AKAMAI-PRODUKTBESCHREIBUNG

Account Protector

Halten Sie Betrüger fern und das Vertrauen intakt – mit Schutz vor Kontomissbrauch

Wie können Sie echte Nutzer von Betrügern unterscheiden? Ihre Kunden verlassen sich darauf, dass Sie dazu in der Lage sind.

Angesichts der Tatsache, dass digitale Transaktionen stark an Bedeutung gewinnen und immer wieder neue digitale Assets eingeführt werden, sind die Risiken und Folgen von Kontomissbrauch schwerwiegender als je zuvor. Ihre Fähigkeit, Ihr digitales Geschäft auszubauen und Ihre Kunden zu schützen, hängt davon ab, ob Sie in einem Umfeld, in dem sich Betrugstaktiken ständig weiterentwickeln, das Vertrauen aufrechterhalten können.

Der Missbrauch von Konten, ob in Form einer betrügerischen Eröffnung von Konten (Betrug mit Neukonten) oder einer Kontoübernahme (Account Takeover, ATO), stellt Unternehmen in allen Branchen vor erhebliche Herausforderungen und Kosten. So können kompromittierte und gefälschte Konten verheerende finanzielle Folgen und Reputationsschäden nach sich ziehen. Wenn ein Konto kompromittiert wird, können Angreifer frei darüber verfügen: Sie können es leeren, betrügerische Transaktionen durchführen, Sicherheitsfunktionen wie MFA deaktivieren oder vertrauliche personenbezogene Daten stehlen. Gefälschte Konten können hingegen eingesetzt werden, um Werbeaktionen wie kostenlose Testversionen und Gutschriften auszunutzen, SMS-Pumping zu betreiben und Plattformen mit Spam oder unangemessenen Inhalten zu überfluten. Die Auswirkungen solcher Angriffe sind erheblich – Unternehmen müssen das Risiko in Kauf nehmen, dass das Vertrauen der Kunden schwindet, Millionenbeträge durch Betrug verloren gehen und sie mit Geldstrafen und Reputationsschäden konfrontiert werden.

Akamai Account Protector

Account Protector ist eine Sicherheitslösung, die Kontomissbrauch während des gesamten Lebenszyklus eines Kontos verhindern soll. Sie greift auf maschinelles Lernen und einen beträchtlichen Datensatz mit Risiko- und Vertrauensindikatoren zurück, um die Rechtmäßigkeit einer Nutzeranfrage zu prüfen. Zudem analysiert sie das Verhalten in Echtzeit, um subtile Anzeichen betrügerischer Aktivitäten bei der Kontoerstellung, der Anmeldung oder sonstigen Aktivitäten zu identifizieren. Sobald verdächtiges oder ungewöhnliches Verhalten erkannt wurde, stellt Account Protector sofortige Abwehroptionen bereit, darunter Sperrungen und Maßnahmen an der Edge, die Bewältigung kryptografischer und verhaltensbezogener Herausforderungen, die Bereitstellung alternativer Inhalte und vieles mehr. Auf diese Weise gewährleistet die Lösung ein nahtloses Nutzererlebnis.

Vorteile für Ihr Unternehmen

Gegenseitiges Vertrauen:
Wenn es Ihnen gelingt, die Rechtmäßigkeit von Interaktionen zu beurteilen, für ein reibungsloseres Nutzererlebnis zu sorgen und betrügerische Aktivitäten abzuwehren, wirkt dies vertrauensbildend.

Maßgeschneiderte Schutzmaßnahmen für Ihr Unternehmen:
Profitieren Sie von der automatisch optimierten Boterkennung und der Fähigkeit, Nutzerbestandsprofile zu verstehen, basierend auf der Art und Weise, wie Nutzer mit Ihrer Website interagieren.

Aussagekräftige Daten und Transparenz:
Treffen Sie auf der Grundlage transparenter Signale und Indikatoren fundierte Entscheidungen.

Verringerter Wiederherstellungsaufwand:
Reduzieren Sie die Kosten und Ressourcen, die Sie aufwenden müssen, um kompromittierte Konten zu untersuchen, gestohlene Assets zu ersetzen oder sonstige Maßnahmen zu ergreifen.

Datenbasierte Sicherheits- und Identitätsentscheidungen:
Durch die Anbindung von Betrugsabwehr-, SIEM und sonstigen Sicherheitstools werden die Risiko- und Vertrauenssignale von Account Protector auch dort nutzbar. Das steigert nicht nur die Genauigkeit, sondern auch den Mehrwert Ihrer Investitionen in diese Tools.

