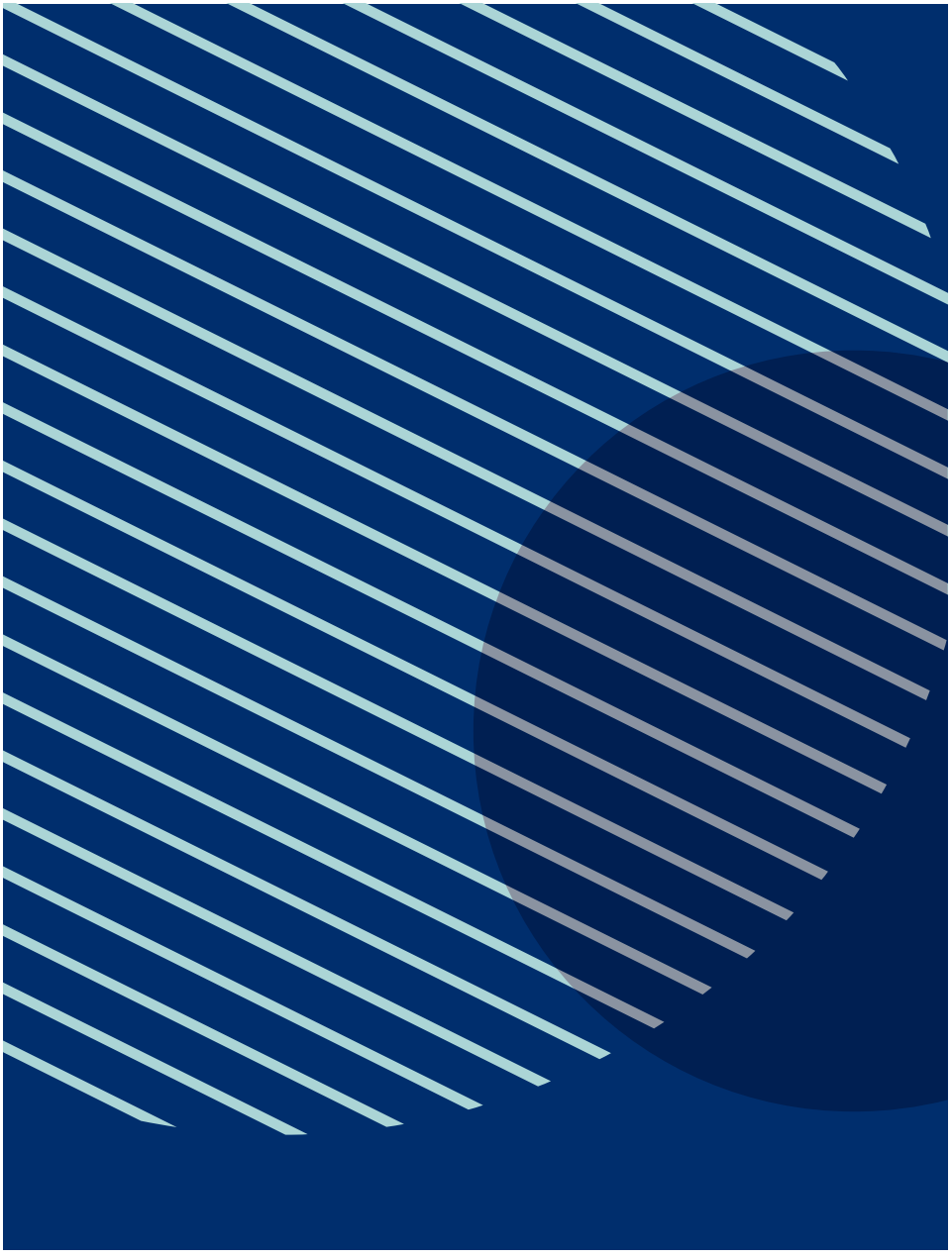
Whitepaper

Juni 2022

Einkaufs-führer Identity & Access Management

Wie Sie die richtige Lösung für Ihre Kunden und Ihre Workforce finden.

