

# ENTERPRISE THREAT PROTECTOR

Targeted Threat Protection in the Cloud



The enterprise threat landscape is fast evolving. Targeted threats such as malware, ransomware, data exfiltration, and phishing are increasing in volume, and malicious actors are getting better at circumventing traditional security approaches. Combined with the adoption of SaaS, Cloud, and IoT in the enterprise, more sophisticated threat delivery has introduced new visibility challenges, control-point complications, and security gaps. Powered by Akamai's unique global insights into Internet and Domain Name System (DNS) traffic, Enterprise Threat Protector enables security teams to proactively block and mitigate targeted threats and enforce an acceptable use policy across the enterprise.

## ENTERPRISE THREAT PROTECTOR

Built on the Akamai Intelligent Platform™ and Akamai's AnswerX™ carrier-grade recursive DNS, Enterprise Threat Protector (ETP) is a quick-to-configure and easy-to-deploy cloud solution that requires no hardware or software to deploy or maintain.

Enterprise Threat Protector leverages real-time Akamai Cloud Security Intelligence and Akamai's proven, globally distributed recursive DNS platform to proactively identify and block targeted threats such as malware, ransomware, DNS data exfiltration, and phishing. Akamai's cloud portal enables security teams to centrally manage and enforce unified security and acceptable use policies in minutes for all employees.

## HOW IT WORKS

The Domain Name System (DNS) is the foundation for all Internet services, yet many malicious domains, including sites hosting malware and ransomware, and the associated command and control (CnC) servers, use recursive DNS for attacks.

When an enterprise's external recursive DNS traffic is directed to Akamai's Enterprise Threat Protector, requested domains are checked against Akamai's real-time domain risk scoring threat intelligence, and enterprises can proactively block employees from accessing malicious domains and services. As this validation happens before the IP connection is made, threats are stopped earlier in the security kill chain, i.e., farther away from an enterprise's perimeter. 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 an employee is attempting to access, and blocked if the content breaches the enterprise's acceptable use policy (AUP).

**Beta** - Deploying the lightweight Enterprise Security Connector on managed laptops also lets companies quickly add an additional layer of proactive security when laptops are used off network.

Enterprise Threat Protector easily integrates with other security products and reporting tools — including Secure Web Gateways, Next-Generation Firewalls, and SIEMs, as well as external threat intelligence feeds — allowing companies to maximize their investments across all layers of their security stack.

## BUSINESS BENEFITS

- **Significantly improve security defenses** by proactively blocking DNS requests to malware and ransomware drop sites, malware command and control (CnC) servers, and DNS data exfiltration and phishing domains based on unique and up-to-date threat intelligence.
- **Instantly add protection without complexity or hardware** with a 100% cloud-based solution that can be configured and deployed in minutes (with no disruption for users) and rapidly scaled.
- **Beta - Simply reduce risk and improve security for off-network laptops without using a VPN** with the lightweight Enterprise Security Connector which enforces your security measures and Acceptable Use Policies.
- **Easily reduce management time** by administering security policies and updates from anywhere in seconds to protect all locations.
- **Quickly and uniformly enforce compliance and your acceptable use policy** by blocking access to objectionable or inappropriate domains and content categories.
- **Immediately increase DNS resilience and reliability** with Akamai's carrier-grade global intelligent platform.

# ENTERPRISE THREAT PROTECTOR

## AKAMAI CLOUD SECURITY INTELLIGENCE (CSI)

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

This intelligence is built on data gathered every day from Akamai's Intelligent Platform, which manages up to 30% of global web traffic and delivers up to 150 billion DNS queries daily. Akamai's intelligence is enhanced with external threat feeds, and the combined data set is analyzed using advanced behavioral analysis. These results are further enhanced by a dedicated threat research team. As new threats are identified, they are immediately added to the ETP service, delivering real-time protection for enterprises and their employees.

## AKAMAI'S INTELLIGENT PLATFORM

The Enterprise Threat Protector service is built on Akamai's carrier-grade Intelligent 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 Akamai's cloud-based Luna portal, enabling management to be done from any location at any time.

Policy management is quick and easy. Changes can be pushed out globally in minutes to ensure that all enterprise locations and employees are protected. Email alerts can be configured to signal 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 DNS traffic, threat events, and AUP activities. 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 DNS 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

- **Akamai-Categorized Threats:** Up-to-the-minute threat intelligence based on Akamai's visibility into 15–30% of daily web traffic is combined with 150 billion 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 existing security investments.
- **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 DNS traffic, as well as threat and AUP events.
- **Logging:** DNS logs are retained for 7 days (**Beta** - 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 AKAMAI ECOSYSTEM

Akamai makes the Internet fast, reliable, and secure. Our comprehensive solutions are built on the globally distributed Akamai Intelligent Platform™, 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.

To learn more about Enterprise Threat Protector and sign up for a FREE trial, visit [akamai.com/etp](https://akamai.com/etp)



As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit [www.akamai.com](https://www.akamai.com), [blogs.akamai.com](https://blogs.akamai.com), or [@Akamai](https://twitter.com/Akamai) on Twitter. You can find our global contact information at [www.akamai.com/locations](https://www.akamai.com/locations), or call 877-425-2624. Published 11/17.