Edge Delivery Services
powered by Akamai

Enterprise Threat Protector for Guest Wi-Fi Protection

Enterprise Threat Protector

Guest Wi-Fi Acceptable Use Policy Control

Providing your customers and patrons with guest Wi-Fi connectivity delivers numerous business benefits. By having the ability to control the types of web content that users can and cannot access, you can enhance reputation and customer loyalty by providing a safe and clean environment to access content on the Internet. Enterprise Threat Protector is a cloud-based service that allows organizations providing guest Wi-Fi connectivity to proactively manage and control the categories of web content that users are allowed to access. Blocking access to inappropriate web content will significantly reduce reputational risk and maintain brand integrity and reputation.

Enterprise Threat Protector

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 proactively identifies and blocks web content categories based on your organization's guest Wi-Fi Acceptable Use Policy (AUP). Our cloud portal allows IT teams to centrally manage and enforce Acceptable Use Policies in minutes for all the locations where you provide guest Wi-Fi.

How It Works

The Domain Name System (DNS) is the foundation for all Internet services, and so provides an effective way to identify the category of web content that is being requested.

By directing DNS traffic from your guest Wi-Fi to Enterprise Threat Protector, and checking the requested domains against our domain database, organizations can proactively control the types of web content that guests and patrons can and cannot access. Everything is managed within the Enterprise Threat Protector service; no software is required to be installed or approved on user devices. As soon as they connect to your guest Wi-Fi, the service is on and monitoring DNS requests.

To allow you to baseline the types of content that guests and patrons are accessing, Enterprise Threat Protector can be configured in monitor mode. This provides visibility into current usage to determine the content categories you may need to block access to (e.g., gambling).

Intelligent Platform

The Enterprise Threat Protector service is built on our carrier-grade Intelligent Platform, which is secure, reliable, and fast. Distributed globally with more than 200,000 servers in 130+ countries and within more than 1,600 networks around the world, the platform delivers a 100% availability SLA and ensures optimal reliability for an enterprise's recursive DNS service.

Business Benefits

- **Significantly reduce reputational risk and maintain brand reputation** by proactively controlling the types of web content that guest Wi-Fi users can access.
- **Optimize network bandwidth** by quickly blocking access to streaming media domains.
- **Maximize IT resources and reduce management time** by managing Acceptable Use Policies from anywhere, and deploy policies in minutes to protect all guest Wi-Fi locations.
- **Dramatically reduce complexity** with a 100% cloud-based solution that can be rapidly scaled, with no hardware or software to deploy or manage.
- **Improve DNS resilience and reliability** with our carrier-grade global intelligent platform.

Cloud-based Management Portal

Policy management is quick and easy, and changes can be pushed out globally in minutes to ensure that your guest Wi-Fi locations are protected instantly. Email alerts can be configured to alert IT teams about critical policy events so that immediate remediation steps can be taken to identify and resolve potential risks. A real-time dashboard provides an instant overview of what Enterprise Threat Protector is seeing, and detailed information on any activity can be gathered by drilling down into individual dashboard elements. This detailed information provides a valuable resource for analysis and remediation of incidents.

All portal functionality can be accessed via APIs, and DNS data logs can be exported a SIEM, allowing Enterprise Threat Protector to easily and effectively integrate with other security solutions. All configuration and ongoing management of Enterprise Threat Protector is accomplished through our cloud-based Luna Portal, enabling management from any location at any time.

Key Capabilities

- **Acceptable Use Policies:** Enforce Guest Wi-Fi Acceptable Use policy and ensure compliance by limiting which content categories can and cannot be accessed.
- **Black and White List Domains:** Customize policies by blocking or allowing specific domains.
- **Policy Management:** Create a single policy for all guest Wi-Fi locations or create policies for individual locations.
- **Analysis and Reporting:** Real-time insight into all outbound enterprise DNS traffic, threat, and AUP events.
- **Logging:** Retain DNS logs for 30 days, which can be easily integrated into a SIEM for further analysis.
- **DNSSEC:** All DNS requests sent to Enterprise Threat Protector have DNSSEC enabled.

©2018 IBM Corporation and Akamai Technologies, Inc. All Rights Reserved. IBM, the IBM logo, ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Akamai and the Akamai wave logo are registered trademarks.