Enterprise Threat Protector

Advanced Threat Protection in the Cloud

As enterprises adopt Direct Internet Access (DIA), software as a service (SaaS) applications, cloud services, mobility, and the Internet of Things (IoT), their attack surface increases dramatically and they face a host of new security challenges. Protecting the organization and users against advanced targeted threats such as malware, ransomware, phishing, and data exfiltration becomes exponentially more difficult. Security control-point complications and complexities, and security gaps in legacy on-premises solutions, need to be managed with limited resources.

Enterprise Threat Protector is a cloud-based secure web gateway (SWG) that is designed to help security teams ensure that users and devices can securely connect to the Internet wherever they happen to be, without the intricacy and management overheads associated with other legacy security solutions. Enterprise Threat Protector is powered by real-time threat intelligence based on Akamai's unrivaled global insights into Internet and domain name system (DNS) traffic and multiple malware-detection engines.

Enterprise Threat Protector

Built on the global Akamai Intelligent Edge Platform and Akamai's carrier-grade recursive DNS service, Enterprise Threat Protector is a quick-to-configure and easy-to-deploy SWG that requires no hardware to be installed and maintained.

Enterprise Threat Protector has multiple layers of protection that leverage real-time Akamai Cloud Security Intelligence and multiple static and dynamic malware-detection engines to proactively identify and block targeted threats such as malware, ransomware, phishing, and DNS-based data exfiltration. Akamai's portal enables security teams to centrally create, deploy, and enforce both unified security policies and acceptable use policies (AUPs) in minutes for all employees, wherever they are connected to the Internet.

swisscom

How it works

Enterprise Threat Protector has multiple layers of protection DNS, URL, and payload analysis delivering security and reducing complexity, without impacting performance. All of this protection can be delivered by simply directing web traffic to Enterprise Threat Protector using a lightweight client or by forwarding web traffic from another web proxy by using proxy chaining.

DNS Inspection: Every requested domain is checked against Akamai's real-time threat intelligence, and requests to identified malicious domains are automatically blocked. Using DNS as an initial security layer proactively blocks threats early in the kill chain and before any web connection is made. In addition, DNS is designed to be effective across all ports and protocols, thus protecting against malware that does not use standard web ports and protocols. Domains can also be checked to determine the type of content a user is attempting to access, and blocked if the content breaches the enterprise's AUP.

URL Inspection: Requested HTTP and HTTPS URLs are checked against Akamai's real-time threat intelligence, and malicious URLs are automatically blocked.

Payload Analysis: The HTTP/S payloads are scanned inline or offline using multiple advanced malware-detection engines. These engines use a variety of techniques including signature, signatureless, machine learning, and sandboxing that deliver comprehensive zero-day protection against potentially malicious files, such as executables and document files. This analysis also protects against malware that is embedded directly into the requested web page, such as obfuscated malicious JavaScript, and zero-day phishing pages.

Enterprise Threat Protector easily integrates with other security products and reporting tools, including firewalls and SIEMs, as well as external threat intelligence feeds, allowing you to maximize investments across all layers of the enterprise security stack.

Additionally, deploying the lightweight Enterprise Client Connector on managed laptops lets companies quickly add an additional layer of proactive security when laptops are used off-network.

Business Benefits

Improve security defenses by proactively blocking requests to malware and ransomware drop sites, phishing sites, malware command and control (C2) servers, and DNS data exfiltration based on unique and up-to-date threat intelligence

Minimize security management time and complexity by reducing false-positive security alerts, decreasing alerts from other security products, and administering security policies and updates from anywhere in seconds to protect all locations

Move web security to the cloud with a cloud-based secure web gateway that can be configured and deployed globally in minutes (with no disruption for users) and rapidly scaled

Block malicious payloads for improved zero-day protection by scanning requested files and web content to stop threats before they reach and compromise endpoint devices

Reduce risk and improve security for off-network laptops without using a VPN with the lightweight Enterprise Client Connector, which enforces both your security policies and AUPs

Enforce compliance and your AUPs quickly and uniformly by blocking access to objectionable or inappropriate domains and content categories

Simplify DIA security by eliminating the need for branch security appliances

Increase resilience and reliability with the Akamai Intelligent Edge Platform

Akamai Cloud Security Intelligence (CSI)

Enterprise Threat Protector is powered by Akamai's Cloud Security Intelligence, which delivers real-time intelligence about threats and the risks that these threats present to enterprises.

Akamai's threat intelligence is designed to provide protection against current and relevant threats that could impact your business and to minimize the number of false-positive alerts that your security teams must investigate.

This intelligence is built on data gathered 24/7 from the Akamai Intelligent Edge Platform, which manages up to 30% of global web traffic and delivers up to 2.2 trillion DNS queries daily. Akamai's intelligence is enhanced with hundreds of external threat feeds, and the combined data set is continuously analyzed and curated using advanced behavioral analysis techniques, machine learning, and proprietary algorithms. As new threats are identified, they are immediately added to the Enterprise Threat Protector service, delivering real-time protection.

Akamai Intelligent Edge Platform

The Enterprise Threat Protector service is built on the Akamai Intelligent Edge Platform, which is fast, intelligent, and secure. Distributed globally, the platform delivers a 100% availability service-level agreement (SLA) and ensures optimal reliability for an enterprise's web security.

Cloud-Based Management Portal

Configuration and ongoing management of Enterprise Threat Protector are done through the cloud-based Akamai Control Center portal, enabling management from any location at any time.

