Enterprise Threat Protector

Fortschrittlicher Bedrohungsschutz in der Cloud

Immer mehr Unternehmen setzen auf Direct Internet Access (DIA), SaaS-Anwendungen, Cloudservices, Mobilität und das Internet of Things (IoT). Doch durch diese Technologien vergrößern sie gleichzeitig erheblich ihre Angriffsfläche und sehen sich so einer Vielzahl neuer Herausforderungen gegenüber. Denn der Schutz von Unternehmen und Nutzern vor gezielten Bedrohungen wie Malware, Phishing und Datenextraktion wird zusehends komplexer. Die entsprechenden Teams haben mit komplexen Sicherheitskontrollen sowie Sicherheitslücken in alten Lösungen zu kämpfen.

Enterprise Threat Protector (ETP) ist ein Secure Internet Gateway (SIG), mit dem Ihre Sicherheitsteams gewährleisten können, dass Nutzer und Geräte unabhängig von ihrem Standort sichere Internetverbindungen herstellen können – ohne die Komplexität, die mit alten Sicherheitslösungen einhergeht. Enterprise Threat Protector basiert auf den Echtzeit-Bedrohungsinformationen, die Akamai aus seinen unvergleichlichen globalen Einblicken in Internet- und DNS-Traffic (Domain Name System) gewinnt.

Enterprise Threat Protector

Enterprise Threat Protector (ETP) basiert auf der Akamai Intelligent Edge Platform™ sowie unserem Carrier-Grade-Service für das rekursive DNS und ist ein SIG, das sich schnell und einfach konfigurieren und implementieren lässt, ohne dass hierfür Hardware installiert oder gewartet werden müsste.

Enterprise Threat Protector nutzt in Echtzeit die Akamai Cloud Security Intelligence und die bewährte globale Plattform von Akamai und erkennt so proaktiv gezielte Bedrohungen wie Malware, Ransomware, Phishing und DNS-basierte Datenextraktion. Über das Akamai-Portal können IT-Teams zentral und in Minutenschnelle Sicherheits- und Nutzungsrichtlinien für sämtliche Mitarbeiter erstellen, implementieren und durchsetzen – egal, von wo aus sich diese Mitarbeiter mit dem Internet verbinden.

swisscom

Funktionsweise

Enterprise Threat Protector verwendet mehrere Verteidigungsebenen (DNS, URL und Inline-Payload-Analyse) und schafft so perfekte Sicherheit, ohne die Komplexität zu steigern oder die Performance zu beeinträchtigen.

DNS-Untersuchung: Durch einfache Umleitung Ihres externen DNS-Traffics (rekursives DNS) an Enterprise Threat Protector werden sämtliche angeforderten Domains anhand der Echtzeit-Risikobewertungen aus den Akamai-Bedrohungsinformationen überprüft. Nutzer werden proaktiv daran gehindert, auf schädliche Domains und Services zuzugreifen, während Anfragen für sichere Domains und Services aufgelöst werden. Da diese Überprüfung stattfindet, bevor die IP-Verbindung hergestellt wird, werden Bedrohungen bereits in frühen Phasen der Kill Chain abgewehrt. Darüber hinaus ist das DNS über alle Ports und Protokolle hinweg aktiv, sodass Sie auch vor Malware geschützt sind, die sich nicht auf standardmäßige Webports und -protokolle verlässt. Domains können auch auf ihren Inhalt hin überprüft werden, um Nutzer am Zugriff auf Inhalte zu hindern, die gemäß Nutzungsrichtlinie ungeeignet sind.

URL-Untersuchung: Domains, die basierend auf den Akamai-Bedrohungsinformationen als riskant eingestuft werden, werden automatisch an einen Cloud-Proxy auf der Akamai Intelligent Edge Platform umgeleitet. Die angeforderte URL wird anhand der URL-Bedrohungsinformationen von Akamai überprüft, und schädliche URLs werden automatisch blockiert. Der Proxy untersucht sowohl HTTP- als auch HTTPS-URLs.

Inline-Payload-Analyse: Die HTTP- und HTTPS-Payloads verdächtiger Domains werden mithilfe verschiedener fortschrittlicher Engines zur Malware-Erkennung in Echtzeit untersucht. Diese Engines verwenden unterschiedliche Technologien, einschließlich signaturbasierter und signaturloser Erkennung sowie maschinellem Lernen. So lässt sich ein umfassender Zero-Day-Schutz vor potenziell schädlichen Dateien, wie z. B. Programmdateien und Dokumenten, sowie vor in angeforderte Webseiten eingebetteter Malware, wie z. B. versteckter schädlicher JavaScript-Code, gewährleisten.

