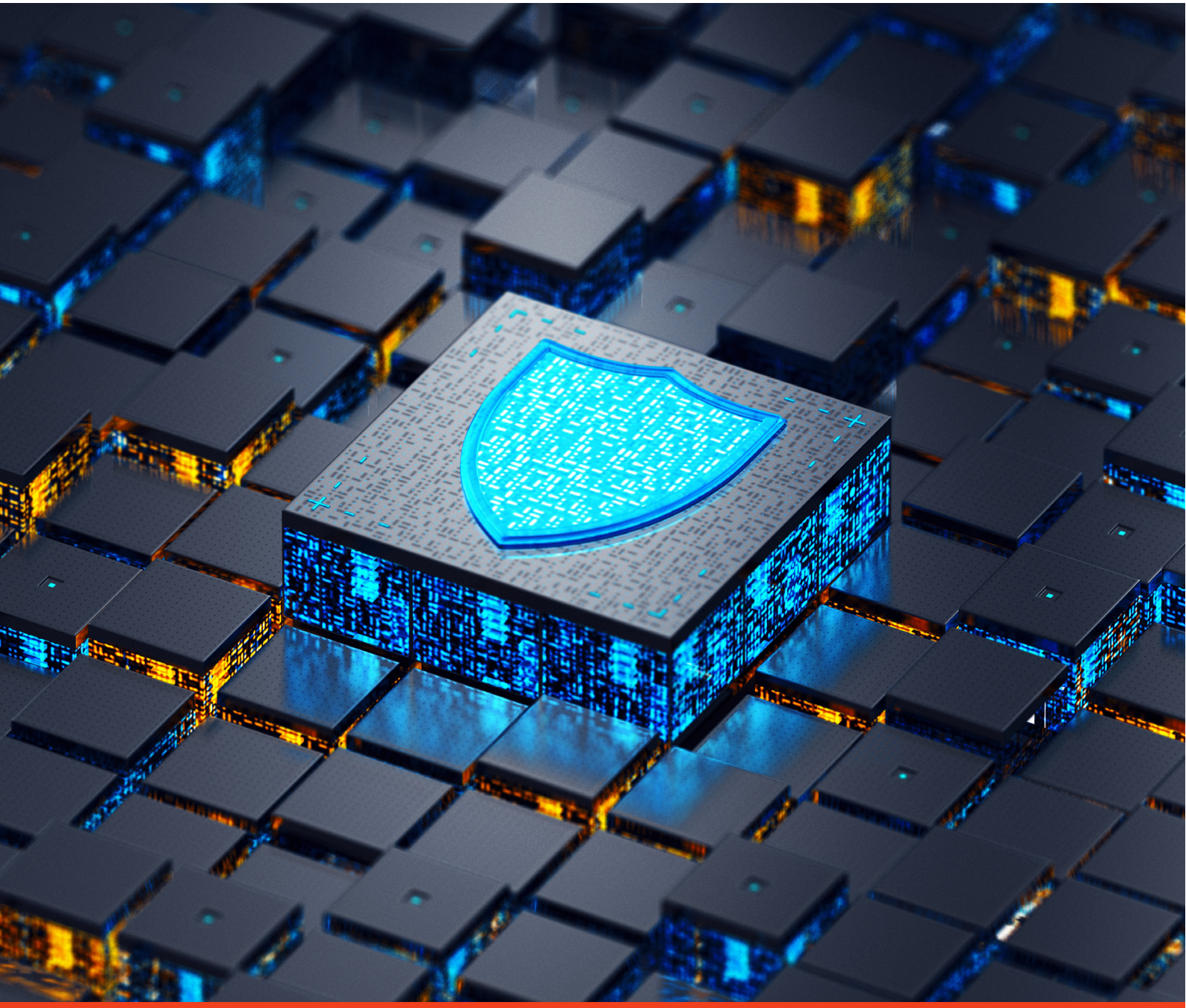
IT WORLD

MENLO SECURITY

Tech Summary | Gitple

# "혁신을 촉진하는 효율적인 망분리"

## 웹 격리 기술을 이용한 망분리 전략 가이드



# “혁신을 촉진하는 효율적인 망분리”
## 웹 격리 기술을 이용한 망분리 전략 가이드

**김성래** | 멘로시큐리티 코리아 지사장

2010년 초반 금융기관의 대형 보안 사고가 연달아 터지면서 2013년 금융기관의 망분리가 법률로 제정됐다. 금융감독원의 금융전산 망분리 가이드라인에 따르면, 내부통신망과 연결된 내부 업무용 시스템은 인터넷 등의 외부 통신망과 분리해야 한다. 인터넷에 접속하는 사용자 PC가 해킹되면 이를 통해 해커가 금융기관의 내부망에 접속할 수도 있기 때문이다. 기술적으로는 가상화를 이용해 내부 업무용 PC와 인터넷용 PC를 분리한 VDI 기반 망분리가 확산됐다.

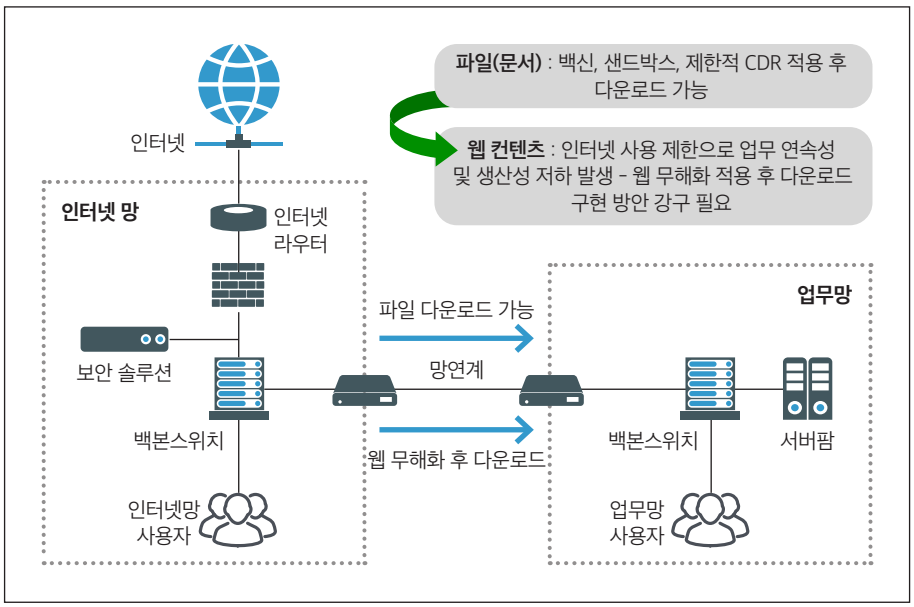
