ENTERPRISE THREAT PROTECTOR (ETP)

クラウドでの高度な脅威防御

セキュリティ	Guest Wi-Fi	Intelligence	Advanced Threat
マルウェア、ランサムウェア、およびフィッシング配信ドメインをブロック		√	√
マルウェア CnC リクエストをブロック		√	√
DNS ベースのデータ窃盗を特定		√	√
リスクの高いドメインをプロキシ経由させ、リクエストされた HTTP および HTTPS URL を検査		√	√
複数のインラインマルウェア分析および検出エンジンを使用して、リスクの高い HTTP および HTTPS ペイロードのリアルタイムインライン分析を実行			√
ファイル共有サイトからダウンロードされたファイルのリアルタイムインライン分析			√
HTTP および HTTPS URL 検査用にカスタマイズされたドメインリストの作成		√	√
インラインペイロード分析用にカスタマイズされたドメインリストの作成			√
新しく発見された脅威の識別とアラートを目的としたお客様のトラフィックログのルックバック分析		√	√
許可／拒否のカスタムリストの作成		√	√
追加の脅威インテリジェントフィードの統合		√	√
カスタマイズ可能なエラーページ	√	√	√
悪意のあるドメインおよび URL に関するインテリジェンスの獲得を目的とした Akamai 脅威データベースへのクエリー		√	√
オフネットワークのノートパソコン（Windows および macOS）のセキュリティの強化		√	√
Acceptable Use Policy（利用規定／AUP）	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
オンネットワークおよびオフネットワークのユーザーに関する AUP 違反のモニタリングまたはブロック	√[1]	√	√
Google、Bing、YouTube に対するセーフサーチの強化	√	√	√
レポート、モニタリング、管理	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
エンタープライズ全体のすべてのアクティビティをカスタマイズ可能なダッシュボードに表示	√[2]	√	√
すべての脅威および AUP イベントの詳細な分析	√[2]	√	√
オンボーディングされたすべてのトラフィックリクエストおよび脅威イベントと AUP イベントの完全なロギングおよび可視化	√[2]	√	√
すべてのログのログ配信：ログは 30 日間保持され API を通じてエクスポート可能	√[2]	√	√
設定、カスタム・セキュリティ・リスト、およびイベントをオープン API で利用可能	√[2]	√	√
SIEM などの他のセキュリティシステムとオープン API を通じて統合	√	√	√
E メールベースのリアルタイムのセキュリティおよび AUP アラート	√[2]	√	√
日次または週次の E メールレポートのスケジュール設定	√	√	√
管理者の委任	√	√	√
AKAMAI INTELLIGENT EDGE PLATFORM™	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
再帰 DNS のお客様別専用 IPv4 および IPv6 VIP	√	√	√
可用性 100% の SLA	√	√	√
最適なパフォーマンスを実現する Anycast DNS ルーティング	√	√	√
DNSSEC の実施によるセキュリティの強化	√	√	√
ENTERPRISE CONNECTOR	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Enterprise Client Connector によるオフネットワークのノートパソコン（Windows および OSX）の保護、およびオフネットワークとオンネットワークのイベントへのマシン名の報告		√	√
Enterprise Client Connector の自動更新		√	√
Enterprise Security Connector によるエンドポイントデバイスの IP アドレスおよびマシン名の識別		√	√

[1] ETP ゲスト Wi-Fi にはオフネットワークの AUP 実施は含まれません。

[2] ETP ゲスト Wi-Fi にはセキュリティ制御は含まれません。そのため、AUP イベントとアクティビティを含むのはアラート、分析、ダッシュボード、ログのみです。

ENTERPRISE THREAT PROTECTOR (ETP)

クラウドでの高度な脅威防御