Edge Delivery Services
powered by Akamai

Enterprise Threat Protector

Advanced Threat Protection in the Cloud

As enterprises adopt Direct Internet Access (DIA), SaaS applications, cloud services, mobility, and the Internet of Things (IoT), their attack surface increases dramatically and they are faced with a host of new challenges. Protecting the organization and users against advanced targeted threats such as malware, phishing, and data exfiltration becomes exponentially more difficult. Security control-point complications and complexities and security gaps in legacy solutions have to be managed. Enterprise Threat Protector (ETP) is a Secure Internet Gateway (SIG) that enables security teams to ensure that users and devices can securely connect to the Internet wherever they happen to be, without the intricacy associated with other legacy security solutions. Enterprise Threat Protector is powered by real-time threat intelligence based on unprecedented global insights into Internet and Domain Name System (DNS) traffic.

Enterprise Threat Protector

Built on our carrier-grade recursive DNS service, Enterprise Threat Protector is a quick-to-configure and easy-to-deploy SIG that requires no hardware to be installed and maintained.

Enterprise Threat Protector leverages real-time cloud security intelligence and our proven, globally distributed platform to proactively identify and block targeted threats such as malware, ransomware, phishing, and DNS-based data exfiltration. Our 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.

How It Works

Enterprise Threat Protector uses multiple layers of protection — DNS, URL, and inline payload analysis — delivering optimal security and reducing complexity, without impacting performance.

DNS Inspection: By simply directing your external recursive DNS traffic to Enterprise Threat Protector, all requested domains are checked against real-time domain risk scoring threat intelligence. Users are proactively blocked from accessing malicious domains and services while requests to safe domains and services are resolved. As this validation happens before the IP connection is made, threats are stopped earlier in the security kill chain. In addition, DNS is 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: Domains that are considered risky based on threat intelligence data are automatically forwarded to a cloud proxy on our platform. The requested URL is checked against URL threat intelligence, and malicious URLs are automatically blocked. The proxy inspects both HTTP and HTTPS URLs.

Inline Payload Analysis: The HTTP and HTTPS payloads from risky domains are then scanned in real time using multiple advanced malware-detection engines. These engines use a variety of techniques — including signature, signatureless, and machine learning — that deliver comprehensive zero-day protection against potentially malicious files, such as executables and document files, as well as other malware that is embedded directly into the requested web page, such as obfuscated malicious JavaScript.

Business Benefits

- **Improve security defenses** by proactively blocking requests to malware and ransomware drop sites, malware command and control (CnC) servers, and DNS data exfiltration and phishing domains and URLs based on unique and up-to-date threat intelligence.
- **Block malicious payloads for improved zero-day protection** by scanning requested files and web content in real time to stop threats before they reach and compromise endpoint devices.
- **Enhance DIA performance** by only proxying suspicious traffic for URL inspection and payload analysis.
- **Add instant protection without complexity or hardware** with a 100% cloud-based solution that can be configured and deployed globally in minutes (with no disruption for users) and rapidly scaled.
- **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.
- **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.
- **Enforce compliance and your AUP quickly and uniformly** by blocking access to objectionable or inappropriate domains and content categories.
- **Increase DNS resilience and reliability** with our intelligent platform.

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.

Cloud Security Intelligence (CSI)

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

Our 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 our platform, which manages up to 30% of global web traffic and delivers up to 2.2 trillion DNS queries daily. This intelligence is enhanced with a large number 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.

Intelligent Edge Platform

The Enterprise Threat Protector service is built on our carrier-grade platform, which is secure, reliable, and fast. Distributed globally, the platform delivers a 100% availability SLA and ensures optimal reliability for an enterprise's recursive DNS service.

Cloud-based Management Portal

All configuration and ongoing management of Enterprise Threat Protector is done through our cloud-based Luna 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 drilldown 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.

Key Capabilities

- **Categorized Threats:** Up-to-the-minute threat intelligence based on our platform's visibility into 15–30% of daily web traffic is combined with 2.2 trillion daily DNS requests to our recursive DNS cloud.
- **Customer-Categorized Threats:** Security teams can quickly integrate existing threat intelligence feeds, extending value from your current security investments.
- **Inline Real-Time Payload Analysis:** Three advanced malware detection engines identify and block complex advanced threats and improve zero-day protection.
- **Acceptable Use Policies:** Enforce enterprise acceptable use policy and ensure 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 a domain or a URL has been added to threat intelligent lists.
- **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.
- **DNSSEC:** All DNS requests sent to Enterprise Threat Protector have DNSSEC enabled.

The IBM® Edge Delivery Services Ecosystem

Our 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 Luna 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.

Edge Delivery Services
powered by Akamai

SECURITY	Guest Wi-Fi	Intelligence	Advanced Threat
Block malware, ransomware, and phishing delivery domains		✓	✓
Block malware command and control (CnC) requests		✓	✓
Identify DNS-based data exfiltration		✓	✓
Proxy risky domains for requested HTTP and HTTPS URL inspection		✓	✓
Real-time inline analysis of risky HTTP and HTTPS payloads using multiple inline malware analysis and detection engines			✓
Real-time inline 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 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 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**	**Advanced Threat**
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**	**Intelligence**	**Advanced Threat**
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	✓	✓	✓
Delegated administration	✓	✓	✓
INTELLIGENT EDGE PLATFORM	**Guest Wi-Fi**	**Intelligence**	**Advanced 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**	**Advanced Threat**
Enterprise Client Connector for protecting off-network laptops (Windows and OSX) 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		✓	✓

[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, analysis, dashboards, and logs only include AUP events and activity.