이렇게 적용된 지 10년이 된 금융 전산 망분리 규제가 올해부터 일부 완화됐다. 연구 개발 목적의 시스템은 물리적 논리적 망분리 대신 대체 정보보호 통제를 적용할 수 있게 된 것이다. 비중요 업무의 SaaS 이용도 망분리 조치의 예외가 적용된다. 이외에도 클라우드 활용 시 이용 절차를 간소화했다. 이번 조치는 핀테크 스타트업을 중심으로 제기된 기존 망분리에 대한 문제 의식이 크게 작용했지만, 기업의 비즈니스 환경 변화에 따라 보안 대응 역시 변화해야 한다는 것을 잘 보여준다.

생산성 및 효율성 향상을 위한 전쟁을 치르고 있는 기업 환경은 코로나19 팬데믹을 계기로 빠르게 변화하고 있다. 재택근무의 확산으로 사용자 업무 환경은 극히 분산되어 원격 협업이 보편화됐으며, 클라우드 서비스와 SaaS 사용은 급격하게 증가했다. 보안 위협 역시 다양한 기술로 여러 계층을 전방위적으로 공격하는 방식으로 진화하면서 기존 데이터센터 중심의 보안 대응은 한계를 드러내고 있다. 그리고 망분리 시스템은 이런 변화와 혁신의 모든 측면을 거스르는 대표적인 기술이 됐다.

