ENTERPRISE THREAT PROTECTOR

보안 위협을 방어하는 클라우드 기반의 고급 솔루션

기업들이 직접 인터넷 접속(Direct Internet Access), SaaS 애플리케이션, 클라우드 서비스, 모빌리티, 사물 인터넷(IoT)을 도입함에 따라 공격받을 수 있는 부분이 크게 증가하고 새로운 보안 도전과제 역시 다수 발생했습니다. 멀웨어, 피싱, 데이터 유출 등 최신 보안 위협으로부터 기업과 사용자를 보호하는 일은 점점 어려워지고 있습니다. 보안 컨트롤 포인트 문제를 해결하고 기존에 사용 중인 보안 솔루션과의 갭(gap)도 관리해야 합니다. Enterprise Threat Protector(ETP)는 일종의 보안 인터넷 게이트웨이(Secure Internet Gateway)로, 기존에 사용 중인 보안 솔루션에 가중되는 복잡함 없이 언제 어디서나 사용자와 디바이스가 인터넷에 안전하게 접속하도록 지원하는 솔루션입니다. 전세계 인터넷 및 DNS(Domain Name System) 트래픽에 대한 독보적인 인사이트를 기반으로 실시간 위협 인텔리전스를 제공합니다.

ENTERPRISE THREAT PROTECTOR

Enterprise Threat Protector는 Akamai의 Intelligent Edge Platform™과 통신사급 리커시브 DNS 서비스를 기반으로 한 SIG(Secure Internet Gateway)입니다. 설정과 구축이 간편하고 하드웨어를 설치하거나 유지관리할 필요가 없습니다.

ETP는 Akamai의 실시간 클라우드 보안 인텔리전스와 전세계적으로 광범위하게 분산된 플랫폼을 활용하여 멀웨어, 랜섬웨어, 피싱, DNS 기반 데이터 유출 등 다양한 표적 위협을 선제적으로 탐지·차단합니다. 보안팀은 Akamai의 포털을 통해 직원들이 인터넷에 접속하는 위치에 상관 없이 통합 보안 정책과 제한적 사용 정책(AUP)을 몇 분만에 일괄적으로 생성·배포·적용할 수 있습니다.

작동 방식

ETP는 멀티레이어 방어(DNS, URL, 인라인 페이로드 분석)를 사용하여 성능에 영향을 주지 않으면서 최적의 보안 기능을 제공하고 복잡성을 감소시킵니다.

DNS 검사: 외부 리커시브 DNS 트래픽을 ETP로 연결시키기만 하면 실시간으로 도메인의 리스크 점수를 책정하는 Akamai의 위협 인텔리전스가 모든 요청된 도메인을 확인합니다. 사용자가 악성 도메인과 서비스에 접속하는 것을 선제적으로 차단할 수 있고 안전한 도메인과 서비스에 대한 요청은 정상적으로 처리됩니다. 이 확인 과정을 거친 후에 IP 접속이 이뤄지기 때문에 모든 위협이 보안 킬 체인과 멀리 떨어진 곳에서 차단됩니다. 또한, DNS는 모든 포트 및 프로토콜에서 사용 가능하기 때문에 표준 웹 포트나 프로토콜을 사용하지 않는 멀웨어 역시 방어할 수 있습니다. 도메인 확인을 통해 사용자가 접속하려는 콘텐츠 종류를 확인하고 해당 콘텐츠가 기업의 제한적 사용 정책(AUP)을 위반할 경우 접속을 차단할 수 있습니다.

URL 검사: Akamai의 URL 위협 인텔리전스가 요청된 URL을 확인하고 악성 URL은 자동 차단됩니다. 요청된 URL이 Akamai의 URL 위협 인텔리전스를 기반으로 확인되고 악성 URL이 자동 차단됩니다. 프록시는 HTTP 및 HTTPS URL을 모두 검사합니다.