Okta Inc.
Oskar-von-Miller-Ring 20
80333 München, Germany
info_germany@okta.com
+49 (89) 26203329



okta

Inhalt

Identity- & Access-Management ist kein ganz neues Thema – aber es gewinnt stetig an Bedeutung. Aber woher kommt das plötzliche Interesse über alle Business Units und Hierarchie-Ebenen hinweg? Warum kommt dem Identity- & Access-Management heute eine Schlüsselrolle zu, und was kann im schlimmsten Fall geschehen, wenn das Projekt schiefgeht? Welche Faktoren gilt es bei der Auswahl einer Lösung im Blick zu behalten?

Dieser Guide soll Ihnen dabei helfen, diese und viele weitere Fragen zu beantworten. Sie erfahren darin alles über die Driver, die den IAM-Markt heute prägen, und die Faktoren, die Sie bei der Auswahl Ihrer neuen Lösung berücksichtigen sollten. Denn am Ende des Tages hängt es maßgeblich von den Markttreibern und den Risikofaktoren ab, wie Ihre neue IAM-Lösung aussehen muss. Sie müssen sorgfältig abwägen, welche Funktionalitäten Ihre Lösung unterstützen soll und wie sich diese auf Ihren Bereich und andere wichtige Stakeholder in Ihrem Unternehmen auswirken. Denn letzten Endes existieren IAM-Lösungen nie in einem Vakuum. Es handelt sich um eine kostspielige, langfristige Investition, die auf alle Bereiche Ihres Unternehmens ausstrahlt – vom Vorstand und C-Level bis hin zum letzten Vollzeitmitarbeiter in jeder Abteilung und jedem Geschäftsbereich Ihres Unternehmens – und in vielen Fällen auch auf Ihre Kunden und andere wichtige Partner außerhalb Ihres Unternehmens.

Warum es diesen Guide gibt?

Es steht viel auf dem Spiel

Das Identity & Access Management gewinnt in Unternehmen über alle Branchen und Regionen hinweg an Bedeutung. Welche Markttreiber führen dazu, dass IAM immer wichtiger wird?

Die Einführung hybrider Arbeitsmodelle erfordert starkes IAM

Die Digitalisierung der Arbeitswelt schreitet rasant voran. Und mit COVID hat die digitale Transformation weltweit noch weiter an Fahrt aufgenommen.

> “
> COVID breitet sich nach wie vor aus – und in einigen Ländern, die versucht haben, wieder zum normalen Arbeitsalltag zurückzukehren, steigen die Zahlen bereits wieder. Wir gehen deshalb davon aus, dass sich in Zukunft andere Workforce-Modelle durchsetzen werden, als wir angenommen haben.
>
> EJ Widun, Chief Technology Officer,
> Oakland County Michigan

Unser Wunsch nach Schnelligkeit und Agilität, unser Bedürfnis nach On-Demand-Diensten und der Flexibilität, jederzeit bedarfsgerecht zu skalieren, und schließlich unser starker Drang nach ständiger Innovation machen den Wechsel in die Cloud zur echten Notwendigkeit. Immer mehr Unternehmen stellen sich dieser Herausforderung: Sie entwickeln und betreiben neue Dienste in der Cloud – und entscheiden sich dabei immer öfter für Best-of-Breed-Lösungen. Damit sind sie beim Betrieb ihrer Lösungen auf eine Vielzahl von Cloud-Infrastruktur-Anbietern, SaaS-Anwendungen, Entwicklungs- und Management-Tools, Analysediensten und Security-Plattformen angewiesen. Und was ist der Klebstoff, der all diese heterogenen Lösungen zusammenhält? Starke Identities. Mit zeitgemäßen IAM-Lösungen können Unternehmen all ihren Benutzern einen einfachen und sicheren Zugriff auf Anwendungen, Geräte und Technologien ermöglichen. Bestehende IAM-Lösungen, die für die alte On-Premises-Welt entwickelt wurden, reichen heute einfach nicht mehr; sie sind in der Regel isoliert und schwer zu warten, und oft ist es nicht möglich, diese Identity-Plattformen ohne Abstriche und Kompromisse nachzurüsten.