### “클라우드를 외면하는” 망분리 시스템의 한계

망분리는 출발부터 보안을 최우선 순위에 두면서 상당한 대가를 치러야 하는 기술이었다. 특히 단순 도메인 중심의 망분리를 적용해 업무 생산성과 효율성이 크게 떨어진다. 내부망과 외부망을 분리하면서 데이터는 내부망에 있고 분석 도구는 외부망에 있어 데이터 활용도는 현저히 떨어진다. 하지만 2023년 현재 망분리의 가장 큰 문제는 바로 혁신을 저해한다는 점이다.

**망분리 환경의 복잡한 인터넷 이용 구조**




클라우드의 시대에 IT 혁신은 대부분 클라우드에서 나온다. 최첨단 디지털 기술 개발의 선봉에 있는 곳이 대형 클라우드 서비스 업체일뿐만 아니라 협업 솔루션은 물론, ERP부터 CRM이나 데이터 웨어하우스, 고급 분석 등 비중이 큰 엔터프라이즈 애플리케이션까지 모두 클라우드 기반 솔루션으로 전환하고 있다. IT 솔루션 업체의 연구 개발 노력도 클라우드를 중심으로 이루어지고, 새로운 기술과 서비스는 모두 클라우드에서 시작된다. 한정된 자원과 인력으로 자체 개발한 애플리케이션으로는 경쟁에 뒤처질 수밖에 없다.

업무망에서 인터넷 사용을 제한하는 것은 업무 연속성 측면에서 치명적인 결과를 가져온다. 인터넷이 필요한 업무는 인터넷망에 연결된 PC를 이용하면 된다고 쉽게 생각할 수 있지만, 필요한 문서 파일 하나라도 업무망으로 가져오려면 복잡한 과정을 거쳐야 한다. 망연계 시스템을 거쳐야 하고, 콘텐츠를 다시 검사해 위협 요소를 제거하는 이른바 '무해화' 과정을 거쳐야 한다. 이메일은 더욱 민감한데, 인터넷망과 업무망 각각을 위한 메일 서버를 구축하기도 한다. 업무망으로 전달되는 모든 이메일을 이미지로 변환해 보여주고 실제 내용은 인터넷망에서 다시 확인해야 하는 환경도 있다. 구축 및 운영에 추가 비용이 들 뿐만 아니라 사용자 경험과 생산성까지 적지 않은 타격을 받는다.

## 하락하는 업무 생산성과 의심스러운 보안

망분리를 적용해도 인터넷망과 내부망 간의 문서 공유를 위한 파일 이동은 불가피하다. 이 때문에 망분리를 통해 얻고자 하는 보안성마저 확실하지 않다. 망연계 시스템의 샌드박스에 적용할 수 있는 보안 기술에 한계가 있기 때문이다. 보통 알려진 침해 지표 기반의 탐지 기능을 수행하는데, 탐지 우회 기능을 갖춘 악성코드 공격에는 무방비 상태가 되기 쉽다.

웹 위협은 빠르게 진화한다. 웹 브라우저를 공격 벡터로 활용하고 다양한 기술을 이용해 보안 시스템의 다계층 탐지를 회피하는 이른바 HEAT(Highly Evasive Adaptive Threat)는 안티바이러스나 샌드박스의 정적 동적 콘텐츠 분석을 회피하는 것은 물론, 개인 이메일과 소셜 미디어를 이용해 악성 콘텐츠를 전송하고 임시 도메인을 사용해 침해 지표 탐지 방식을 회피한다. 심지어 실제 사이트와 거의 동일한 웹 사이트로 사용자 탐지까지 회피한다.