Enterprise Threat Protector lässt sich mühelos in andere Sicherheitsprodukte und Reportingtools integrieren, einschließlich Firewalls, SIEM-Systeme und externe Bedrohungsfeeds. So können Sie sämtliche Investitionen in die Sicherheit maximieren.

Darüber hinaus können Sie mit der Bereitstellung des kompakten Enterprise Client Connector schnell eine zusätzliche proaktive Schutzebene hinzufügen, wenn Laptops außerhalb des Netzwerks verwendet werden.

Vorteile

Erhöhte Sicherheit dank proaktiver Blockierung von Anfragen für Websites, auf denen Malware und Ransomware gehostet wird, CnC-Server (Command and Control) sowie DNS-Datenextraktions- und Phishing-Domains – basierend auf unseren umfassenden und topaktuellen Bedrohungsinformationen

Reduzierter Zeitaufwand für die Sicherheitsverwaltung durch die Minimierung von False Positives, die Reduzierung der Warnungen anderer Sicherheitsprodukte und die blitzschnelle, ortsunabhängige Verwaltung von Sicherheitsrichtlinien und -updates, um sämtliche Standorte zu schützen

Verbesserter Schutz ohne zusätzliche Komplexität oder Hardware mit einer zu 100 % cloudbasierten Lösung, die in Minutenschnelle und ohne Unterbrechungen für Nutzer konfiguriert und bereitgestellt werden kann und sich blitzschnell skalieren lässt

Blockieren schädlicher Payloads für besseren Zero-Day-Schutz durch Echtzeituntersuchung angeforderter Dateien und Webinhalte, um Bedrohungen abzuwehren, bevor sie Endgeräte erreichen und infizieren

Geringeres Risiko und mehr Sicherheit für Laptops außerhalb des Netzwerks – ganz ohne VPN dank des kompakten Enterprise Security Connector, der Ihre Sicherheits- und Nutzungsrichtlinien durchsetzt

Schnelle und einheitliche Durchsetzung von Compliance-Vorgaben und Nutzungsrichtlinien, die den Zugriff auf ungeeignete oder unzulässige Domains und Inhaltskategorien blockieren

Verbesserte DIA-Performance dank des Einsatzes von Proxys für verdächtigen Traffic, sodass die URL untersucht und die Payload analysiert werden kann

Gesteigerte DNS-Ausfallsicherheit und -zuverlässigkeit dank Akamai Intelligent Edge Platform

Akamai Cloud Security Intelligence (CSI)

Enterprise Threat Protector wird durch Akamai Cloud Security Intelligence unterstützt. Dieser Service stellt Echtzeitdaten zu Bedrohungen sowie zu den Risiken bereit, die diese Bedrohungen für Unternehmen darstellen.

Die Bedrohungsinformationen von Akamai bieten Schutz vor aktuellen relevanten Bedrohungen, die sich auf Ihr Unternehmen auswirken könnten, und minimieren die Anzahl von False Positives, die Ihre Sicherheitsteams untersuchen müssen.

Die Informationen basieren auf den Daten, die wir rund um die Uhr über die Akamai Intelligent Edge Platform gewinnen. Hier werden täglich 30 % des globalen Webtraffics bereitgestellt und bis zu 2,2 Milliarden DNS-Abfragen beantwortet. Die gewonnenen Daten werden durch eine Vielzahl externer Bedrohungsfeeds ergänzt, und die kombinierten Datensätze werden dann ausführlich analysiert und mithilfe verschiedener Verhaltensanalysen, maschineller Lerntechnologien und eigens entwickelter Algorithmen untersucht. Werden hierbei neue Bedrohungen erkannt, werden diese umgehend zu Enterprise Threat Protector hinzugefügt, sodass Echtzeitschutz gewährleistet wird.

Akamai Intelligent Edge Platform

Enterprise Threat Protector basiert auf der Akamai Intelligent Edge Platform, einer Carrier-Grade-Plattform, die sicher, zuverlässig und schnell agiert. Dank ihrer globalen Verteilung erreicht die Plattform eine Verfügbarkeit von 100 %, die wir auch durch unsere Service Level Agreements garantieren. Damit bieten wir Unternehmen optimale Servicezuverlässigkeit im Hinblick auf das rekursive DNS.