Bestehende Lösungen reichen nicht

	Bestehende Identity-Lösungen On-Premises	Moderne Cloud-basierte Identity-Lösungen
Integration mit Cloud-Technologien		X
Anbindung persönlicher Devices		X
Management von Usern außerhalb des Unternehmens		X
Hochwertige Experience für Endanwender		X

Moderne Security erfordert ein starkes IAM

Unsere Welt hat sich in den letzten Jahren rasant und dynamisch verändert – hin zu dezentralen und hybriden Arbeitsumgebungen. Sie ist exponentiell digitaler geworden, und so wurde der traditionelle Netzwerk-Perimeter über Nacht zu einem veralteten Sicherheitsmodell. Der neue Perimeter ist die Identity. Es überrascht nicht, dass die Zahl der identitätsbasierten Bedrohungen und Angriffe drastisch gestiegen ist.

Ein Verizon Data Breach Report stellt fest, dass 89 % aller webbasierten Angriffe auf den Missbrauch von Zugangsdaten zurückgehen.

Angesichts der zunehmenden Zahl von Security-Breaches benötigen Unternehmen mehr Systeme, Protokolle und Standards zum Schutz ihrer Daten. In der Folge haben sich nicht nur die Datenschutz-, Security- und Compliance-Vorgaben verschärft. Auch der Zeit-, Ressourcen- und Kostenaufwand für die Einhaltung dieser Standards – und die Einführung eines Zero-Trust-Modells – ist damit gestiegen. Kurz: Mit der Beschleunigung der digitalen Roadmap sind auch die Risiken und die damit verbundenen Kosten gestiegen, und es wird immer wichtiger, „es gleich beim ersten Mal richtig zu machen“.

Unternehmen mit sehr ausgeprägtem Omnichannel-Kundenkontakt können im Schnitt 89 % ihrer Kunden langfristig binden. Bei Unternehmen mit schwachem Omnichannel-Ansatz sind es gerade einmal 33 %

Aberdeen Group

Steigende Kundenanforderungen machen IAM notwendig

Und als ob das noch nicht genug wäre: Während Unternehmen vor der Herausforderung stehen, ihre digitalen Systeme auszubauen und immer mehr komplexe, Identity-basierte Angriffe abzuwehren, erwarten die Verbraucher (sowohl interne Mitarbeiter als auch externe Kunden) jederzeit eine hochwertige Experience. In den letzten zwei Jahren mussten Unternehmen ganz neu darüber nachdenken, was es bedeutet, ihre Mitarbeiter und Kunden anzubinden. Die Konversionsrate mobiler Anwendungen zu maximieren oder 1:1-Beziehungen mit Käufern, Patienten oder Kunden zu etablieren, ist ein wichtiger erster Schritt, um den Umsatz zu steigern und Kunden dauerhaft zu binden. Dabei ist es von entscheidender Bedeutung, ein starkes Security-Fundament zu legen, das Vertrauen schafft – eine entscheidende Komponente beim Aufbau von Markentreue. Unternehmen bewegen sich dabei auf einem schmalen Grat zwischen robuster Security und hochwertiger User-Experience. Und sie müssen schon im ersten Anlauf alles richtig machen, da der Wettbewerb stets nur einen Klick entfernt ist.

An wen richtet sich dieser Guide? Und warum?

Eine Entscheidung mit hoher Tragweite

Ganz egal, ob Sie sich für Build oder für Buy entscheiden, eines ist sicher: Die IAM-Lösung wird die Beziehung Ihres Unternehmens zu seinen Kunden nachhaltig und umfassend prägen. Daher ist es von zentraler Bedeutung, alle wichtigen Stakeholder zu identifizieren und für den Evaluierungs-, Kauf- und Implementierungsprozess ein bereichsübergreifendes Team mit klar definierten Zuständigkeiten zu bilden. Wenn Sie alle Stakeholder frühzeitig einbeziehen, erhöhen Sie Ihre Chancen, die beste langfristige strategische Investitionsentscheidung für Ihr Unternehmen zu treffen.

> “
> Wenn Sie nicht die Unterstützung aller Entscheidungsträger haben – bis hinauf zum CIO und CISO – können Sie gleich wieder einpacken.
>
> Trey Ray, Manager,
> Cybersecurity, FedEx

Unabhängig davon, wer für das Projekt verantwortlich zeichnet, ist es wichtig, die verschiedenen Stakeholder und ihre jeweiligen Ziele zu kennen – die internen und die externen.