인라인 페이로드 분석: 다수의 멀웨어 고급 탐지 엔진을 사용해 위험한 도메인의 HTTP 및 HTTPS를 스캔합니다. 이 엔진은 시그니처, 시그니처리스, 머신 러닝 등 다양한 기술을 사용해 잠재적인 악성 파일(실행 및 문서파일) 뿐만 아니라 요청된 웹 페이지에 직접 임베디드된 멀웨어(난독화된 악성 JavaScript) 등 제로데이 공격을 광범위하게 차단합니다.

ETP는 다른 보안 제품, 리포팅 툴(방화벽, SIEM), 외부 위협 인텔리전스 피드와 간편하게 통합되기 때문에 기업 보안 스택 전반에 걸쳐 투자 효과를 극대화할 수 있습니다.

또한, Enterprise Client Connector를 노트북에 구축하면 노트북을 사내 외부 네트워크에서 사용할 때 선제적인 보안 레이어를 빠르게 추가할 수 있습니다.

기업이 누릴 수 있는 혜택

- **보안 체계 강화** - 최신 위협 인텔리전스를 기반으로 멀웨어·랜섬웨어 드롭 사이트, 멀웨어 명령 및 제어(CnC) 서버, DNS 데이터 유출, 피싱 도메인 및 URL에 대한 요청을 사전에 차단합니다.
- **제로데이 방어를 위해 악성 페이로드 차단** - 엔드포인트 디바이스에 도달하여 감염시키기 전에 요청된 파일과 웹 콘텐츠를 실시간으로 스캔하여 위협을 차단합니다.
- **DIA 성능 강화** - 의심스러운 트래픽만 프록시로 전달해 URL 검사와 페이로드 분석을 진행합니다.
- **하드웨어 없이 손쉽게 보안 강화** - 100% 클라우드 기반 솔루션으로 몇 분 안에 설정·구축이 가능하며 별도의 하드웨어가 필요하지 않으므로 사용자 불편을 초래하지 않으면서 신속하게 확장하고 보안을 강화합니다.
- **VPN 없이 외부 네트워크에서 사용되는 노트북에 대한 리스크 감소와 보안 강화** - Enterprise Client Connector를 통해 보안 정책과 AUP를 모두 적용합니다.
- **보안 관리 시간과 복잡성 최소화** - 오탐 및 다른 보안 제품의 알람 건수를 감소시키고 장소에 상관 없이 보안 정책 및 업데이트를 신속히 관리하여 모든 지역의 사용자를 보호합니다.
- **컴플라이언스 및 AUP를 일관성 있고 신속하게 적용** - 문제가 있거나 부적절한 도메인 및 콘텐츠 카테고리에 대한 접속을 차단합니다.
- **DNS 안정성 및 신뢰성 증대** - Akamai Intelligent Edge Platform으로 안정성과 신뢰성을 극대화합니다.

ENTERPRISE THREAT PROTECTOR

AKAMAI CSI(CLOUD SECURITY INTELLIGENCE)

ETP는 보안 위협과 리스크에 대한 인텔리전스를 실시간으로 제공하는 Cloud Security Intelligence를 기반으로 합니다.

Akamai의 위협 인텔리전스는 비즈니스에 영향을 미칠 수 있는 현재 위협과 관련 위협을 방어하고 보안팀의 조사가 필요한 오탐 알람 건수를 최소화하도록 설계되었습니다.

이 인텔리전스는 매일 글로벌 웹 트래픽의 최대 30%를 처리하고 2조 2천억 개의 DNS 쿼리를 전송하는 Akamai Intelligent Edge Platform에서 연중무휴 24시간 수집된 데이터로부터 도출됩니다. Akamai 인텔리전스는 대규모 외부 위협 피드를 통해 강화되며, 통합된 데이터는 고급 행동 분석 기법, 머신 러닝, 독점 알고리즘을 사용하여 지속적으로 분석 및 관리됩니다. 새로운 보안 위협이 탐지될 때마다 즉각적으로 ETP서비스에 추가되기 때문에 실시간 보안이 가능합니다.

