

Bekämpfen Sie Kontoübernahmeangriffe und Betrug mit KI-gesteuerter Zugriffsortchestrierung

ForgeRock Autonomous Access: am Identity Perimeter

Inhaltsverzeichnis

Einführung	2
Geschäftliche Herausforderungen und die Auswirkungen der digitalen Transformation	2
Cyberbedrohungen mit künstlicher Intelligenz und maschinellem Lernen begegnen	2
Starke Sicherheit für ein großartiges Benutzererlebnis	3
Layered Intelligence und Anomalieerkennung	3
Mobilfreundlicher Zugang	4
Administratorfreundliche Informationen	4
Teure Integrationen	4
Wir stellen vor: ForgeRock Autonomous Access	4
Bereitstellung in der ForgeRock Identity Cloud	5
Integriert in Intelligent Access User Journeys	5
Weniger Reibungsverluste, mehr Sicherheit	5
Schützt vor bekannten Bedrohungen	6
Unterstützt intelligentere Zugriffsentscheidungen	6
Dashboards bieten Transparenz auf Makro- und Mikroebene	7
Anomalieerkennung einfach erklärt	7
Risiken definieren	8
Benutzererlebnisse in ForgeRock Intelligent Access erstellen	9
Erweiterte User Journeys dank Autonomous Access	9
Bestehende User Journeys erweitern	11
Der Autonomous Access-Vorteil	11
Layered Intelligence	11
Journeys orchestrieren – grenzenlos und ohne Code	11
Umfassende Integration in die ForgeRock-Identitätsplattform	11
Erklärbare KI	12
Fazit	12

Einführung

Die Verbraucher*innen verbringen heute weniger Zeit beim Einkauf im Geschäft und kaufen stattdessen verstärkt online ein. Zwischen 2019 und 2021 ist der E-Commerce in den USA um mehr als 50 % gewachsen.¹ Auch weltweit zeigt der Online-Handel ein dramatisches Wachstum: In Südkorea entfallen fast 26 % des Einzelhandelsumsatzes auf Online-Einkäufe, gefolgt von China mit 25 % und Großbritannien mit 23 %.² Seit dem Ausbruch der Pandemie im Jahr 2020 haben sich die Unternehmen schnell auf die Situation eingestellt und für viele ihrer Mitarbeitenden einen Remote-Zugang eingerichtet. Eine Jobbörse geht davon aus, dass 25 % aller Arbeitsplätze in Nordamerika bis Ende 2023 remote sein werden.³

Da digitales Einkaufen und Homeoffice mittlerweile zur Norm geworden sind, ist das Risiko von **Kontoübernahmeangriffen** und anderen betrügerischen Handlungen sprunghaft gestiegen. Von einer Kontoübernahme (Account Takeover – ATO) spricht man, wenn ein Angreifer (ein Mensch oder ein Bot) unbefugten Zugriff auf das digitale Identitätskonto eines Users erhält. ATO ist für globale Unternehmen eine der größten Bedrohungen und häufig die Ursache für Datenschutzverletzungen, Diebstahl und andere betrügerische Aktivitäten, die letztlich zu Umsatzverlusten, einer Beschädigung der Marke und erheblichen Kosten führen können.

Die Zunahme der Online-Aktivitäten im Rahmen von alltäglichen Transaktionen hat auch die Erwartungen der Verbraucher erhöht: Sie erwarten, dass ihre persönlichen Daten sicher sind, und wünschen sich eine problemlose Anmeldung und Registrierung sowie personalisierte Interaktionen mit den Marken und Unternehmen, die sie bevorzugen.⁴ Berufstätige wollen von jedem beliebigen Ort aus arbeiten können, und zwar über unkomplizierte und sichere Zugänge. Um Sicherheit und ein positives Benutzererlebnis zu gewährleisten, müssen Unternehmen eine moderne IAM-Lösung (Identity and Access Management) einsetzen, die unerwünschte Reibungsverluste beseitigt und gleichzeitig für mehr Sicherheit sorgt.

In diesem Whitepaper lesen Sie, wie sich IAM weiterentwickelt, um diese Herausforderungen zu meistern, und wie ForgeRock Autonomous Access, eine KI-gestützte Lösung zum Schutz vor Bedrohungen, Unternehmen hilft, Kontoübernahmeangriffe und betrügerische Aktivitäten bereits an der Identitätsgrenze zu verhindern.

Geschäftliche Herausforderungen und die Auswirkungen der digitalen Transformation

Die digitale Transformation des Verbraucher-, Bürger- und Mitarbeitererlebnisses hat zu immer mehr Cyberbedrohungen und kostenintensiven Datenschutzverletzungen geführt, die für großes Aufsehen in der Öffentlichkeit gesorgt haben. Angesichts der großen Mengen an online gespeicherten personen-, berufs- und unternehmensbezogenen Informationen ist die Möglichkeit, dass Daten gestohlen, offengelegt und für kriminelle Zwecke genutzt werden, eine Gefahr, die alle digitalen Bürger betrifft.

Viele Cyberbedrohungen beginnen mit einer Form des unbefugten Zugriffs, der durch eine kompromittierte Identität erlangt wird. ATO, die Erzeugung synthetischer Identitäten, Transaktionsbetrug und Ransomware sind nur einige Beispiele dafür, wie Kriminelle die Identität für persönliche, finanzielle und kriminelle Zwecke nutzen. Die Folgen dieser betrügerischen Aktivitäten können den Ruf Ihres Unternehmens schädigen, das Vertrauen Ihrer Kunden untergraben und die Produktivität Ihrer Mitarbeiter verringern. Sie können nicht nur zum Verlust geistigen Eigentums führen, sondern verursachen fast immer auch hohe Kosten.