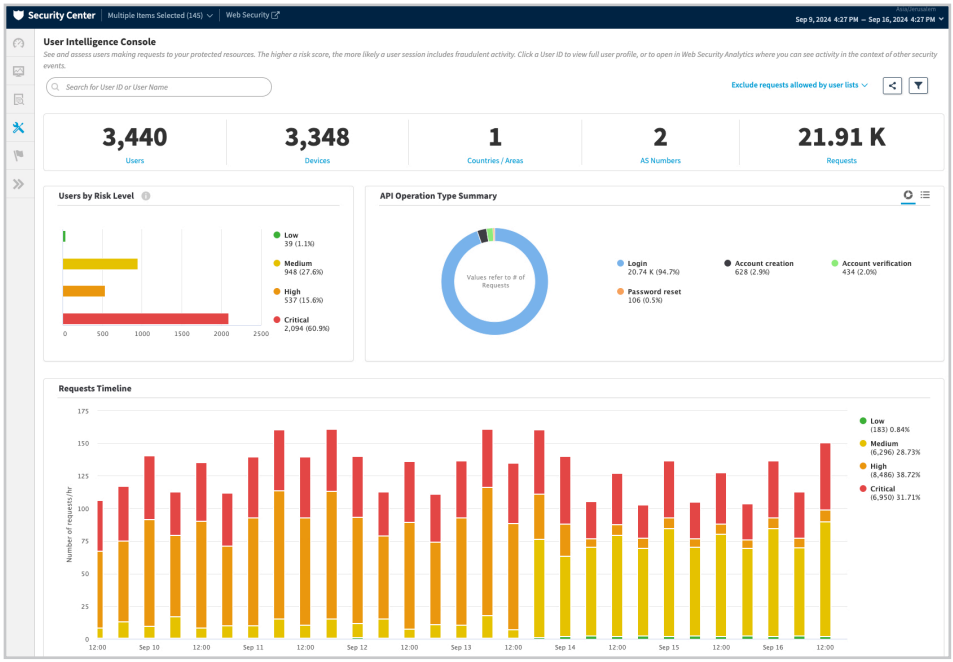
Ganzheitlicher Schutz vor Kontomissbrauch

Schützen Sie Nutzerkonten während ihres gesamten Lebenszyklus vor Missbrauch und sorgen Sie für erweiterten Schutz vor der missbräuchlichen Erstellung von Konten, Kontoübernahmen und anderen damit zusammenhängenden Angriffsmethoden.

Missbräuchliche Erstellung von Konten: Gehen Sie gegen die Erstellung gefälschter Konten vor, mit denen Werbeaktionen ausgenutzt, SMS-Pumping-Aktionen betrieben, gestohlene Kreditkarteninformationen getestet, Inventare gehortet und viele weitere Handlungen getätigt werden.

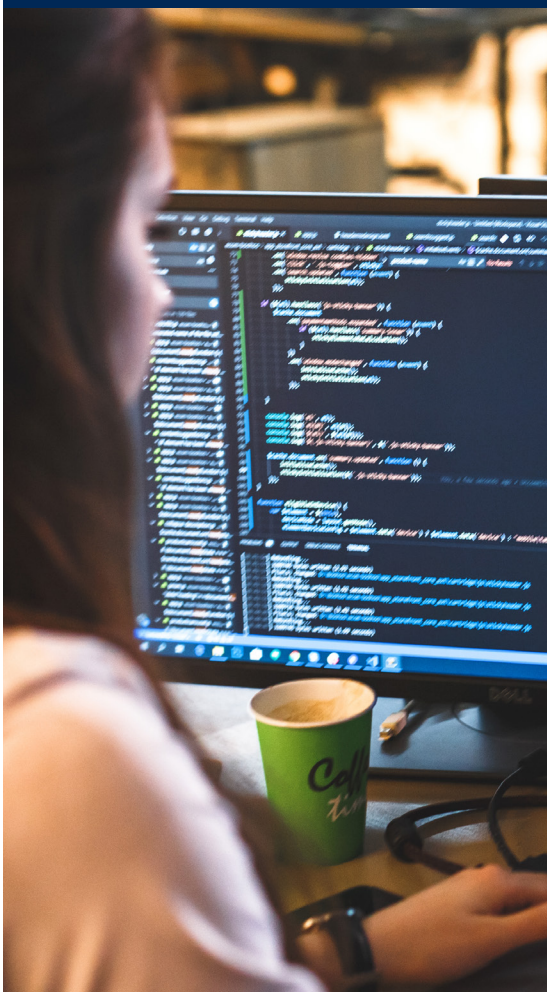
Kontoübernahme: Schützen Sie sich vor Betrügern, die Zugang zu legitimen Kundenkonten erlangen, um sie zu leeren, sensible Daten zu stehlen und betrügerische Transaktionen durchzuführen.

Raffinierte Bot-Angriffe: Schützen Sie Nutzerkonten vor Credential Stuffing, Bestandsmanipulation und anderen automatisierten Angriffen, die häufig zusammen mit der missbräuchlichen Erstellung von Konten oder ATO gestartet werden, um wertvolle Produkte, Geld oder andere wertvolle Assets zu stehlen.



Schutz, Vertrauen und optimale Nutzererlebnisse

Analysieren Sie Risiken und stoppen Sie Missbrauch in Echtzeit. Überwachen Sie Konten während des gesamten Lebenszyklus kontinuierlich auf Anzeichen verdächtiger Verhaltensweisen.