AKAMAI INTELLIGENT EDGE PLATFORM

ETP 서비스는 속도, 보안성, 안정성이 뛰어난 통신사급 Akamai Intelligent Edge Platform을 기반으로 합니다. Akamai 플랫폼은 전세계적으로 촘촘하게 분산되어 있으며 100% 가용성을 보장하는 SLA를 제공하고 기업의 리커시브 DNS 서비스에 대한 최적의 안정성을 보장합니다.

클라우드 기반 관리 포털

ETP의 설정 및 관리는 클라우드 기반의 Luna Control Center에서 가능하며 시간과 장소의 제약 없이 솔루션을 관리할 수 있습니다.

정책을 쉽고 빠르게 관리할 수 있고 전세계적으로 정책을 변경하는 데 몇 분밖에 걸리지 않기 때문에 지역에 상관없이 모든 사용자를 보호할 수 있습니다. 보안팀은 중요한 정책 이벤트에 대한 알람을 실시간 이메일로 받아볼 수 있고 보고서도 정기적으로 받을 수 있기 때문에 잠재적인 보안 위협이 발생했을 때 신속하게 탐지하고 즉각적인 조치를 취할 수 있습니다. 실시간 대시보드는 트래픽, 위협, AUP 이벤트에 대한 정보를 제공합니다. 개별 활동에 대한 자세한 정보 역시 대시보드를 드릴다운해 확인할 수 있습니다. 이 세부 정보는 보안 인시던트를 분석하고 해결하는 데 유용한 리소스를 제공합니다.

모든 포털 기능은 API를 통해 접속 가능하고 데이터 로그는 SIEM으로 내보낼 수 있기 때문에 ETP는 다른 보안 솔루션 및 리포팅 툴과 효율적이고 간편하게 통합될 수 있습니다.

주요 기능

- **Akamai가 보유한 위협 정보:** 매일 글로벌 웹 트래픽의 15~30%와 Akamai의 리커시브 DNS 클라우드로 전달되는 2조 2천억 건의 DNS 요청을 처리하면서 최신 보안 인텔리전스를 구축하고 있습니다.
- **고객이 보유한 위협 정보:** 고객사의 보안팀이 보유하고 있는 기존의 위협 인텔리전스 피드와 신속하게 통합할 수 있기 때문에 현재 보안 투자 효과를 높일 수 있습니다.
- **인라인 실시간 페이로드 분석:** 3개의 멀웨어 고급 탐지 엔진이 복잡하고 정교한 위협을 식별·차단하고 제로데이 공격 방어 역량을 개선합니다.
- **제한적 사용 정책(AUP):** 접속 가능한 콘텐츠 카테고리를 제한함으로써 제한적 사용 정책을 실시하고 컴플라이언스를 강화할 수 있습니다.
- **분석 및 보고:** 대시보드는 모든 아웃바운드 웹 트래픽, 위협, AUP 이벤트에 대한 정보를 실시간으로 제공합니다.
- **보안 인사이트:** Akamai가 도메인 또는 URL을 위협 인텔리전스 목록에 추가한 이유를 신속하게 확인할 수 있습니다.
- **로깅:** 트래픽 로그는 30일 동안 유지되며, CSV 파일 형태로 간편하게 내보내거나 추가 분석을 위해 SIEM에 통합할 수 있습니다.
- **DNSSEC:** ETP로 전송되는 모든 DNS 요청은 DNSSEC를 통해 이루어집니다.

AKAMAI 생태계

Akamai Intelligent Edge Platform은 기업과 클라우드 등 모든 곳으로 확장하고 있고 고객의 비즈니스가 빠르고, 스마트하며, 안전하게 운영될 수 있도록 지원합니다. Akamai의 모든 솔루션은 맞춤 설정 가능한 통합 Luna Control Center를 통해 관리되어 뛰어난 가시성과 제어 능력을 제공하는 동시에 고객사가 전략 변경에 맞게 혁신을 주도해 나갈 수 있도록 Professional Service 전문가의 지원을 받습니다.