- 82 % der Unternehmen hatten im Zuge der digitalen Transformation mindestens eine **Datenschutzverletzung** zu verzeichnen.⁵
- Mehr als 75 % der Unternehmen weltweit gaben an, dass Zero Trust wichtig ist, um die zunehmenden Sicherheitsbedrohungen und den Verlust von geistigem Eigentum durch unbefugten Zugriff zu bekämpfen.⁶

Cyberbedrohungen mit künstlicher Intelligenz und maschinellem Lernen begegnen

Um der sich ständig verändernden Bedrohungslandschaft zu begegnen, müssen IAM-Lösungen über bloße statische Regeln und manuelle Prozesse hinaus weiterentwickelt werden. IAM muss künstliche Intelligenz (KI) und maschinelles Lernen (ML) integrieren, um riesige Mengen von Echtzeit-Transaktionen und Big Data auf eine Art und Weise zu analysieren und Muster zu erkennen, wie

es Menschen unmöglich ist. Dank dieser erweiterten Intelligenz kann das KI/ML-fähige IAM-System das Zugriffsverhalten umfassender analysieren und effektiver vor neuen Cyber-Bedrohungen schützen.

KI/ML stimmt die Authentifizierungssensitivität darauf ab, wer sich anmeldet und ob sich dieser Anmeldeversuch oder das Online-Verhalten von früheren Ereignissen unterscheidet. Wenn sich der Kontext ändert, z. B. Standort oder Gerät des Users oder die Sensitivität der Anwendung, auf die zugegriffen wird, können weitere risikobasierte Authentifizierungsmaßnahmen oder andere Aktionen ausgelöst werden.

Ein KI/ML-gestütztes IAM-System lernt im Laufe der Zeit den Kontext verschiedener Risikosignale, um unterschiedliche Ergebnisse zu erzielen.

KI/ML-gestützte IAM erfasst mehrere Risikosignale für jeden User und jedes Authentifizierungsereignis. Solche Signale können auch Verhaltensmuster der Nutzer*innen beinhalten: Standort und Tageszeit, zu der sie sich anmelden, sowie Gerät, Browser und Betriebssystem, das sie verwenden. Basierend auf den Nutzer*innen im Unternehmen und den Anwendungen, die sie normalerweise verwenden, kann KI analysieren, ob der Zugriff einem ähnlichen Muster folgt. Zwar können wir Regeln manuell integrieren, aber im Laufe der Zeit können diese Regeln löchrig werden und schließlich nicht mehr funktionieren, wenn weitere Signale hinzugefügt werden müssen und neue Arten von Zugangsereignissen auftreten. Das Hinzufügen einer KI-Engine ist bei weitem effektiver und erfordert im Vorfeld weniger Konfigurationsaufwand beim Administrator.

Die Analyse-Engine berücksichtigt mehrere Signale, um für jedes Zugriffsereignis eine Risikobewertung zu generieren. Diese Risikowerte lassen sich in Bandbreiten gruppieren und niedrigen, mittleren und hohen Risikokategorien zuordnen. Sie können für jede Kategorie unterschiedliche Maßnahmen festlegen und die Reaktionen entsprechend den Sicherheitsrichtlinien Ihres Unternehmens anpassen.

So generieren beispielsweise eine Mitarbeiterin bzw. ein Mitarbeiter, die sich im Büro über einen vom Unternehmen gestellten Laptop anmelden, einen niedrigen Risikowert und nach erfolgreicher Authentifizierung ist der ungehinderte Zugang möglich.

Dieselbe Person, die sich manchmal in einem anderen Kontext anmeldet – von einem neuen Standort, über ein anderes Gerät, zu einer ungewöhnlichen Zeit – kann als mittleres Risiko eingestuft und aufgefordert werden, eine weitere Authentifizierungsstufe zu durchlaufen.

Manche Aktionen führen zu einer hohen Risikobewertung, beispielsweise mehrere Benutzer*innen, die sich von derselben IP-Adresse aus anmelden, ein Anmeldeversuch von zwei zu weit voneinander entfernten Standorten aus oder mehrere fehlgeschlagene Anmeldungen von derselben IP-Adresse aus. Sie können weitere Authentifizierungsstufen hinzufügen, zur Verifizierung der Identität auffordern, sie zur weiteren Überwachung an ein Honeypot-System senden oder einfach den Zugang sperren.

Starke Sicherheit für ein großartiges Benutzererlebnis

Zu den Zielen jedes IAM-Providers gehört es, für mehr Sicherheit zu sorgen und das Benutzererlebnis zu verbessern. Die Nutzer erwarten hohe Sicherheit und ein angemessenes Maß an Reibungsverlusten. Gleichzeitig wollen sie aber auch einen möglichst schnellen Anmeldeprozess. KI-gestütztes Zugriffsmanagement sollte das Beste aus beiden Welten bieten und es ermöglichen, eine beliebige Anzahl von Pfaden in einer User Journey zu definieren.

Ohne aufwendiges Customizing einer IAM-Lösung können die meisten Unternehmen keine kontextbezogenen User Journeys anhand unterschiedlicher Bedrohungssignale wie Benutzertyp, Zielanwendung und Grad der

Darüber hinaus sind sie nicht in der Lage, die richtigen Authentifizierungsoptionen für die richtigen Nutzer*innen zur richtigen Zeit bereitzustellen.

Layered Intelligence und Anomalieerkennung

Das KI/ML-gestützte IAM-System sollte nicht nur Risikobewertungen generieren können, sondern auch aus jedem Zugriffsereignis lernen, um daraus Muster abzuleiten, die dynamisch auf künftige Ereignisse angewendet werden können. So könnten Reibungsverluste beim Login für bekannte Mitarbeitende

reduziert werden, die regelmäßig von denselben Standorten aus arbeiten, während für zunehmend anomale Zugriffsmuster, die auf Bedrohungen hinweisen könnten, zusätzliche Authentifizierungsstufen eingerichtet werden. Die Kombination von künstlicher Intelligenz, maschinellem Lernen und Big Data bietet einen Echtzeitschutz gegen Bedrohungen während der Authentifizierung.

Mobilfreundlicher Zugang

Etwa die Hälfte des weltweiten Internetverkehrs ist der Nutzung von Mobilgeräten zuzurechnen.⁷ Das KI/ML-gestützte IAM-System sollte die Nutzung von Mobilgeräten erkennen, Optionen für die biometrische Authentifizierung auf dem Gerät bieten und die Nutzer auf mobilfreundliche Seiten weiterleiten. Zudem sollte es ein Software Development Kit (SDK) bereitstellen, um ein mobiles Betriebssystem, Version, Gerätemodell, Typ und jailbroken oder gerootete Geräte zu erkennen und eine eingebaute biometrische Authentifizierung häufiger Nutzer*innen zu ermöglichen. Alle diese Risikesignale sind SDK-fähige Features, die bei der Ermittlung der Risikowerte der jeweiligen Benutzer*innen genutzt werden können.