Wichtige Funktionen

Umfassender Kontenschutz während des gesamten Lebenszyklus: Identifizieren und analysieren Sie das Nutzerrisiko in jeder Phase, von der Kontoerstellung bis hin zu Aktivitäten nach der Anmeldung wie Kontoaktualisierungen, Passwortänderungen und Zahlungen.

Risikobewertungen von Nutzersitzungen in Echtzeit: Bewertet Risiken und Vertrauen während der gesamten Nutzersitzung, um zu bewerten, ob eine Nutzeranfrage von einem legitimen Nutzer oder einem Betrüger stammt.

E-Mail-Intelligence: Analysiert die Syntax einer E-Mail-Adresse und die abnormale Verwendung einer E-Mail, um schädliche Muster zu erkennen.

E-Mail-Domain-Intelligence: Wertet das Aktivitätsmuster einzelner E-Mail-Domains aus, einschließlich Einweg-Domains und übermäßiger Nutzung einer Domain.

Globale Erfassung vertrauenswürdiger Nutzer: Bietet Einblick in das Nutzerverhalten im gesamten Akamai-Netzwerk, um fundiertere Entscheidungen hinsichtlich der Vertrauenswürdigkeit eines Login zu treffen.

Nutzerverhaltensprofile: Die zuvor beobachteten Standorte, Netzwerke, Geräte, IP-Adressen und Aktivitätszeiten bilden die Grundlage für die Erstellung eines Verhaltensprofils, um wiederkehrende Nutzer zu erkennen.

Bestandsprofile: Durch die Zusammenfassung der Nutzerprofile des Unternehmens in einer Obermenge lassen sich Abweichungen im Verhalten auch mit dem gesamten Nutzerbestand vergleichen und so Anomalien erkennen.

Zuverlässigkeit des Ursprungs: Wie zuverlässig ein Ursprung ist, lässt sich anhand früherer schädlicher Aktivitäten beurteilen, die bei Akamai-Kunden beobachtet wurden. Dazu zählen auch viele der weltweit größten und am häufigsten attackierten Websites mit dem meisten Traffic.

Indikatoren: Risiko-, Vertrauens- und allgemeine Indikatoren fließen bei den einzelnen Anfragen in die Einschätzung des Risikos von Kontomissbrauch ein. Die Indikatoren werden zusammen mit der endgültigen Risikobewertung des Nutzers bereitgestellt und können zu Analysezwecken verwendet werden.

Fortschrittliche Boterkennung: Damit unbekannte Bots schon bei der ersten Interaktion erkennbar werden, kommt eine Vielzahl an KI-/ML-Modellen und -Techniken zum Einsatz. Dazu zählen unter anderem die Analyse von Nutzerverhalten/Telemetriedaten, Browser-Fingerprinting, automatisierte Browsererkennung, Erkennung von HTTP-Anomalien und hohe Anfrageraten.

Analyse und Reporting: Das Reporting erfolgt sowohl in Echtzeit als auch im Verlauf. So können Sie Aktivitäten an einzelnen Endpoints analysieren, einen bestimmten Nutzer untersuchen, Nutzer nach Risikostufe prüfen und umfassende Daten gewinnen.

Erweiterte Abwehrmaßnahmen: Verhindern Sie Kontomissbrauch durch zahlreiche Maßnahmen. Hierzu gehören Funktionen zum Warnen, Sperren, Verzögern, Bewältigen kryptografischer und verhaltensbezogener Herausforderungen, Bereitstellen alternativer Inhalte und vieles mehr. Zusätzlich können Sie je nach URL, Tageszeit, Standort, Netzwerk oder Traffic-Anteil unterschiedliche Maßnahmen festlegen.

Header-Einspeisung: Sendet Risikoinformationen für Nutzer zur Analyse und zur Abwehr in Echtzeit. Dabei wird in die weitergeleitete Anfrage ein zusätzlicher Anfrageheader eingespeist. Dieser enthält Informationen zur Risikobewertung des Nutzers sowie zu den darin eingeflossenen Risiko-, Vertrauens- und allgemeinen Indikatoren, anhand derer weitere Analysen und Echtzeit-Abwehrmaßnahmen möglich sind.

Automatisierung durch ML: Die Merkmale und Verhaltensweisen, die bei der Erkennung betrügerischer Aktivitäten von Personen und Bots zum Einsatz kommen, werden automatisch aktualisiert – angefangen von Verhaltensmustern bis hin zu aktuellen Zuverlässigkeitsdaten auf der gesamten Akamai-Plattform.

SIEM-Integration (optional): Kunden, die eine stärkere Anbindung ihrer Sicherheitssysteme wünschen, haben die Möglichkeit, Nutzerrisikodaten in ihre SIEM-Tools zu integrieren. So können Sie Ihre bestehenden Tools um die Daten aus Account Protector ergänzen und weiter aufwerten.

Weitere Informationen erhalten Sie von Ihrem Akamai-Vertriebsmitarbeiter oder unter Akamai.com.