Cloudbasiertes Managementportal

Sämtliche Konfigurations- und Verwaltungsaktivitäten von Enterprise Threat Protector erfolgen über das cloudbasierte Luna-Portal von Akamai. So können Sie den Service jederzeit und von überall aus problemlos managen.

Richtlinien lassen sich schnell und einfach verwalten, und Änderungen können in Minutenschnelle global verteilt werden. Damit sind Ihre Standorte und Mitarbeiter optimal geschützt. Sie können Echtzeit-Benachrichtigungen per E-Mail sowie geplante Berichte konfigurieren, um Sicherheitsteams über kritische Richtlinienereignisse zu informieren, damit diese sofort reagieren und potenzielle Bedrohungen schnell erkennen und abwehren können. Ein Echtzeit-Dashboard bietet eine Übersicht über den Traffic sowie über Bedrohungs- und Nutzungsrichtlinien-Ereignisse. Ausführliche Informationen zu sämtlichen Aktivitäten können über detaillierte Ansichten oder individuelle Dashboard-Elemente angezeigt werden. Diese detaillierten Informationen stellen wertvolle Ressourcen für die Analyse und Behebung von Sicherheitsvorfällen dar.

Sämtliche Portalfunktionen sind per API verfügbar, und die Datenprotokolle können an ein SIEM-System exportiert werden. So lässt sich Enterprise Threat Protector einfach und effektiv in Ihre vorhandenen Sicherheitslösungen und Reportingtools integrieren.

Akamai Umgebung

Die Akamai Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Unsere umfassenden Lösungen werden über das einheitliche, individuell anpassbare Luna Control Center verwaltet, das für Transparenz und Kontrolle sorgt, und von Professional-Services-Experten unterstützt, die Ihnen bei der Einrichtung helfen und Innovationsmöglichkeiten aufzeigen.

Weitere Informationen zu Enterprise Threat Protector sowie eine kostenlose Testversion finden Sie auf www.akamai.com/etp.

Wichtige Funktionen

Bedrohungskategorisierung durch Akamai: Topaktuelle Bedrohungsinformationen, die auf den unvergleichlichen Einblickenvon Akamai in 15 bis 30 % des Webtraffics basieren, werden mit ca. 2,2 Billionen täglichen DNS-Anfragen an unsere Cloud für rekursives DNS kombiniert.

Bedrohungskategorisierung durch Kunden: Sicherheitsteams können die verfügbaren Threat-Intelligence-Feeds schnell integrieren und somit den Wert aktueller Sicherheitsinvestitionen steigern.

Inline-Payload-Analyse in Echtzeit: Drei fortschrittliche Engines zur Malwareerkennung finden und blockieren komplexe fortschrittliche Bedrohungen und verbessern den Zero-Day-Schutz.

Protokollierung: Trafficprotokolle werden 30 Tage lang gespeichert und können einfach in eine CSV-Datei exportiert oder zur weiteren Analyse in ein SIEM-System integriert werden.

Nutzungsrichtlinien: Setzen Sie Nutzungsrichtlinien durch, und gewährleisten Sie Compliance durch Beschränkung der zulässigen bzw. unzulässigen Inhaltskategorien.

Analyse und Reporting: Dashboards bieten Echtzeiteinblicke in sämtlichen ausgehenden Webtraffic sowie in Bedrohungs- und Nutzungsrichtlinien-Ereignisse.

Sicherheitseinblicke: Finden Sie schnell heraus, warum Akamai eine Domain oder URL zu den Listen mit Bedrohungsinformationen hinzugefügt hat.

DNSSEC: Für sämtliche an Enterprise Threat Protector gesendeten DNS-Anfragen ist DNSSEC aktiviert.

Akamai Intelligent Edge Platform™	Guest Wi-Fi	Intelligence	Advance Threat
Dedizierte IPv4- und IPv6-VIPs pro Kunde für rekursives DNS	✓	✓	✓
SLA für 100-prozentige Verfügbarkeit	✓	✓	✓
Anycast-DNS-Routing für optimale Performance	✓	✓	✓
Durchsetzen von DNSSEC zur Erhöhung der Sicherheit	✓	✓	✓