Administratorfreundliche Informationen

IAM- und Sicherheitsadministratoren sind zudem mit schlechten Benutzererlebnissen konfrontiert, wenn sie versuchen, mit neueren KI/ML-gestützten Add-ons zu ihrem bestehenden IAM zu arbeiten. Am Ende müssen sie mehrere Systeme pflegen, selbst wenn diese vom selben Anbieter stammen. Aufgesetzte Sicherheitslösungen mit Ereignisprotokollierung ohne Interpretationsfunktion erfordern einen Menschen, der die Daten liest, interpretiert und entsprechend handelt. Ohne Automatisierung und menschenlesbare Informationen bleiben die Daten häufig ungenutzt, was dazu führt, dass potenzielle Cyberrisiken nicht erkannt werden und nichts dagegen unternommen wird.

Teure Integrationen

Viele Anbieter im IAM-Markt entwickeln ihre Angebote weiter, um erweiterte Sicherheitsfeatures wie **UEBA (User and Entity Behavior Analytics)**, Heuristik, Zugriffsschutz und Betrugsprävention zu integrieren. Allerdings ist die Integration dieser Lösungen in einen vorhandenen IAM-Stack häufig mit erheblichem Zeit- und Kostenaufwand verbunden, um einen ganzheitlichen Schutz gegen Bedrohungen zu implementieren, der keine negativen Auswirkungen auf das Benutzererlebnis hat. Diese Komplexität ist darauf zurückzuführen, dass es sich bei vielen dieser Produkte entweder um eigenständige Einzellösungen handelt oder um Lösungen, die

eingekauft und ohne ausreichende Integration auf andere IAM-Produkte „aufgesetzt“ wurden.

Das Integrationsproblem wird dadurch verschärft, dass Bedrohungssignale oft aus einer Vielzahl von Quellen gesammelt werden, und zwar in der Regel von Lösungen mehrerer Anbieter. Wenn Sicherheitssysteme nicht gut mit IAM-Systemen integriert werden, bleiben die Signale entweder auf der Strecke oder Unternehmen müssen erheblichen Zeit- und Ressourcenaufwand treiben, um maßgeschneiderte Integrationen zu schaffen, um sie nutzen zu können.

Sie müssen den Bedrohungen immer einen Schritt voraus sein, ohne Ihre berechtigten Nutzer*innen zu behindern. Sie benötigen leistungsstarke Intelligenz, um exakte Zugriffsentscheidungen zu beschleunigen. Sie benötigen eine Lösung, die Administratoren größtmögliche Flexibilität an die Hand gibt, um User Journeys zu schaffen, die auf Ihre Sicherheitsstrategie abgestimmt sind. Und all dies muss Teil einer integrierten Plattform sein, die KI-gestützte Sicherheit an der Identitätsgrenze liefert.

Wir stellen vor: ForgeRock Intelligent Access

ForgeRock Autonomous Access ist eine KI-gestützte Lösung zur Erkennung von Bedrohungen, mit deren Hilfe sich Unternehmen vor Kontoübernahmeangriffen und betrügerischen Aktivitäten an der Identitätsgrenze schützen können. Sie nutzt eine einzigartige Kombination von KI, maschinellem Lernen und modernster Mustererkennung, um Bedrohungssignale und anomale Verhaltensmuster zu erkennen, und stellt Risikobewertungen bereit, damit böswillige Akteure in Echtzeit gestoppt werden können.

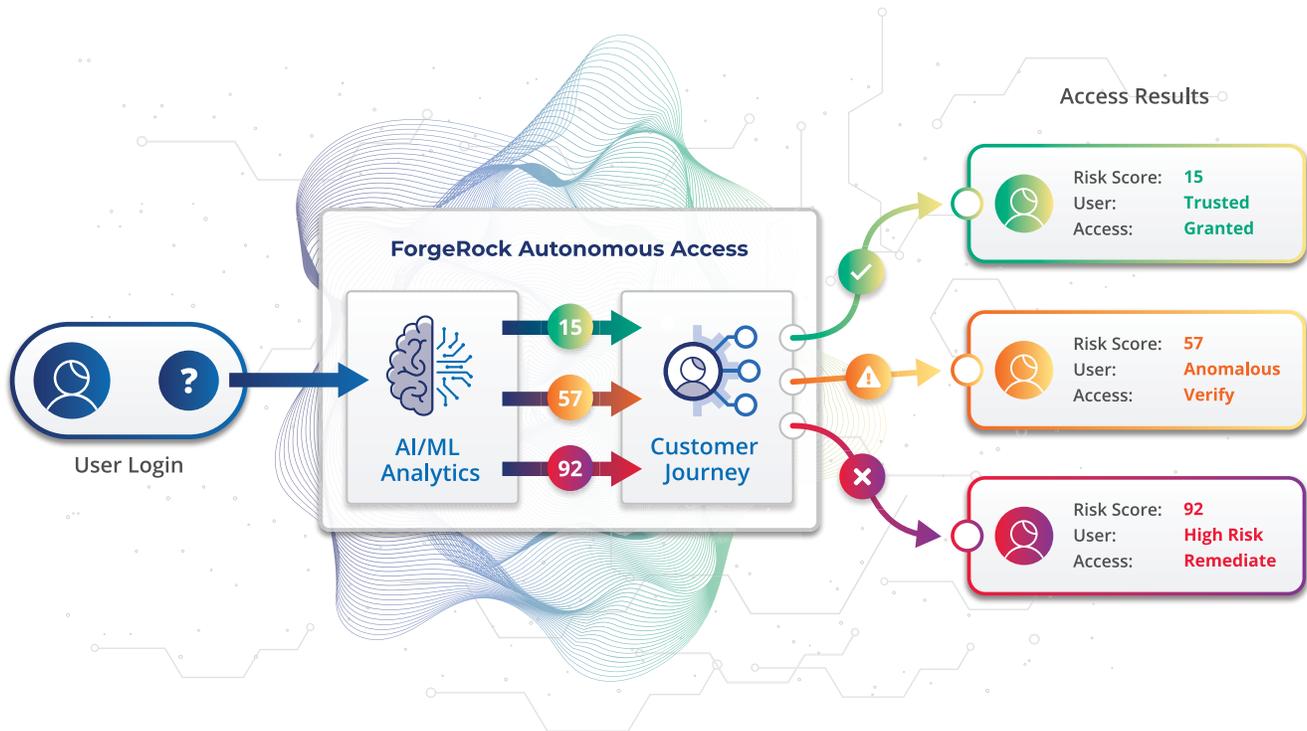


Abbildung 1. ForgeRock Autonomous Access

Bereitstellung in der ForgeRock Identity Cloud

Autonomous Access wird in Ihrem Mandanten in Ihrer privaten ForgeRock Identity Cloud implementiert, der vollständig von anderen Mandanten getrennt ist. Dieses einzigartige Datenschutz- und Sicherheitsmodell schützt Ihre Daten sowie die personenbezogenen Daten Ihrer Kunden.