Enterprise Threat Protector에 대해 자세히 알아보려면 akamai.com/etp를 참조하고 무료체험을 신청하시기 바랍니다.

ENTERPRISE THREAT PROTECTOR

보안	Guest Wi-Fi	Intelligence	Advanced Threat
멀웨어, 랜섬웨어, 피싱 전송 도메인 차단		X	X
멀웨어 명령 및 제어(CnC) 요청 차단		X	X
DNS 기반 데이터 유출 식별		X	X
요청된 HTTP 및 HTTPS URL를 검사하기 위해 위험한 도메인을 프록시로 전달		X	X
다수의 인라인 멀웨어 분석 및 탐지 엔진을 사용해 위험한 HTTP 및 HTTPS 페이로드를 실시간 인라인 분석			X
공유 사이트에서 다운로드한 파일의 실시간 인라인 분석			X
HTTP 및 HTTPS URL를 검사하기 위해 맞춤형 도메인 목록 생성		X	X
인라인 페이로드 분석을 위해 맞춤형 도메인 목록 생성			X
고객 트래픽 로그 재분석을 통해 새로 발견된 위협 탐지 및 통보		X	X
맞춤형 허용/거부 목록 생성		X	X
추가적인 위협 인텔리전스 피드 통합		X	X
맞춤형 오류 페이지	X	X	X
Akamai의 위협 데이터베이스 쿼리를 통해 악성 도메인 및 URL에 대한 인텔리전스 확보		X	X
외부 네트워크 노트북(Windows 및 MacOS)에 보안 적용		X	X
제한적 사용 정책(AUP)	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
내부 및 외부 네트워크 사용자에 대한 AUP 위반 모니터링 및 차단	X[1]	X	X
Google, Bing, YouTube에 SafeSearch 적용	X	X	X
리포팅, 모니터링, 관리	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
기업 전반의 모든 활동에 대한 가시성을 제공하는 맞춤형 대시보드	X[2]	X	X
모든 위협 및 AUP 이벤트에 대한 상세 분석	X[2]	X	X
모든 온보딩된 트래픽 요청, 위협, AUP 이벤트에 대한 전체 로깅 및 가시성	X[2]	X	X
모든 로그 전송(로그는 30일 동안 유지되고 API를 통해 내보낼 수 있음)	X[2]	X	X
Open API를 통해 지원되는 설정, 맞춤형 보안 목록, 이벤트	X[2]	X	X
Open API를 통해 기타 보안 시스템(예: SIEM)과 통합	X	X	X
이메일 기반 실시간 보안 및 AUP 알람	X[2]	X	X
일별 또는 주별로 보고서를 이메일로 전송	X	X	X
관리 위임	X	X	X
Akamai Intelligent Edge Platform™	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
리커시브 DNS에 대한 고객별 전용 IPv4 및 IPv6	X	X	X
100% 가용성을 보장하는 SLA	X	X	X
최적의 성능을 위한 Anycast DNS 라우팅	X	X	X
보안 강화를 위해 적용되는 DNSSEC	X	X	X
ENTERPRISE CONNECTORS	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
외부 네트워크 노트북(Windows 및 OSX)을 보호하고 외부 및 내부 네트워크 이벤트와 관련된 시스템을 리포팅하기 위한 Enterprise Client Connector		X	X
Enterprise Client Connector 자동 업데이트		X	X
엔드포인트 디바이스의 IP 주소 및 시스템 이름을 식별하기 위한 Enterprise Security Connector		X	X

1. ETP Guest Wi-Fi에는 외부 네트워크 AUP 적용이 포함되지 않습니다.
2. ETP Guest Wi-Fi에는 보안 관리 기능이 포함되지 않기 때문에 알람, 분석, 대시보드, 로그에는 AUP 이벤트 및 활동만 포함됩니다.