AKAMAI-PRODUKTBESCHREIBUNG

Produktbeschreibung Brand Protector

Erkennen und stoppen Sie Phishing-Websites, gefälschte Shops und Markenimitationen, um Schaden für Endnutzer zu vermeiden und das Risiko von groß angelegten Betrugs- und Missbrauchsangriffen zu reduzieren.

Ihre bekannte Marke schafft messbaren Mehrwert – sowohl außerhalb als auch innerhalb Ihres Unternehmens. Indem Sie Ihre Markenelemente schützen, kann Ihr Unternehmen die Kundenbindung nicht nur aufrechterhalten, sondern sogar steigern, und gleichzeitig Verluste, Produktivitätseinbußen und schlechtes Kundenfeedback minimieren. Aus Sicherheitsperspektive unterbricht die Kontrolle von Markenimitationen die Kill Chain und verhindert so das Abgreifen von Anmeldedaten und Kontomissbrauch.

Nicht alle Angriffe zielen auf das Haupttor eines Unternehmens ab. Überall im Internet geben sich Angreifer mit digitalen Nachahmungen als Ihre Marke aus, um vertrauliche Daten, Anmeldedaten und Direktzahlungen von Ihren Kunden abzugreifen. Markenimitationen und Phishing werden zunehmend zu einer ressourcenintensiven Herausforderung, da sie dank kurzer Dauer und ständig wechselnden Standorten der Kampagnen schwer zu erkennen und zu beseitigen sind.

Akamai Brand Protector nutzt eine der größten Threat-Intelligence-Datenbanken und kombiniert Datenfeeds von Erst- und Drittanbietern, um die Erkennung zu beschleunigen und die Genauigkeit zu verbessern. Integrierte Abwehrfunktionen machen Brand Protector zu einem effektiven und unverzichtbaren Tool zur frühzeitigen Verhinderung von Betrug und Missbrauchsangriffen.

Akamai Brand Protector erkennt und verhindert gezielte Angriffe wie Phishing, Imitationen und Markenmissbrauch über Websites, soziale Medien und App-Marketplaces hinweg. Und was noch wichtiger ist: Mit Brand Protector schützen Sie Ihre vertrauensvollen Beziehungen.

Jede Woche werden mehr als 50.000 neue Phishing-Websites erstellt. Brand Protector untersucht täglich Billionen digitaler Aktivitäten aus internen und externen Quellen, um den Missbrauch der Marke oder der Markenelemente Ihres Unternehmens schnell und effizient aufzudecken – und das häufig, bevor ein Angriff gestartet wird.

Um all dies zu erreichen, nutzt Brand Protector einen vierstufigen Ansatz zur Bewältigung betrügerischer Imitationen: Informationsgewinnung, Erkennung, Transparenz und Abwehr.

Vorteile für Ihr Unternehmen

Zuverlässige Angriffserkennung
Unser proprietäres globales Netzwerk und zusätzliche Feeds sind ein einzigartiger Vorteil bei der Erkennung von Markenimitierungen.

Genauigkeit und Geschwindigkeit
Unsere schnelle algorithmische Erkennung kann noch vor dem Start von Angriffskampagnen Warnungen ausgeben und False Positives minimieren.

Umsetzbare Erkenntnisse
Umfassende Daten werden als verwertbare Erkenntnisse bereitgestellt, wobei Risikobewertungen den Schweregrad und die Reichweite des Angriffs auf einen Blick zusammenfassen.

Transparenz für jeden Kunden
Informationsgewinnung speziell für Ihre Marke, Ihre Produkte und zugehörige Elemente auf Websites, in den sozialen Medien und auf App-Marketplaces.

Nutzerfreundlichkeit
Erhalten Sie Echtzeiteinblicke und leiten Sie innerhalb von Minuten Gegenmaßnahmen für diesen wachsenden Angriffsvektor ein.

Seitenschließung und Abwehr
Nutzen Sie den in Brand Protector integrierten Service zur Seitenschließung oder unterbrechen Sie den Traffic mit einer Warnung für sicheres Surfen, um produktiv zu bleiben.

Informationsgewinnung

Die Herausforderung bei der Erkennung von Phishing und Markenimitationen beginnt in der Phase der Informationsgewinnung und Datenerfassung.

