

# ENTERPRISE DEFENDER

## 엣지에서의 제로 트러스트 보안



방어 가능한 네트워크 경계는 더이상 존재하지 않습니다. 적어도 우리가 인식할 수 있는 형태로 존재하지 않습니다. 20년 전에 만들어진 보안 및 접속 방식을 현재 환경에 사용하는 것은 적합하지 않고 어떤 경우에는 위험하기도 합니다. 이는 단순히 이론에 불과하지 않습니다. 최근 5년간 일어난 데이터 유출 사고의 발생 건수와 그 규모에서 명백하게 드러납니다. 데이터 유출 사고의 대부분은 네트워크 경계 내부를 신뢰했기 때문에 발생했습니다. 이제는 제로 트러스트 보안을 받아들여야 할 때입니다. 기업 네트워크 내부에 있다고 해서 신뢰하는 것이 아니라 ID, 디바이스, 사용자 컨텍스트에 따라 자동적으로 접속을 제공하는 보안 모델이 필요합니다.

## ENTERPRISE DEFENDER

Enterprise Defender는 Akamai Intelligent Edge Platform을 기반으로 설계되었습니다. 멀웨어 차단, 탄력적인 애플리케이션 접속, 보안, 가속을 하나로 결합한 사용 편의성이 높은 보안 서비스입니다. Enterprise Defender는 하드웨어나 어플라이언스를 추가하지 않고 제로 트러스트 보안 체계를 구축하도록 지원합니다. Enterprise Defender를 적용하면 리스크와 복잡성을 줄이면서 사용자 경험을 개선할 수 있습니다.

## 작동 방식

Enterprise Defender는 Akamai Intelligent Edge Platform을 기반으로 모든 기업용 애플리케이션과 사용자를 안전하게 보호합니다. 성능 저하 없이 보안을 최적화하고 복잡성을 감소시킵니다. 기업이 제어하는 애플리케이션에 안전하게 접속할 수 있도록 하고 기업이 제어하지 않는 애플리케이션에 사용자가 접속할 때 발생하는 리스크를 경감시킵니다.

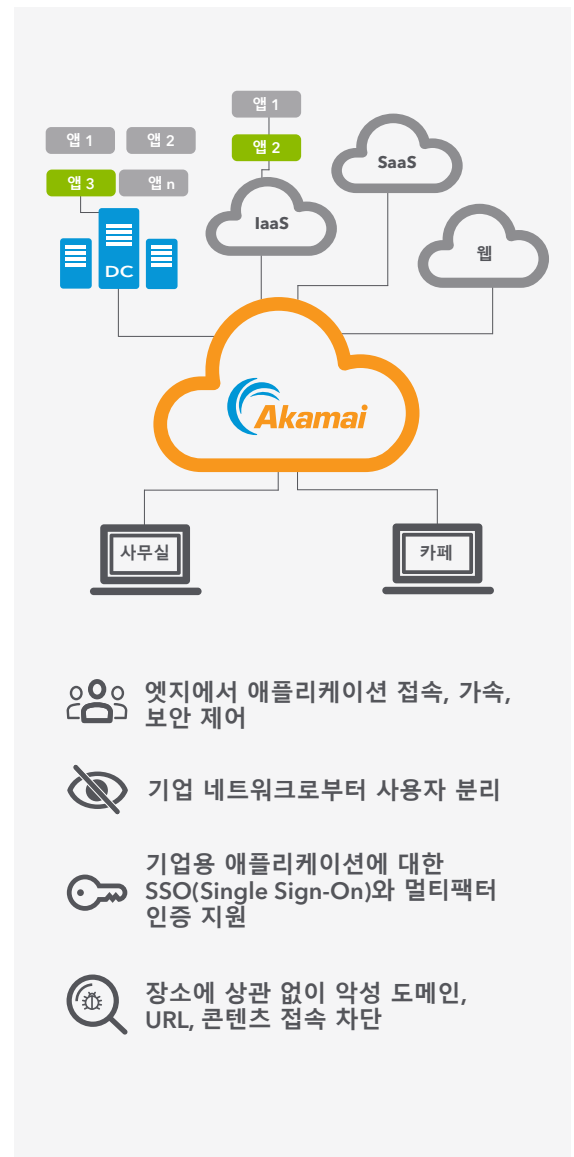
Enterprise Defender의 주요 기능은 다음과 같습니다. 사용자별, 월별로 사용이 가능한 편의성이 높은 서비스입니다.

**멀웨어 방어:** Akamai가 제공하는 Secure Internet Gateway(SIG)는 사용자와 디바이스가 인터넷과 기업이 제어하지 않는 애플리케이션에 안전하게 접속할 수 있도록 지원합니다. 또한 기존에 사용 중인 접근 방식에 가중되는 복잡함 없이 언제 어디서나 사용자 및 디바이스가 인터넷과 제어하지 않는 애플리케이션에 안전하게 접속하도록 지원하는 보안 인터넷 게이트웨이(SIG)를 제공합니다.

**안전한 애플리케이션 접속:** Akamai는 권한이 부여된 사용자 및 디바이스가 기업의 전체 네트워크가 아닌, 필요한 내부 애플리케이션에만 접속하도록 허용합니다. 애플리케이션을 퍼블릭 인터넷으로부터 숨기기 때문에 어떤 사용자도 애플리케이션에 직접 접속할 수 없습니다. Enterprise Defender는 데이터 경로 보호, SSO(Single Sign-On), ID, 애플리케이션 접속, 관리 가시성, 제어 등 모든 기능이 하나로 결합된 서비스입니다.

