

# ENTERPRISE THREAT PROTECTOR (ETP)

Advanced Threat Protection in the Cloud



SECURITY	Guest Wi-Fi	Intelligence	Advanced Threat
Block malware, ransomware, and phishing delivery domains		X	X
Block malware command and control (CnC) requests		X	X
Identify DNS-based data exfiltration		X	X
Proxy risky domains for requested HTTP and HTTPS URL inspection		X	X
Real-time inline analysis of risky HTTP and HTTPS payloads using multiple inline malware analysis and detection engines			X
Real-time inline analysis of files downloaded from file sharing sites			X
Create a customized list of domains for HTTP and HTTPS URL inspection		X	X
Create a customized list of domains for inline payload analysis			X
Lookback analysis of customer traffic logs to identify and alert on newly discovered threats		X	X
Create custom allow/deny lists		X	X
Incorporate additional threat intelligence feeds		X	X
Customizable error pages	X	X	X
Query Akamai's threat database to gain intelligence on malicious domains and URLs		X	X
Enforce security for off-network laptops (Windows and macOS)		X	X
ACCEPTABLE USE POLICY (AUP)	Guest Wi-Fi	Intelligence	Advanced Threat
Monitor or block AUP violations for on-network and off-network users	X <sup>1</sup>	X	X
Enforce SafeSearch for Google, Bing, and YouTube	X	X	X
REPORTING, MONITORING, AND ADMINISTRATION	Guest Wi-Fi	Intelligence	Advanced Threat
Enterprise-wide view of all activity with customizable dashboards	X <sup>2</sup>	X	X
Detailed analysis of all threat and AUP events	X <sup>2</sup>	X	X
Full logging and visibility of all onboarded traffic requests and threat and AUP events	X <sup>2</sup>	X	X
Log delivery of all logs; logs are retained for 30 days and can be exported via an API	X <sup>2</sup>	X	X
Configuration, custom security lists, and events available via an open API	X <sup>2</sup>	X	X
Integrate with other security systems, such as SIEMs, via an open API	X	X	X
Email-based real-time security and AUP alerts	X <sup>2</sup>	X	X
Schedule daily or weekly email reports	X	X	X
Delegated administration	X	X	X
AKAMAI INTELLIGENT EDGE PLATFORM™	Guest Wi-Fi	Intelligence	Advanced Threat
Dedicated IPv4 and IPv6 VIPs per customer for recursive DNS	X	X	X
SLA for 100% availability	X	X	X
Anycast DNS routing for optimal performance	X	X	X
DNSSEC enforced for increased security	X	X	X
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		X	X
Auto-updating of Enterprise Client Connector		X	X
Enterprise Security Connector for identifying the IP addresses and machine names of endpoint devices		X	X

<sup>1</sup> ETP Guest Wi-Fi does not include off-network AUP enforcement.

<sup>2</sup> ETP Guest Wi-Fi does not include any security controls so alerts, analysis, dashboards, and logs only include AUP events and activity.

# ENTERPRISE THREAT PROTECTOR (ETP)

Advanced Threat Protection in the Cloud



Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit [www.akamai.com](http://www.akamai.com), [blogs.akamai.com](http://blogs.akamai.com), or [@Akamai](https://twitter.com/Akamai) on Twitter. You can find our global contact information at [www.akamai.com/locations](http://www.akamai.com/locations). Published 09/18.