더구나 보안 역시 클라우드의 시대를 부인할 수 없다. 사실 인프라가 외부에 있고 서비스가 외부에 있는데 보안 솔루션을 계속 내부에 둘 수는 없다. 이미 방화벽이나 침입탐지시스템 같은 전통적인 보안 솔루션은 물론, EDR이나 XDR 같은 진화된 보안 기술은 모두 클라우드를 기반으로 한다. 보호해야 할 대상이 클라우드에 더 많기 때문이다. 사실 기업이 자체 개발한 애플리케이션이나 시스템이라도 결국 트래픽은 인터넷으로 향하게 되며, 이런 트래픽의 안전성 여부를 판단하는 기능은 클라우드에 있는 것이 더 합리적이다.

## 핵심 공격 루트를 차단하는 웹 격리 기술

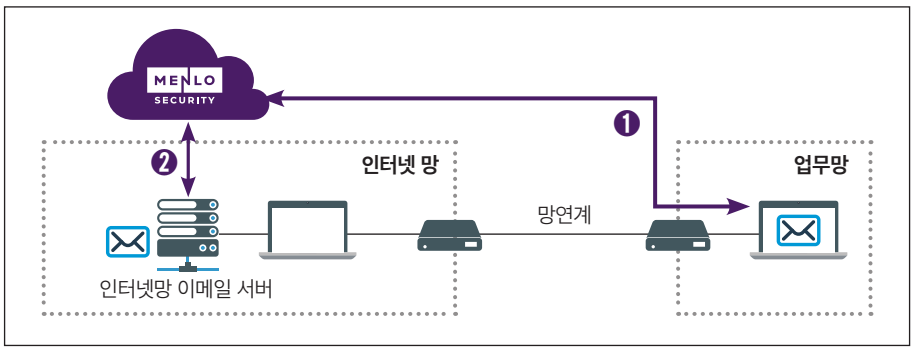
웹 격리 기술(Remote Browser Isolation)은 실질적인 웹 활동은 격리된 가상 브라우저에서 실행하고 사용자에게는 안전한 실행 결과만을 전달한다. 사이버 공격의 90% 이상이 웹과 이메일을 통해 이루어진다는 점에 주목한 기술로, 사용자의 실제 웹 브라우저는 인터넷과 직접 접속하지 않기 때문에 웹을 통해 침투하는 악성코드를 차단하는 데 매우 효과적이다.

특히 웹 격리 기술은 사용자 경험에 아무런 영향을 미치지 않기 때문에 업무 생산성을 높일 수 있다. 사용자는 기존 웹 브라우저 환경과 동일한 방식으로 웹 서핑이나 이메일 등을 사용하지만, 트래픽은 멘로시큐리티와 같은 웹 격리 솔루션 업체의 격리 플랫폼인 가상 브라우저로 먼저 전달된다. 실제로 외부 웹과 트래픽을 주고받는 시스템은 이 가상 브라우저이다. 격리 플랫폼은 웹 콘텐츠에서 실행 가능한 컴포넌트를 제거하고 웹 리소스를 변경하고 재작성하는 CDR(Content Disarm and Reconstruction) 기능을 수행한다.

가상 브라우저는 악성 스크립트 및 파일을 제거한 안전한 렌더링 정보만 사용자 브라우저에 전달한다. 사용자 브라우저는 격리 플랫폼으로부터 DOM 처리 명령 정보만 다운로드하고, 격리 플랫폼은 사용자 브라우저로부터 키보드와 마우스의 입력 정보만 수신한다.

사용자가 의심스러운 웹 사이트를 방문해도 악성코드는 가상 브라우저에서 걸러지기 때문에 사용자에게 악성코드가 전달될 가능성은 전혀 없으며, 사용자는 망분리 환경의 VDI보다 빠르고 안전한 업무 환경을 확보할 수 있다.

**업무망과 인터넷의 안전한 연결을 지원하는 웹 격리 기술**




이메일 환경 역시 웹 격리 기술을 적용할 수 있다. 업무망 사용자는 업무망 이메일 서버가 아니라 격리 플랫폼을 통해 안전하게 인터넷망의 이메일 서버에 접속할 수 있으며, 격리 플랫폼은 웹 접속과 마찬가지로 악성 콘텐츠를 제거한 안전한 이메일을 사용자에게 전달할 수 있다. 악성 링크는 안전하게 재작성된 페이지를 다운로드하고 악성 첨부 문서 역시 문서 내용을 프리뷰 형태로 사전에 확인할 수 있다. 필요하면 문서를 안전한 PDF로 변환해 다운로드할 수도 있다.