Um Ihnen einen ersten Eindruck von dem Team zu vermitteln, das Sie zusammenstellen sollten, finden Sie im Folgenden eine Liste der Abteilungen, die typischerweise vor Business-Challenges stehen, bei denen ein strategischer Identity-Partner helfen kann. Denken Sie aber daran, dass die Zusammenstellung eines solchen bereichsübergreifenden Teams von Unternehmen zu Unternehmen variiert. Seien Sie im Zweifelsfall lieber zu inklusiv, und binden Sie Stakeholder aus allen Bereichen ein, die für Ihr Unternehmen sinnvoll sind.

Security z.B.: CSO, CISO	• Minimieren Sie die Gefahr eines Security-Incidents • Stellen Sie die Weichen für eine schnelle Erkennung und kurze Reaktionszeiten • Minimieren Sie die Folgen eines Security-Incidents	Vollständige Integration aller Anwendungen, Domänen und Geräte und Konsolidierung des Security-Managements und des Security-Monitorings an einem Punkt.
Informations- und Business-Technologie z.B.: CIO	• Senken Sie die IT-Ausgaben und ermöglichen Sie einen effizienten Betrieb • Machen Sie Ihre IT-Infrastruktur performanter und zuverlässiger • Steigern Sie die Produktivität, Zufriedenheit und Loyalität Ihrer Mitarbeiter • Stellen Sie die Weichen für Innovation und Digitalisierung • Beschleunigen Sie M&A-, Joint-Venture- und Carve-Out-Projekte	Automatisierung administrativer Prozesse, Beschleunigung der Services für Mitarbeiter und letztendlich Kostensenkung. Ihre IAM-Lösung sollte den Lifecycle Ihrer Anwendungen und Benutzer optimieren, um einen raschen Rollout von Anwendungen zu gewährleisten.
Marketing & Digital z.B.: CDO, VP Marketing	• Verkürzen Sie die Time-to-Market • Gewinnen und binden Sie Kunden • Verbessern Sie die Zusammenarbeit mit Business-Partnern • Verbessern Sie die Customer-Experience	Ihre IAM-Lösung sollte flexible Anmeldeoptionen wie Social Login unterstützen und leistungsfähige Identity-Features wie Progessive Profiling und biometrische Authentifizierung bieten, um eine reibungslose Customer-Journey zu ermöglichen.
Infrastruktur und Betrieb e.g. VP I&O	• Abkehr von der On-Prem-Architektur ermöglicht Einsparungen und einfacheres Management • Garantiert durchgängige Verfügbarkeit, Resilienz und Performance (keine planmäßigen Downtimes)	Eine Cloud-First-Architektur, die sich problemlos mit vorhandenen lokalen Komponenten integrieren lässt, um hochgradig resiliente und hochverfügbare Services mit einer SLA von mindestens 99,99 % bereitzustellen.
Produkt & Entwicklung z.B.: CPO, CTO, Leiter Entwicklung	• Weichenstellung für einen effizienteren Betrieb, damit sich die Entwicklungsteams auf das Kerngeschäft konzentrieren können • Kürzere Entwicklungs- und Release-Zyklen für ihre Kunden	Bereitstellung einer leistungsfähigen, auf die Anforderungen der Entwickler ausgerichteten Identity- und Autorisierungs-Plattform für Ihre Entwickler

Suchen Sie nicht ein einfaches Tool, suchen Sie eine strategische Lösung

So geht es richtig

Die richtige IAM-Lösung zu finden, ist nicht leicht – zumal, wenn man bedenkt, wie viel auf dem Spiel steht und welche weitreichenden Auswirkungen diese Entscheidung für Ihr Unternehmen hat. Aber wenn Sie sich konsequent auf eine überschaubare Zahl von Schlüsselfaktoren konzentrieren, können Sie Ihre Optionen eingrenzen und eine Lösung wählen, die dauerhaft zu Ihnen passt.

