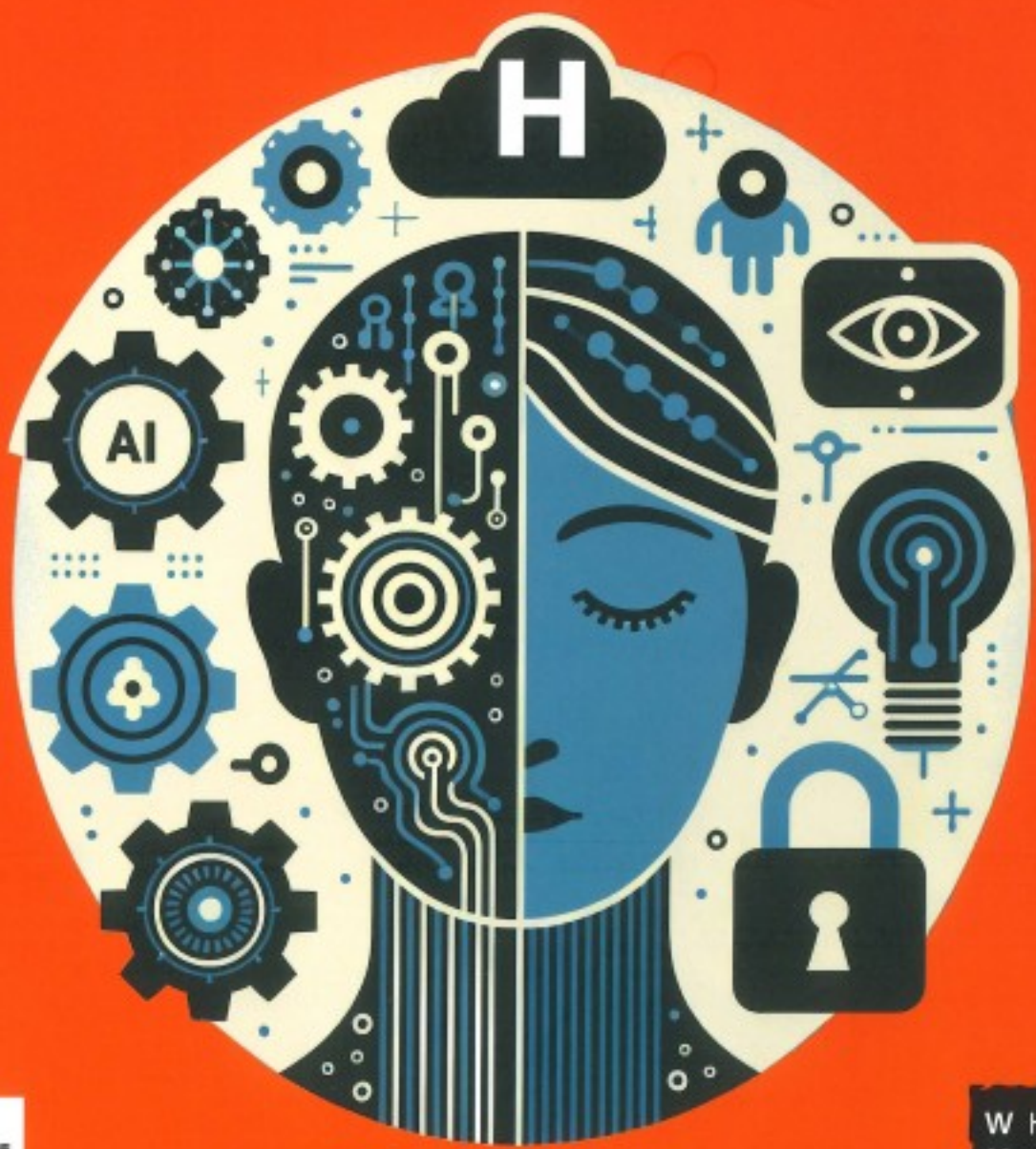
트러스트KMS는 2017년부터 제1금융권에 공급돼 안정성을 인정받아 고객에게 꾸준한 관심을 받아 오고 있으며, 지속적인 금융권 마케팅 및 타 산업부분으로의 영업확대를 통해 시장 지배력을 높이고 있다.

유넷시스템즈 02-2088-3030 www.unet.kr

제로 트러스트
핵심 철학

사람 중심 보안

SECURITY GUIDE 2024 vol. 19



ISBN 979-11-88051-08-3

WHASAN MEDIA