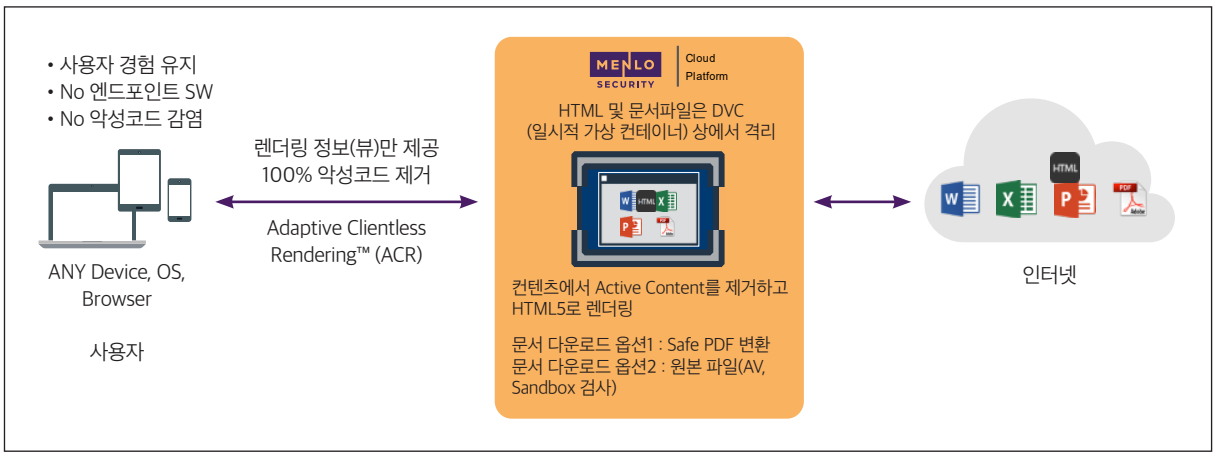
태생부터 클라우드인 웹 격리 기술의 특성은 보안성과 편의성도 한층 높여준다. 사용자별 일회용 컨테이너(Disposable Virtual Container, DVC)를 이용하면, 사용자가 브라우저를 닫거나 입력 없이 대기 중일 때 메모리에서 제거되기 때문에 저장 데이터에 대한 보안 문제를 미연에 방지한다. 또한, 클라우드 서비스의 특성 상 사용자 디바이스의 종류나 위치에 관계없이 웹 격리 서비스를 제공할 수 있으며, 사용자가 급증해도 즉각 대응할 수 있다.

## 제로 트러스트 인터넷으로 망분리의 현실적인 대안 제시

망분리가 인터넷을 통해 업무망으로 악성코드를 비롯한 웹 위협이 침투하는 것을 방지하기 위한 것이라는 점에서 웹 격리 기술은 망분리 도입을 통해 얻고자 하는 주된 목적을 더 효과적으로 달성할 수 있다. 물론 망분리는 PC 전체를 인터넷과 격리한다는 점에서 웹 격리 기술이 망분리를 완벽하게 대체할 수는 없다. 하지만 적지 않은 도입 및 관리 비용이 드는 망분리 시스템에 대한 의존도를 줄임으로써 비용을 절감하는 것은 물론, 업무 생산성을 해치지 않는 방식으로 더 많은 사용자가 안전한 업무 환경을 이용할 수 있다.

예를 들어, 현재 가장 많이 활용되는 망분리 방식인 논리적 망분리는 VDI(Virtual Desktop Infrastructure) 솔루션을 이용하는데, 사용자당 라이선스 비용부터 VDI 서비스를 위한 인프라 구축까지 적지 않은 비용이 든다. 이 때문에 논리적 망분리를 조직의 전체 사용자에게 적용하는 경우는 드물고, 개인 정보를 취급하는 등 반드시 망분리 환경이 필요한 사용자 외에는 부서별로 적절한 비율로 할당해 공유하는 방식으로 활용한다. 당연히 사용자의

**제로 트러스트 인터넷을 구현하는 웹 격리 기술**




인터넷 활용은 매우 번거롭고 불편한 환경이 될 수밖에 없다.