Integriert in Intelligent Access User Journeys

Autonomous Access steht in Form von drei neuen Autonomous Access-Knoten⁸ zur Verfügung, die per Drag & Drop in jede beliebige neue oder bestehende User Journey innerhalb der **ForgeRock Intelligent Access**-Benutzerschnittstelle integriert werden können. Autonomous Access-Knoten erfassen und analysieren Risikosignale und generieren Risikobewertungen. Diese Risikowerte können Ihnen granularere

Zugriffsentscheidungen ermöglichen. So können Sie beispielsweise verdächtige Anmeldeversuche zusätzlich erschweren oder Nutzer*innen nach erfolgreicher Authentifizierung den ungehinderten Zugang gewähren.

Anders als herkömmliche IAM-Lösungen, die sich auf statische Regeln und manuelle Prozesse verlassen, prüft Autonomous Access kontinuierlich, lernt und passt Authentifizierungsentscheidungen an. Die Lösung nutzt Informationen aus einer Vielzahl von Quellen und ergänzt diese durch Intelligenz und Automatisierung. Sie kombiniert Heuristik zum Schutz vor bekannten Bedrohungen mit KI und maschinellem Lernen, um zwischen normalem Verhalten und neuen Bedrohungsmustern zu unterscheiden.

Weniger Reibungsverluste, mehr Sicherheit

Autonomous Access trägt dazu bei, den Kompromiss zwischen Benutzersicherheit und Benutzererfahrung zu

beseitigen. Sowohl für Ihre Mitarbeiter als auch für Ihre Kunden erkennt es zur Laufzeit kontinuierlich normale Verhaltensmuster rund um die Authentifizierung und identifiziert anomale Verhaltensweisen und Bedrohungen, die auf einen Kontoübernahmeangriff hindeuten. Autonomous Access verbessert das Benutzererlebnis, indem es Benutzer*innen mit niedrigem Risiko eine schnelle Anmeldung ermöglicht und für verdächtige Benutzer*innen oder Bedrohungen zusätzliche Hindernisse implementiert.

Schützt vor bekannten Bedrohungen

Autonomous Access nutzt einen erweiterten Musterabgleich, um alle Zugriffsereignisse vor bekannten Bedrohungen zu schützen, wie:

- **Credential Stuffing:** erkennt die automatische Eingabe von gestohlenen Benutzernamen- und Passwort-Kombinationen in Website-Formulare, um unbefugten Zugang zu erhalten.⁹
- **Verdächtige IP-Adressen:** prüft, ob dieselbe IP-Adresse von mehreren Benutzer*innen genutzt wird.
- **Impossible Travel:** erkennt, wenn ein Anmeldeformular auf einen unmöglichen Weg zwischen der aktuellen und der letzten Anmeldung eines Users hindeutet oder die Entfernung zwischen einem Gerät, von dem sich der User anmeldet, und seinem registrierten MFA-Gerät zu groß ist (Beispiel: Anmeldung an einem Laptop in Argentinien und SMS-Antwort von einem Gerät in Australien).
- **Brute-Force-Angriff:** erkennt wiederholte fehlgeschlagene Anmeldeversuche.
- **Automatische Benutzeragenten:** erkennt Bots.

Unterstützt intelligentere Zugriffsentscheidungen

Autonomous Access nutzt KI/ML, um die Echtzeit-Authentifizierung auf Basis des Nutzerverhaltens kontinuierlich zu prüfen, zu lernen und anzupassen. Es erkennt Kontoübernahmeangriffe und betrügerische Aktivitäten bei der Authentifizierung und stoppt sie dort, ehe ein Konto infiltriert werden kann. Es nutzt drei unterschiedliche KI-Modelle, die automatisch ausgewählt werden, je nachdem, ob es sich um häufige, gelegentliche oder Erst-User handelt.

UEBA-Signale (User and Entity Behavioral Analytics): Dieses KI-Modell erkennt Anomalien häufiger Nutzer*innen anhand von Stadt, Land, Wochentag, Tageszeit, Betriebssystem, Betriebssystemversion,

Gerätemodell, Gerätetyp und für die Anmeldung benutzten Browser.

Benutzergruppen: Dieses KI-Modell erkennt Anomalien durch Vergleich des Anmeldeverhaltens gelegentlicher User mit dem Verhalten anderer Mitglieder der Gruppe, zu der sie gehören. Diese Technik wird genutzt, wenn es nicht genügend Informationen zum normalen Verhalten dieses Users gibt. So vergleicht das Modell beispielsweise das Anmeldeverhalten eines Users aus der Finanzgruppe mit dem Anmeldeverhalten anderer Mitglieder der Finanzgruppe, um zu sehen, ob eine Anomalie vorliegt.

Alle User: Dieses KI-Modell wird bei Erst-Usern angewendet, für die es keine Historie zum Vergleichen gibt. In diesem Fall können wir das Verhalten dieses Users mit dem Verhalten aller anderen bekannten User vergleichen, um zu sehen, ob eine Anomalie vorliegt.

Erklärbar: Autonomous Access meldet den Grund für die Anomalie oder Bedrohung auf der Grundlage der erkannten Daten.