Enterprise Connectors	Guest Wi-Fi	Intelligence	Advance Threat
Enterprise Client Connector zum Schutz von Laptops außerhalb des Netzwerks (Windows und OS X) und zur Ermittlung des Gerätenamens bei Ereignissen inner- und außerhalb des Netzwerks		✓	✓
Automatische Updates des Enterprise Client Connector		✓	✓
Enterprise Security Connector zur Erkennung der IP-Adressen und Namen von Endgeräten		✓	✓

Sicherheit

	Guest Wi-Fi	Intelligence	Advance Threat
Blockieren von Malware, Ransomware sowie Phishing-Domains und -URLs		✓	✓
Blockieren von Malware-C2-Anfragen (Command and Control)		✓	✓
Erkennen DNS-basierter Datenextraktion		✓	✓
Proxy für gefährliche Domains zur Untersuchung angeforderter HTTP- und HTTPS-URLs		✓	✓
Proxy für den gesamten Webtraffic für DNS-, URL- und Payload-Analyse			✓
Inline- und Offline-Echtzeitanalyse von HTTP- und HTTPS-Payloads mit verschiedenen Engines für Malware-Analyse und -Erkennung*			✓
Cloud-Sandbox für die dynamische Offlineanalyse von Payloads			✓
Inline-Echtzeitanalyse von Webseiten zur Erkennung von Zero-Day-Phishing-Seiten*			✓
Inline- oder Offline-Echtzeitanalyse der von Filesharing-Sites heruntergeladenen Dateien			✓
Erstellen individueller Domainlisten zur HTTP- und HTTPS-URL-Untersuchung		✓	✓
Erstellen individueller Domainlisten zur Inline-/Offline-Payload-Analyse			✓
Rückblickende Analyse der Kunden-Trafficprotokolle zur Erkennung neu entdeckter Bedrohungen		✓	✓
Erstellen nutzerdefinierter White-/Blacklists		✓	✓
Einbinden zusätzlicher Feeds mit Bedrohungsinformationen		✓	✓
Anpassbare Fehlerseiten	✓	✓	✓
Abfragen der Akamai-Bedrohungsdatenbank, um Informationen zu schädlichen Domains und URLs einzuholen		✓	✓
Sicherheit auf Laptops außerhalb des Netzwerks (Windows und macOS)		✓	✓

Nutzungsrichtlinie

	Guest Wi-Fi	Intelligence	Advance Threat
Erstellen gruppenbasierter Nutzungsrichtlinien			✓
Überwachen oder Blockieren von Verstößen gegen die Nutzungsrichtlinie durch Nutzer innerhalb und außerhalb des Netzwerks	✓ [1]	✓	✓
Durchsetzen von SafeSearch für Google, Bing und YouTube	✓	✓	✓

Reporting, Überwachung und Verwaltung	Guest Wi-Fi	Intelligence	Advance Threat
Unternehmensweite Übersicht aller Aktivitäten dank anpassbarer Dashboards	✓ 2	✓	✓
Detaillierte Analyse aller Bedrohungs- und Nutzungsrichtlinien-Ereignisse	✓ 2	✓	✓
Vollständige Protokollierung und Transparenz sämtlicher Trafficanfragen und Bedrohungs-/ Nutzungsrichtlinien-Ereignisse	✓ 2	✓	✓
Bereitstellung sämtlicher Protokolle: Protokolle werden 30 Tage lang aufbewahrt und können per API exportiert werden	✓ 2	✓	✓
Konfiguration, nutzerdefinierte Sicherheitslisten und Ereignisse über offene API verfügbar	✓ 2	✓	✓
Integration in andere Sicherheitssysteme, wie z. B. SIEMs, per offener API	✓	✓	✓
E-Mail-basierte Echtzeitbenachrichtigungen zu Sicherheits- und Nutzungsrichtlinien-Ereignissen	✓ 2	✓	✓
Planung täglicher oder wöchentlicher E-Mail-Berichte	✓	✓	✓
Delegierte Verwaltung	✓	✓	✓

* Die Cloud-Sandbox ist ein optionales Add-on und für die Offlineanalyse großer Dateien erforderlich.
1) ETP Guest Wi-Fi umfasst nicht die Durchsetzung der Nutzungsrichtlinie außerhalb des Netzwerks.
2) ETP Guest Wi-Fi umfasst keine Sicherheitskontrollen. Daher decken Warnungen, Analysen, Dashboards und Protokolle nur Nutzungsrichtlinien-Ereignisse und -Aktivitäten ab.

www.swisscom.com/digital-media
+41 58 221 76 21
digital.media@swisscom.com

Copyright © 2021 Swisscom Broadcast AG