웹 격리 솔루션은 규제에 의해 반드시 VDI를 적용해야 하는 사용자를 제외하고 전체 직원에게 적용해 업무 생산성과 보안을 모두 만족하는 환경을 구현할 수 있다. 사용자당 라이선스 비용도 VDI 솔루션의 1/10~1/20 수준이며, 전 직원이 업무를 위해 인터넷을 사용하는 환경을 운영하더라도 망분리 시스템의 비용을 50% 이상 절감할 수 있다.

망분리 시스템에 새로운 시스템을 추가해도 복잡성을 염려할 필요는 없다. 웹 격리 솔루션은 클라우드 기반의 SaaS 서비스이기 때문에 핵심 처리 기능은 모두 서비스 업체의 데이터센터, 즉 클라우드에 있다. 조직은 사용료만 지불하면 바로 배치할 수 있으며, 사용자는 웹 트래픽에 대한 프록시 설정만 변경하면 된다.

더 나아가 웹 격리 기술은 외부 인터넷의 잠재적 위협에 대한 강력한 방어책을 제공한다. 웹 콘텐츠의 위험성을 100% 정확하게 판별하기는 어렵다. 어제 정상이었던 콘텐츠가 오늘은 악성 콘텐츠일 수 있다. 웹 격리 기술은 어떤 웹 콘텐츠도 신뢰하지 않고 모두 무해한 콘텐츠로 변환해 사용자에게 전달하기 때문에 웹 트래픽의 보안성을 극대화할 수 있다. 또한 막대한 트래픽을 분석하고 위험한 사이트나 파일을 탐지하는 데 드는 인력과 시간도 절감할 수 있다. 이를 통해 망분리를 대체 및 보완하는 것은 물론, 일종의 제로 트러스트 인터넷 환경을 구축할 수 있다.

## 선도적인 웹 격리 플랫폼의 조건

2013년 설립된 멘로시큐리티(Menlo Security)는 JP모건 체이스나 HSBC 같은 대형 금융 고객을 확보하며 전 세계 웹 격리 시장을 선도하고 있다. 최근에는 미국 국방부와 350만 명 규모의 웹 격리 서비스 공급 계약을 체결해 업계의 주목을 받기도 했다. 삼성전자, SK하

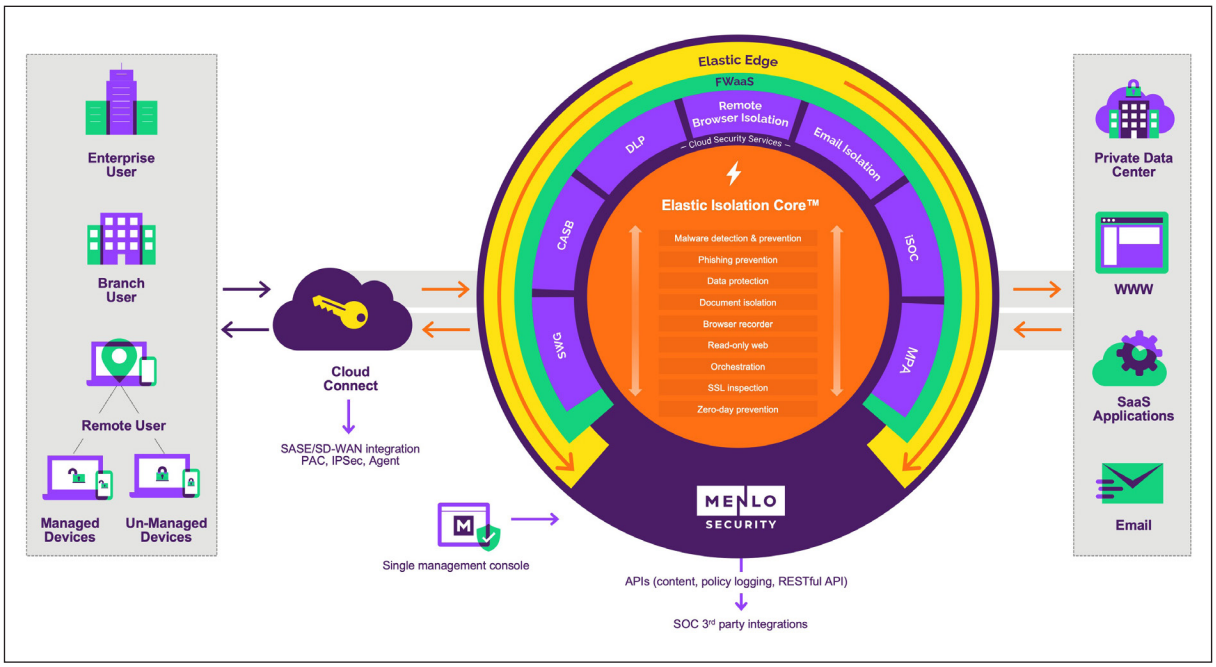
이닉스를 포함해 전 세계 톱 3 반도체 기업 역시 멘로시큐리티의 솔루션을 활용하고 있다.