Dashboards bieten Transparenz auf Makro- und Mikroebene

Über die in Intelligent Access Trees verfügbaren Knoten hinaus stellt Autonomous Access ein Access Dashboard bereit, mit dem Sie anomale und riskante Zugriffsversuche untersuchen und den Kontext von Bedrohungen ermitteln können. Das Dashboard bietet neben einem Überblick über die Bedrohungen auch spezielle Ansichten für Betrugsanalysten und Systemadministratoren.

Das Dashboard in Abbildung 2 zeigt geografische Standorte, an denen Zugriffe mit hohem Risiko festgestellt wurden.



Abbildung 2. Globale Ansicht von Zugriffen mit hohem Risiko

Anomalieerkennung einfach erklärt

Wird eine Bedrohung erkannt, ist es wichtig zu verstehen, warum ein Verhalten risikobehaftet war, und die Ursache dafür schneller zu ermitteln – ohne dass es notwendig ist, Regeln zu konfigurieren und zu bearbeiten. Das Autonomous Access Dashboard erläutert diese Informationen in menschenlesbarer Form.

Jedes Ereignis im Dashboard kann ausgewählt werden, um eine detaillierte Darstellung von Zugriffsereignissen nach User und Risikobewertung zu erhalten, und zwar zusammen mit einer Erklärung des risikobehafteten Authentifizierungsversuchs. Abbildung 3 zeigt, dass ein User in Singapur in der Vergangenheit versucht hat Anmeldeinformationen zu stehlen (Credential Stuffing), was den Risikowert dieses Users auf 100, die höchste Stufe, setzt.

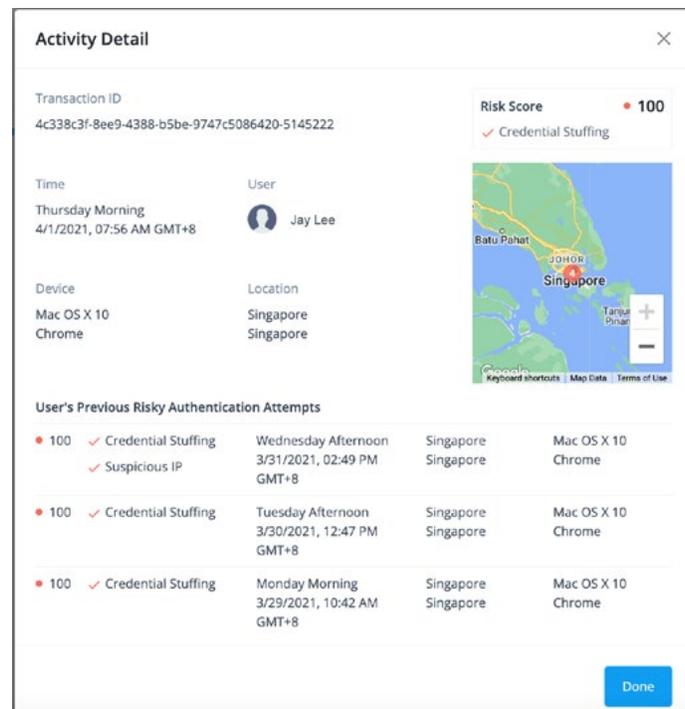


Abbildung 3. Aktivitätsdetails risikobehafteter Authentifizierungsversuche

Darüber hinaus können Sie sich auch Zugriffsversuche für einen bestimmten Zeitraum anzeigen lassen: heute, diese Woche, dieser Monat, ein vom User definierter Zeitraum (s. Abbildung 4).