**WAF(Web Application Firewall):** Akamai는 가장 규모가 크고 정교한 DDoS 및 웹 애플리케이션 공격으로부터 중요한 웹 애플리케이션을 안전하게 보호합니다. Akamai WAF는 강력한 웹사이트 보안 기능을 제공합니다. 업계 최고의 위협 연구팀은 이 기능을 업데이트하고 기업이 진화하는 보안 위협에 대응할 수 있도록 지원합니다.

**애플리케이션 가속:** Akamai는 비용 효율적인 방식으로 애플리케이션을 빠르고 안정적이며 안전하게 전송합니다. 따라서 기업은 인터넷을 통해 비즈니스 애플리케이션을 전송할 때 발생하는 도전과제를 해결할 수 있습니다. 애플리케이션 전송 기능을 포함하고 있는 Akamai Intelligent Edge Platform은 사용자, 클라우드, 온프레미스 워크로드와 아주 가까운 곳에 배치되어 있습니다.



## ENTERPRISE DEFENDER

### 기업이 얻을 수 있는 혜택

- 멀웨어 확산 및 측면 이동(lateral movement) 차단**  
 경계 기반의 네트워크는 네트워크 가시성이 떨어지고 분할이 잘 되어 있지 않기 때문에 멀웨어가 매우 깊숙이 침투합니다. Enterprise Defender는 애플리케이션 접속을 보다 정밀하게 제어하고 위협을 선제적으로 차단합니다. 따라서 멀웨어가 확산되거나 공격자가 다른 워크로드에 접속하는 것을 어렵게 만듭니다.
- 복잡성 감소와 운영 효율성 개선**  
 Enterprise Defender는 클라우드 기반의 보안 솔루션입니다. 유지 관리에 많은 비용이 드는 가상 또는 하드웨어 어플라이언스를 간단한 엣지 보안 서비스로 대체할 수 있습니다.
- 보안 자본지출 및 운영비 절감**  
 보안을 강화하려면 비용이 증가하게 마련입니다. 하지만 CISO나 보안팀이 Enterprise Defender를 사용해 보안을 강화하면 오히려 비용을 절감할 수 있습니다. 클라우드 기반의 간편한 솔루션으로 여러 보안 기능을 통합할 수 있기 때문입니다.
- 가시성 향상 및 유출 탐지 시간 단축**  
 유출 사고가 발생하면 "악성 공격자들이 수 개월 동안 탐지되지 않았다", "악성 공격자들은 네트워크 경계를 통과한 후에 자유롭게 네트워크를 이동할 수 있었다" 같은 표현이 자주 등장합니다. Enterprise Defender는 애플리케이션 접속을 보다 정밀하게 제어하고 DNS 기반의 보안 기능을 제공합니다. 따라서 보다 큰 가시성을 확보할 수 있고 데이터 유출을 탐지하는데 소요되는 시간을 단축할 수 있습니다.
- 내부 데이터 유출 차단**  
 데이터가 악성 공격자의 손에 넘어가면 비즈니스에 심각한 피해를 끼칠 수 있습니다. 개인정보를 적절히 보호하지 못해 벌금이 부과될 수도 있고 지적 재산 또는 전략이 유출되면서 매출이 감소할 수 있습니다. Enterprise Defender는 '최소 권한' 기반의 탄력적인 접속 제어와 DNS 기반의 가시성·보안을 통해 내부 데이터 유출을 차단합니다.
- 디지털 비즈니스 혁신 추구**  
 IT·보안팀은 디지털 혁신의 핵심 파트너가 될 수 있습니다. 하지만 경계 기반의 보안 모델에서는 보안팀이 새로운 클라우드 서비스, 파트너, 고객 모델을 지원하기 위해 기업 경계에 대한 접속을 허용하면 기업의 전체 네트워크에 대한 접속을 허용하게 됩니다. Enterprise Defender는 전체 네트워크에 대한 접속을 허용하지 않습니다. ID와 보안 컨텍스트를 기반으로 일부 애플리케이션에만 제한적으로 접속을 허용합니다. 또한, 악성 도메인, URL, 콘텐츠에 대한 접속을 차단함으로써 사용자가 사무실에 있던 근처 커피숍에 있는지 상관 없이 모든 곳에서 일할 수 있는 기업 문화를 가능하게 만듭니다.



Akamai는 전 세계 주요 기업들에게 안전하고 쾌적한 디지털 경험을 제공합니다. Akamai의 Intelligent Edge Platform은 기업과 클라우드 등 모든 곳으로 확장하고 있고 고객의 비즈니스가 빠르고, 스마트하며, 안전하게 운영될 수 있도록 지원합니다. 대표적인 글로벌 기업들은 Akamai 솔루션을 통해 멀티 클라우드 아키텍처를 강화하고 경쟁 우위를 확보하고 있습니다. Akamai는 가장 가까운 곳에서 사용자에게 의사 결정, 앱, 경험을 제공하고 공격과 위협을 먼 곳에서 차단합니다. Akamai 포트폴리오는 엣지 보안, 웹·모바일 성능, 엔터프라이즈 접속, 비디오 전송 솔루션으로 구성되어 있고 우수한 고객 서비스, 애널리틱스, 24시간 연중무휴 모니터링 서비스를 제공합니다. 대표적인 기업과 기관에서 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지([www.akamai.co.kr](http://www.akamai.co.kr)) 또는 블로그([blogs.akamai.com](http://blogs.akamai.com))를 방문하거나 Twitter에서 @Akamai를 팔로우하시기 바랍니다. 전 세계 Akamai 연락처 정보는 [www.akamai.com/locations](http://www.akamai.com/locations)에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다. 2019년 4월 발행.