멘로시큐리티 웹 격리 솔루션인 Menlo Security RBI(Remote Browser Isolation)는 인터넷 악성코드를 막기 위해 제로 트러스트 전략을 구현하는 데 필요한 가시성과 통제 역량을 제공한다. 오늘날 위협 인자는 전통적인 보안 방어책을 우회하고 최신 브라우저의 표준 기능을 이용해 악성코드를 배포하는 HEAT 공격으로 웹 브라우저를 노린다. 악성코드가 방어책을 악용하는 상황에서 위협을 파악하기보다는 브라우저 격리를 통해 모든 웹 트래픽이 클라우드 기반 원격 브라우저를 먼저 통과하도록 해 안전한 콘텐츠만 최종 사용자에게 전달되도록 하는 것이 더 효율적이다. Menlo Security RBI는 모든 콘텐츠가 악성 콘텐츠라고 가정하고 그에 맞게 처리하는 제로 트러스트 원칙을 채택하고 있다.

브라우저 격리와 함께 멘로시큐리티는 모든 보안 웹 게이트웨이 기능을 단일 클라우드 네이티브 플랫폼에 통합했다. SWG(Secure Web Gateway)뿐만 아니라 CASB(Cloud Access Security Broker), DLP(Data Loss Prevention), 프록시, FWaaS까지 통합해 확장된 API와 정책 관리, 리포팅, 위협분석을 위한 단일 인터페이스를 제공한다.

멘로시큐리티 클라우드 플랫폼은 독자 기술인 아이솔레이션 코어(Isolation Core)를 기반으로 하며, 아무리 많은 사용자라도 신속하게 온보딩할 수 있는 탄력적인 확장성을 갖췄다. 인력이나 트래픽 규모의 변동이 심하더라도 별도의 용량 계획이나 복잡한 환경 구성없이 바로 배치할 수 있다. 사용자는 웹 기반의 정보와 업무 생산성 툴을 아무런 장애없이 이

**멘로시큐리티의 포괄적인 클라우드 보안 플랫폼**



용할 수 있다.

사용자가 기존 방식대로 업무를 수행하는 한편, 관리자는 감염된 웹 사이트부터 파일 업로드와 다운로드는 물론 알려지지 않은 위협까지 차단할 수 있는 유용한 사용 정책을 수립할 수 있다. 사용 정책은 사용자와 부서, 파일 종류, 웹 사이트 분류, 클라우드 애플리케이션에 따라 언제 콘텐츠를 차단할지, 읽기 모드만 허용할지, 원본 콘텐츠를 허용할지 결정할 수 있다.