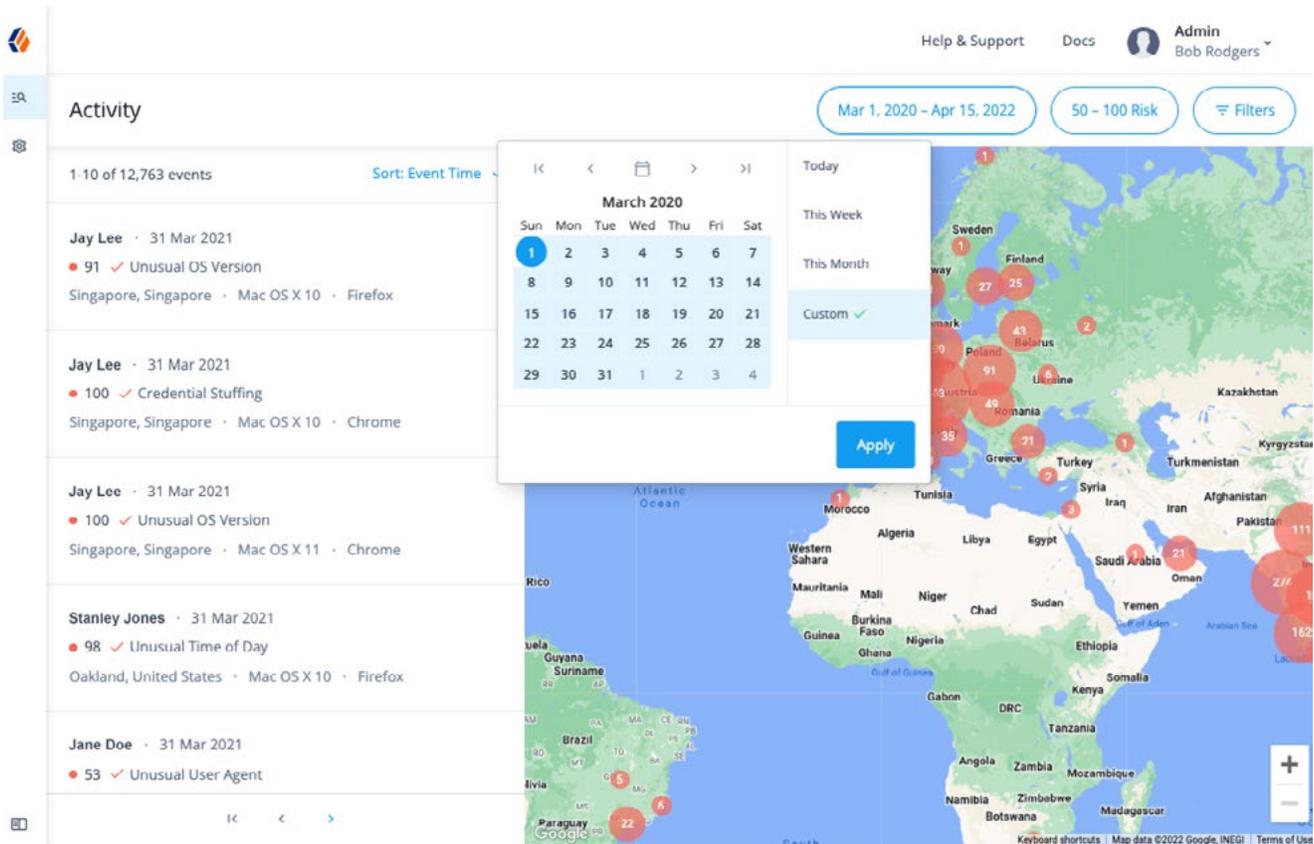


Abbildung 4. Weltweite Zugriffsaktivitäten in einem bestimmten Zeitraum

Risiken definieren

Mit ForgeRock Autonomous Access können Sie User Journeys gestalten, die Authentifizierungen mit hohen, mittleren und niedrigen Risiken unterschiedlich behandeln.



Vertrauenswürdig:

Ein User mit niedrigem Risiko meldet sich zur selben Zeit, am selben Ort und über dasselbe Gerät an.



Anomales Verhalten:

Ein vertrauter Benutzer, der möglicherweise ein neues Gerät verwendet oder sich zu einer ungewöhnlichen Zeit oder an einem ungewöhnlichen Ort anmeldet. Der User muss einen zusätzlichen Identitätsnachweis erbringen.



Bekannte Bedrohung

Ein höchstwahrscheinlich böswilliger Hochrisiko-User, möglicherweise ein Bot, mit mehreren fehlgeschlagenen automatischen Anmeldeversuchen. Anmeldeanforderungen können abgefangen oder gänzlich blockiert werden.

Benutzererlebnisse in ForgeRock Intelligent Access erstellen

Ehe Autonomous Access eingesetzt wird, muss man unbedingt verstehen, wie User Journeys (Bäume) in Intelligent Access erstellt werden. Wenn Sie mit Intelligent Access nicht vertraut sind, lesen Sie das Whitepaper [Wir stellen vor: ForgeRock Intelligent Access](#).

Zu den Grundbausteinen einer Authentifizierungs-Journey gehören:

- Ein **Knoten für die Zugangsdatenerfassung** – z. B. für Benutzernamen und Passwort, biometrische Daten oder Hardware-Token. Verwenden Sie einen Seitenknoten, um mehrere Knoten für die Zugangsdatenerfassung zu kombinieren, damit der User alle Elemente auf einer einzigen Seite sieht.
- Ein **Entscheidungsknoten** zur Überprüfung der Gültigkeit eines Authentifizierungsversuchs. So kann beispielsweise ein Data-Store-Entscheidungsknoten Benutzernamen und Passwort gegen ein Verzeichnis prüfen und „true“ (wahr) bzw. „false“ (falsch) zurückliefern, je nachdem, ob sich der User erfolgreich mit seinen bzw. ihren Anmeldedaten in einem Verzeichnisdienst authentifiziert hat.
- Ein **Ergebnis**, das als Erfolg/Fehler (Success/Failure), richtig/falsch (True/False) definiert ist, oder willkürlichere und dynamischere Ergebnisse.

Abbildung 5 zeigt eine einfache Authentifizierungsbaumstruktur mit Knoten zur Erfassung des Benutzernamens und des Passworts. Durch den Data-Store-Entscheidungsknoten mit True- und False-Ergebnissen erhält der User Zugriff, wenn er/sie sich erfolgreich beim ersten Datenspeicher authentifiziert, oder er/sie wird auf die Benutzernamen/Passwort-Seite zurückgeleitet, wenn die Authentifizierung fehlschlägt.

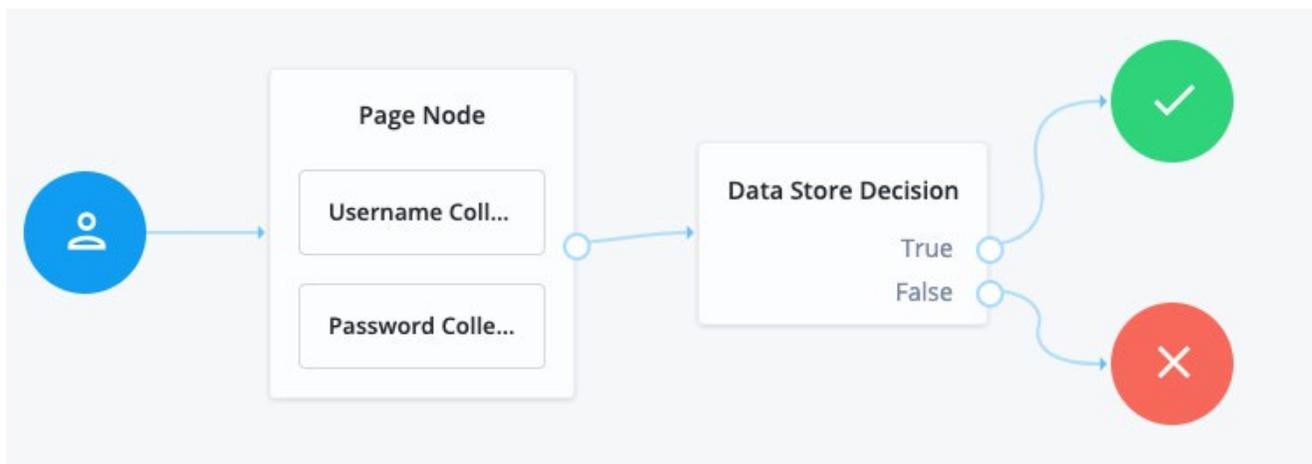


Abbildung 5. Einfacher Authentifizierungsbaum für Benutzername und Passwort

Erweiterte User Journeys dank Autonomous Access

Es gibt drei neue Knoten für Autonomous Access, die Sie direkt per Drag & Drop in Ihre User Journeys integrieren können:

- **Autonomous Access Signal-Knoten** – erstellt eine Risikobewertung auf Grundlage spezifizierter Faktoren und ermöglicht Ihnen Authentifizierungsentscheidungen auf Basis dieser Bewertung.
- **Autonomous Access Decision-Knoten** – ermöglicht es Ihnen, eine Reihe von Entscheidungen für hohe, mittlere und niedrige Risikowerte zu definieren.
- **Autonomous Access Result-Knoten** – stellt die endgültigen Rückmeldungen der Ergebnis- und Risikovorhersage für Access Analytics bereit

Abbildung 6 zeigt, wie sich ein einfacher Benutzernamen- und Passwortbaum mit Autonomous Access-Knoten erweitern lässt, um einen risikobasierten Authentifizierungsprozess einzurichten. Autonomous Access-Knoten bieten zusätzliche Informationen zur Risikostufe für jede Authentifizierung. Ziehen Sie einfach per Drag & Drop die Autonomous Access-Knoten in die User-Journey-Palette nach dem Data-Store-Entscheidungsknoten. Wählen Sie den Autonomous Access Signal-Knoten aus, um die Risikofaktoren anzuzeigen und auszuwählen, die Sie erkennen möchten, indem Sie die im rechten Bereich angezeigten Kontrollkästchen verwenden.

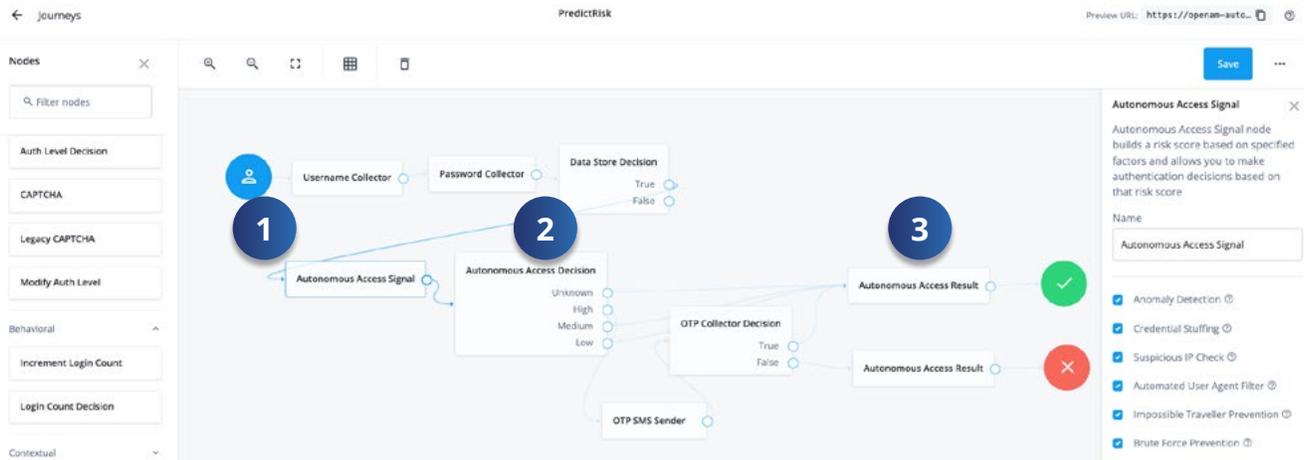


Abbildung 6. Einfacher Authentifizierungsbaum mit Autonomous Access-Risikovorhersage

1. Der erste Knoten auf der linken Seite ist der **Autonomous Access Signal**-Knoten, der eine Risikobewertung auf Basis der Faktoren erstellt, die Sie im rechten Bereich auswählen.

Die Risikowerte liegen zwischen 0 und 100. Sie können entweder jeweils die Standardwerte wählen oder Ihre eigenen Konfiguration erstellen. Beispiel:

- 0-19 Niedriges Risiko, vertrauenswürdiger User
- 20-79 Mittleres Risiko, anomales Verhalten
- 80-100 Hohes Risiko, bekannte oder unbekannte Bedrohung

2. Der zweite Knoten von links ist der **Autonomous Access Decision**-Knoten. Dieser Knoten ermöglicht es Ihnen festzulegen, wie Sie Authentifizierungen behandeln wollen, die den Gruppen „Unbekannt“, „Hoch“, „Mittel“ und „Niedrig“ zugeordnet sind. Auf Basis der Risikobewertung können Sie beliebige Aktionen durchführen:
 - Im Beispiel aus Abbildung 6 muss der User bei Hochrisiko-Authentifizierungen ein Einmalpasswort (OTP) eingeben, das ihm oder ihr per SMS zugeschickt wird. Hinweis: Alternativ zur SMS können Sie eine beliebige Anzahl von Methoden für die verstärkte Authentifizierung aus der Intelligent Access-Oberfläche auswählen.
 - Der OTP Collector Decision-Knoten lässt den Zugriff zu, wenn die richtige OPT eingegeben wird.
 - Authentifizierungen mit mittlerem oder niedrigem Risikowert erhalten unmittelbaren Zugang und werden nicht zu einer verstärkten Authentifizierung aufgefordert.
3. Der **Autonomous Access Result**-Knoten meldet das Ergebnis der User Journey an die Autonomous Access-Analyseengine zurück und trägt so dazu bei, ein Benutzerprofil und im Laufe der Zeit die Zugriffsmuster dieses Users zu erstellen. Stellen Sie sicher, dass Sie Autonomous Access Result-Knoten für erfolgreiche **und** fehlgeschlagene Authentifizierungen definieren.

Bestehende User Journeys erweitern

Autonomous Access kann Ihre User Journeys effizienter gestalten, ohne dass Sie dazu die User Journey neu erfinden müssen, die Sie bereits konfiguriert haben. Sobald Sie die Autonomous Access-Journey(s) entworfen haben, die Sie nutzen wollen, können Sie diese einfach über den Inner Tree Evaluator-Knoten zu Ihren vorhandenen User Journeys hinzufügen. Es gibt keine Einschränkungen hinsichtlich der Tiefe verschachtelter Bäume.

Der **Inner Tree Evaluator-Knoten** (siehe Abbildung 7) ermöglicht die Verschachtelung und Auswertung von Authentifizierungsbäumen als Kinder innerhalb eines übergeordneten Baums. Abbildung 7 zeigt, wie ein Autonomous Access-Baum in einen bestehenden Authentifizierungsbaum eingefügt wird. Dazu wird der Inner Tree Evaluator-Knoten und im rechten Bereich die gewünschte Autonomous Access-Baumvorlage in der Dropdown-Liste ausgewählt.