Policy management is quick and easy, and changes can be pushed out globally in minutes to ensure that all of your locations and users are protected. Real-time email notifications and scheduled reports can be configured to alert security teams about critical policy events so that immediate remediation steps can be taken to quickly identify and resolve potential threats. A real-time dashboard provides an overview of traffic, threat, and AUP events. Detailed information on any activity can be viewed through drill-down on individual dashboard elements. This detailed information provides a valuable resource for analysis and remediation of security incidents.

All portal functionality can be accessed via APIs, and data logs can be exported to a SIEM, allowing Enterprise Threat Protector to easily and effectively integrate with your other security solutions and reporting tools.

The Akamai Ecosystem

The Akamai Intelligent Edge Platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Our comprehensive solutions are managed through the unified, customizable Akamai Control Center for visibility and control, and supported by professional services experts who get you up and running easily, and inspire innovation as your strategies evolve.

To learn more about Enterprise Threat Protector and sign up for a free trial, visit www.akamai.com/etp.

Key Capabilities

Akamai-Categorized Threats: Up-to-the-minute threat intelligence based on Akamai's visibility into 15% to 30% of daily web traffic is combined with 2.2 trillion daily DNS requests to Akamai's recursive DNS cloud

Customer-Categorized Threats: Security teams can quickly integrate existing threat intelligence feeds, extending value from your current security investments

Inline and Offline Payload Analysis: Four advanced malware-detection engines identify and block complex advanced threats and improve zero-day protection

Logging: Traffic logs are retained for 30 days and can easily be exported as a .CSV file or integrated into a SIEM for further analysis

Acceptable Use Policies: Enforce enterprise AUPs and compliance by limiting which content categories can and cannot be accessed

Analysis and Reporting: Dashboards provide real-time insight into all outbound enterprise web traffic, as well as threat and AUP events

Security Insights: Quickly understand why Akamai has added a domain or a URL to its threat intelligence lists

DNSSEC: All DNS requests sent to Enterprise Threat Protector have DNSSEC enabled

Akamai Intelligent Edge Platform	Guest Wi-Fi	Intelligence	Advance Threat
Dedicated IPv4 and IPv6 VIPs per customer for recursive DNS	✓	✓	✓
SLA for 100% availability	✓	✓	✓
Anycast DNS routing for optimal performance	✓	✓	✓
DNSSEC enforced for increased security	✓	✓	✓

Enterprise Connectors	Guest Wi-Fi	Intelligence	Advance Threat
Enterprise Client Connector for protecting off-network laptops (Windows and OS X) and reporting machine name for off- and on-network events		✓	✓
Auto-updating of Enterprise Client Connector		✓	✓
Enterprise Security Connector for identifying the IP addresses and machine names of endpoint devices		✓	✓

Security

	Guest Wi-Fi	Intelligence	Advance Threat
Block malware, ransomware, and phishing delivery domains and URLs		✓	✓
Block malware command and control (C2) requests		✓	✓
Identify DNS-based data exfiltration		✓	✓
Proxy risky domains for requested HTTP and HTTPS URL inspection		✓	✓
Proxy all web traffic for DNS, URL, and payload analysis			✓
Inline and offline analysis of HTTP and HTTPS payloads using multiple malware analysis and detection engines*			✓
Cloud sandbox for offline dynamic payload analysis*			✓
Real-time inline analysis of web pages to detect zero-day phishing pages			✓
Real-time inline or offline analysis of files downloaded from file-sharing sites*			✓
Create a customized list of domains for HTTP and HTTPS URL inspection		✓	✓
Create a customized list of domains for inline/offline payload analysis			✓
Lookback analysis of customer traffic logs to identify and alert on newly discovered threats		✓	✓
Create custom allow/deny lists		✓	✓
Incorporate additional threat intelligence feeds		✓	✓
Customizable error pages	✓	✓	✓
Query Akamai's threat database to gain intelligence on malicious domains and URLs		✓	✓
Enforce security for off-network laptops (Windows and macOS)		✓	✓

Acceptable Use Policy (AUP)

	Guest Wi-Fi	Intelligence	Advance Threat
Create group-based AUP policies			✓
Monitor or block AUP violations for on-network and off-network users	✓ [1]	✓	✓
Enforce SafeSearch for Google, Bing, and YouTube	✓	✓	✓

Reporting, Monitoring, and Administration	Guest Wi-Fi	Intelli-gence	Advance Threat
IDP and Active Directory integration			✓
Enterprise-wide view of all activity with customizable dashboards	✓ [2]	✓	✓
Detailed analysis of all threat and AUP events	✓ [2]	✓	✓
Full logging and visibility of all onboarded traffic requests and threat and AUP events	✓ [2]	✓	✓
Log delivery of all logs; logs are retained for 30 days and can be exported via an API	✓ [2]	✓	✓
Configuration, custom security lists, and events available via an open API	✓ [2]	✓	✓
Integrate with other security systems, such as SIEMs, via an open API	✓ [2]	✓	✓
Email-based real-time security and AUP alerts	✓ [2]	✓	✓
Schedule daily or weekly email reports	✓ [2]	✓	✓
Delegated administration	✓ [2]	✓	✓

* Cloud sandbox is an optional add-on and is required for offline analyses of large files
1) ETP Guest Wi-Fi does not include off-network AUP enforcement
2) ETP Guest Wi-Fi does not include any security controls so alerts, analyses, dashboards, and logs only include AUP events and activity

www.swisscom.com/digital-media
+41 800 22 40 40
digital.media@swisscom.com