Menlo Security RBI는 이런 작업을 비교할 수 없는 성능과 규모로 수행한다. 100% 네이티브 클라우드 서비스로, 오토 스케일링을 통해 서비스 가용성과 확장성을 극대화했으며, 전 세계 17개 리전에 POP를 보유해 99.9% 이상의 서비스 가용성을 보장한다. 한국 역시 POP 센터를 지원하고 이중화된 데이터센터를 보유하고 있다. 멘로시큐리티는 웹 격리 적용 후 PC 감염이 발생하면 최대 100만 달러를 보상하는 악성코드 제로 보증제를 실시할 만큼 기술에 자신감을 가지고 있다.

## 진화하는 웹 격리 솔루션의 가치

외부 공격자로부터 기업 업무 환경을 지키기 위한 기술은 끊임없이 발전하고 있다. 날로 정교해지는 위협을 탐지하고 차단하기 위한 노력이 계속되는 한편, 위협의 근원인 인터넷과의 격리를 통해 안전한 환경을 확보하려는 시도 역시 진화하고 있다. 현재 망분리 환경에 주로 적용되는 VDI는 가상화 기술로 PC 자체를 인터넷과 격리한다. 애플리케이션 가상화 역시 인터넷과 접속하는 특정 애플리케이션을 격리하는 데 이용할 수 있다.

웹 격리 솔루션, 즉 RBI(Remote Browser Isolation) 기술은 인터넷에 접촉하는 통로인 웹 브라우저를 가상화해 격리하는 개념이다. 외부에 있는 해커를 막으면서 기존 업무 환경에 미치는 영향을 최소화할 수 있다. 이런 장점 때문에 적지 않은 업체가 웹 격리 솔루션과 서비스를 제공한다.

하지만 단순 명료한 웹 격리 기술의 개념을 실제로 구현하는 구현하는 것은 간단하지 않다. 실제 사용자의 업무 환경이 너무나 다양하기 때문이다. 웹 브라우저는 제2의 운영체제라고 해도 과언이 아닐 만큼 다양한 용도로 활용된다. 웹 브라우저를 기반으로 한 기업용 애플리케이션도 헤아릴 수 없이 많으며, 기존의 스탠드얼론 애플리케이션도 웹 애플리케이션으로 전환하고 있다. 오피스 365나 구글 워크스페이스에서 알 수 있듯이 현재 웹 브라우저는 모든 업무 생산성 툴이 동작하는 환경이다. 이런 다양한 업무 환경을 기존 웹 환경처럼 지원하지 않으면 웹 격리 솔루션은 망분리의 대안 기술이 될 수 없을 것이다.

멘로시큐리티는 웹 격리 기술의 선도업체로서 이런 장애물을 누구보다 먼저 누구보다 많이 해결하면서 솔루션을 최적화해 왔다. 끊임없이 변화하는 웹 환경에서 '완성된 솔루션'이란 없다. 멘로시큐리티 역시 웹 격리 환경에서 고객을 확대하면서 수많은 장애물을 넘어왔다. 웹 격리 환경에서 마우스 오른쪽 클릭으로 프린트를 지원하는 것부터 구글 번역 앱을 아무런 불편없이 사용할 수 있도록 지원하는 것까지 수많은 사용자의 패턴을 지원하며 성장해 왔다.

가트너는 이미 2019년에 기업이 모든 공격을 탐지하려는 노력을 중단하고 격리를 통해 공격 범위를 줄여야 한다고 권고한 바 있다. 격리가 웹과 이메일을 통한 위협 노출을 획기적으로 줄여주는 핵심 방어 전략이라고 평가한 것이다.

이제 보안은 모든 기업의 최우선순위에 있다. 하지만 기존 솔루션은 제한적일 뿐만 아니라 사후 대응적이다. 이제 근본적으로 다른 접근이 필요하다. 멘로시큐리티는 독보적인 격리 기반 보안 플랫폼으로 악성코드의 위협을 완전히 제거하면서 생산성을 완벽하게 보호한다. 가장 안전한 제로 트러스트 전략으로 악성 공격을 방어하고 사용자를 방해하지 않고 보안팀의 운영 부담도 없는 솔루션을 찾는 기업에 최상의 선택지가 될 것이다.