Abbildung 7. Nutzung des Inner Tree Evaluators für Autonomous Access

Der Autonomous Access-Vorteil

Der IAM-Markt entwickelt sich weiter, um die Herausforderungen bewältigen zu können, die die ständigen Bedrohungen sowie die vielfältigen Möglichkeiten von Kontoübernahmen und betrügerischen Aktivitäten mit sich bringen. KI/ML und UEBA (User & Entity Behavioral Analytics) stehen bei den IAM-Anbietern ganz oben auf der Liste. ForgeRock Autonomous Access ist die am besten integrierte IAM-Lösung zur Abwehr von Bedrohungen, die heute am Markt verfügbar ist. Dies sind einige der Vorteile:

Layered Intelligence

ForgeRock Autonomous Access kombiniert einen erweiterten Musterabgleich mit KI/ML-Algorithmen in einer Big-Data-Engine. Layered Intelligence identifiziert bekannte Angreifermuster (Menschen und Bots), kennzeichnet anomale Verhaltensmuster für die weitere Analyse und lernt neue Bedrohungsmuster.

Journeys orchestrieren – grenzenlos und ohne Code

Dank der Integration mit ForgeRock Intelligent Access-Bäumen können Sie No-Code User Journeys für viele Anwendungsfälle orchestrieren und maßgeschneiderte Login-Erlebnisse auf Basis der jeweilige Risikostufe erstellen. Ziehen Sie einfach Autonomous Access-Knoten per Drag & Drop in eine beliebige Access Journey und verschachteln Sie Autonomous Access-Journeys mit Ihren bestehenden User Journeys, um zusätzliche Einblicke zu erhalten. Zudem können Sie mit Autonomous Access auch einige Ihrer komplexeren User Journeys vereinfachen.

Umfassende Integration in die ForgeRock-Identitätsplattform

Viele KI/ML-gestützte IAM-Angebote erfordern zeit- und kostenaufwendige kundenspezifische Integrationen, um das gewünschte Geschäftsergebnis zu erzielen. Dies ist darauf zurückzuführen, dass es sich bei den meisten dieser Produkte entweder um eigenständige Einzellösungen oder um Lösungen handelt, die eingekauft und ohne ausreichende Integration auf andere Produkte „aufgesetzt“ wurden. ForgeRock Autonomous Access ist eine SaaS-Lösung ohne kostspielige, langwierige Integrationen. Aktivieren Sie einfach Autonomous Access in ForgeRock Identity Cloud und nutzen Sie Autonomous Access-Knoten in ForgeRock Intelligent Access.

Erklärbare KI

KI/ML sollte mehr können, als nur eine Risikobewertung zu liefern. Sie sollte auch eine erklärbare, nachvollziehbare Begründung für Administrator und Endbenutzer*in liefern. Autonomous Access unterstützt die Weitergabe menschenlesbarer Informationen an den bzw. die Endbenutzer*in in der Benutzeroberfläche.

Fazit

ForgeRock Autonomous Access ist eine leistungsstarke Lösung zur Abwehr von Bedrohungen, die es Ihnen ermöglicht, auf Basis mehrerer Signale und Analysen intelligentere Zugangsentscheidungen zu treffen. Autonomous Access hilft Ihnen, zwischen bekannten Usern, Usern mit anomalem Verhalten oder bekannten Bedrohungen zu unterscheiden. Darüber hinaus können Sie die Anmeldung entsprechend vereinfachen oder erschweren.

Das Ergebnis ist eine stärkere Sicherheitslandschaft, die identitätsbezogene Datenschutzverletzungen und Betrug verhindert und dabei den personalisierten und reibungslosen Zugriff für Ihre legitimen User ermöglicht.

¹ <https://www.digitalcommerce360.com/article/us-ecommerce-sales/>

² <https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales>

³ <https://www.theladders.com/press/25-of-all-professional-jobs-in-north-america-will-be-remote-by-end-of-next-year>

⁴ <https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying>

⁵ Ponemon Report: Digital Transformation 2020

⁶ Forrester-Studie im Auftrag von Illumio. <https://www.illumio.com/news/press-releases/forrester-trusting-zero-trust>

⁷ <https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices>

⁸ Intelligent Access-Knoten sind kleine Arbeitseinheiten, aus denen sich eine User Journey zusammensetzt. Jeder Knoten erfüllt einen bestimmten Zweck: Er legt bestimmte Aktionen fest, die während einer User Journey ausgeführt werden. ForgeRock Intelligent Access verfügt über zahlreiche vorprogrammierte Knoten, die digitale Signale erkennen, Entscheidungen treffen und die User Journey steuern. Mit einer Kombination aus mehreren Knoten können Sie Signale erfassen, die Sie in Intelligent Access konfigurieren, und so festlegen, ob die Zugriffsebenen eines Benutzers während einer Sitzung verändert werden sollten. Diese Signale werden in einem Sitzungstoken gespeichert, das Informationen über die Benutzersitzung für nachgelagerte Anwendungen bereitstellt. Wenn Sie mit den Konzepten von Knoten und Bäumen in Intelligent Access nicht vertraut sind, lesen Sie bitte das Whitepaper „Wir stellen vor: ForgeRock Intelligent Access“ (<https://www.forgerock.com/resources/whitepaper/eine-einfuehrung-forgerock-intelligent-access>).

⁹ https://owasp.org/www-community/attacks/Credential_stuffing

Über ForgeRock

ForgeRock® (NYSE: FORG) ist ein weltweit führender Anbieter im Bereich digitale Identität, der einen einfachen und sicheren Zugang zur vernetzten Welt ermöglicht. Die ForgeRock Identity Platform bietet skalierbare Identitätslösungen der Enterprise-Klasse für Kunden, Beschäftigte und vernetzte Geräte. Mehr als 1.300 Unternehmen vertrauen auf die umfassende Plattform von ForgeRock, wenn es um die Verwaltung und Sicherung von Identitäten mittels Identitätsorchestrierung, dynamischer Zugriffskontrolle, Governance und APIs in sämtlichen Cloud- oder Hybridumgebungen geht. Weitere Informationen finden Sie unter: www.forgerock.com.

Folgen Sie uns