Als weltweit größte Edge- und Cloudplattform analysiert der proprietäre Überblick von Akamai über den weltweiten Webtraffic täglich über 788 TB an Daten. Die von Brand Protector gewonnenen Informationen werden durch Datenfeeds von Drittanbietern erweitert, um einen ganzheitlichen Einblick in Angriffsaktionen zu erhalten. Außerdem können Sie Ihre eigene URL und Domains zur Analyse durch die Brand Protector Detection Cloud hinzufügen.

Erkennung

Die schnelle und präzise Erkennung von Brand Protector basiert auf einer Kombination aus dem proprietären Feed zur Informationsgewinnung von Akamai und Analysealgorithmen, die die Erkennung und Genauigkeit verbessern und die Rate der False Positives senken.

Markenangriffe automatisieren schädliche, kurzlebige Websites. Die meisten Technologien sind nicht schnell genug, um diese Angriffsressourcen zu erkennen und abzuwehren, bevor sie Ihre Kunden beeinträchtigt haben. Der Ansatz von Akamai ist anders: Wir verfolgen den Traffic in Echtzeit, um Markenmissbrauch zu erkennen, anstatt sich auf aktualisierte Listen oder verzögerte Feeds zu verlassen. Mit Brand Protector kann Ihr Sicherheitsteam Phishing-Websites erkennen, sobald die erste HTTP/HTTPS-Anfrage erfolgt – und damit oft bevor die Kampagne Ihre Kunden erreicht.

Transparenz

Das kundenorientierte Design bietet Sicherheitsteams in einer einzigen Dashboard-Ansicht wichtige Einblicke in die Sicherheit.

Informationen werden empfangen und die Datensignale durch eine Reihe heuristischer und KI-Detektoren geleitet. Obwohl eine überwältigende Menge an Daten und Beweisen erfasst wird, bietet die vereinfachte Nutzeroberfläche von Akamai einen Überblick über aktive Bedrohungen für Ihre Kunden in Bezug auf Imitationen.

Kundenspezifischer Traffic sowie Bedrohungserkennungen und -daten werden im Kundenportal von Akamai zu umsetzbaren Erkenntnissen. Die Ergebnisse werden nach einer zusammengefassten Bedrohungsbewertung geordnet. Klicken Sie auf eine Warnung, um analysierte Bedrohungsdaten anzuzeigen, einschließlich Konfidenzwert, Bewertung des Schweregrads, Anzahl der betroffenen Nutzer und eine Zeitleiste der Angriffsereignisse.

Jede Erkennung wird durch Beweise unterstützt – Sie können den Code, Screenshots, Erkennungsindikatoren und Domaininformationen in einem einzigen Erkennungs-bildschirm anzeigen lassen.

Abwehr

Integrierte Services zur Seitenschließung schließen den Kreislauf und bekämpfen Markenbetrug.

Mit Brand Protector kann Ihr Team direkt auf dem Erkennungsbildschirm eine Anfrage zur Schließung der missbräuchlichen Website stellen. Anfragen zur Seitenschließung (die an einen Partner von Akamai gesendet werden) für Brand Protector werden automatisch mit den Erkennungsbeweisen und zusätzlichen Informationen kombiniert, um die Verwendung zu vereinfachen. Sie können den Abwehrstatus im Portal verfolgen und anzeigen.

Entwickelt für Ihre Marke

Zonenschutz
Diese Lösung aus unserem Edge-Sicherheitsportfolio kann die Sicht Ihres Sicherheitsteams auf den Schutz früh in der Kill Chain erweitern. Sie sucht proaktiv nach Permutationen der Domains Ihrer Marke, durch die Ihre Kunden zu Phishing-Opfern werden können.

Überwachung der sozialen Medien
Da auch in den sozialen Medien zunehmend Markenimitationen auftreten, erkennt und neutralisiert unsere neue erweiterte Überwachungsfunktion für soziale Medien Online-Betrug und schützt Ihre Marke und Kunden auf verschiedenen Plattformen.

Erkennung gefälschter Apps
Die Überwachung von App-Marketplaces ist eine neue Funktion, die offizielle und inoffizielle App-Repositorys durchsucht, um gefälschte Anwendungen zu erkennen, die Ihre Markenidentität missbrauchen, und eine umfassende Verteidigung in der gesamten digitalen Landschaft zu bieten.