> “
>
> Identity ist kritisch, Security ist kritisch. Sicherzustellen, dass nur die richtigen Anwender Zugang zu den richtigen Daten erhalten, ist kritisch.
>
> Harry Moseley, CIO,
> Zoom

Natürlich gibt es eine ganze Reihe von „Nice-to-have“-Funktionen. Doch Sie sollten sich auf das konzentrieren, was wirklich wichtig ist. Im Folgenden analysieren wir vier Schlüsselfaktoren, die Vorteile, die sie bieten, und einige Fragen, mit denen Sie herausfinden können, wie wichtig diese Attribute für Ihr Unternehmen sind.

Faktor #1: Neutral und herstellerunabhängig

Ihre IAM-Lösung muss herstellerunabhängig sein, um Ihrem Business die nötige Flexibilität zu bieten. So können Sie Ihre Softwarelösungen stets gemäß Ihrer konkreten Anforderungen wählen – und nicht aufgrund des Identity-Providers.

Wenn Ihr Unternehmen bereits in die Cloud migriert ist, betreiben viele Abteilungen eigene Technologie-Stacks, die eine Reihe von Best-of-Breed-Lösungen umfassen. Diese Tech-Stacks sind wahrscheinlich schon kompliziert genug, ohne dass Sie sich wegen der fehlenden Flexibilität Ihres Identity-Providers weiter einschränken müssten. Identity ist die eine Komponente, die Ihre Lösungen und Stacks über alle Abteilungen Ihres Unternehmens zusammenführt. Wenn Sie die Agilität Ihres Unternehmens auf Dauer sicherstellen wollen, muss diese herstellerneutral sein. Wenn Ihre Identity-Plattform für sich in Anspruch nimmt, ein One-Stop-Shop zu sein, ist es um ihre Neutralität wahrscheinlich nicht gut bestellt.

Stellen Sie bei der Evaluierung einer IAM-Lösung sicher, dass diese folgenden Anforderungen gerecht wird:	Ihre Vorteile im Überblick:
• Breites und tiefes Set schlüsselfertiger Konfigurationen • Integrationen, die den neuesten und gängigsten offenen Standards entsprechen • Risiko-basiertes Ökosystem mit enger Integration von Network Security-, Endpoint Detection- und Mobile Device Management-Anbietern • Nahtlose Directory-Integration, die die Weichen für einen vollständig automatisierten End-to-End-Identity-Lifecycle stellt – von der Provisionierung bis zur Deaktivierung – mit einer flexibel wählbaren Single Source of Truth • Unterstützung aller offenen Authentisierungsstandards • Sicherer hybrider IT-Zugriff auf geschäfts-kritische Business-Anwendungen und Multi-Cloud-Umgebungen über eine konsolidierte Identity-Plattform	• Freie Auswahl von Best-of-Breed-Lösungen – jetzt und in Zukunft • Die Möglichkeit, das Potenzial bestehender Investitionen voll auszuschöpfen (z. B. Public-Cloud-Anbieter) • Reduzierung des manuellen Aufwands für Mitarbeiter, Administratoren und Entwickler • Schnellerer Rollout und kürzere Time-to-Market • Mehr Effizienz im Betrieb und in der Entwicklung • Stärkeres Security-Standing

Um einzuschätzen, wie wichtig Herstellerunabhängigkeit für Ihr Unternehmen ist, stellen Sie sich die folgenden Fragen:

- Wie viele Abteilungen Ihres Unternehmens werden auf den Identity-Anbieter angewiesen sein?
- Wie viele Technologie-Stacks muss Ihre IAM-Lösung unterstützen?
- Wie oft integrieren Ihre Stakeholder oder Business-Units neue Technologien?
- Wie lange dauert es im Schnitt, eine neue, unternehmensweite Anwendung auszurollen, oder eine „Big Bang“-Technologie? Erwartet man von Ihnen, dass Sie Rollouts immer schneller abwickeln?
- Wie viel könnte Ihr Unternehmen sparen, wenn Rollouts weniger Zeit in Anspruch nehmen würden?

> “
>
> Jede neue Anwendung, die Sephora einführt, wird sofort in Okta integriert. Die technische Umsetzung der Integration einer neuen App nahm früher Wochen oder sogar Monate in Anspruch. Mit Okta dauert sie weniger als einen Tag.
>
> Arnaud Feyssaguet, IT Infrastructure Manager, Sephora

Faktor #2: Individualisierung

Ihre IAM-Lösung sollte sich an Sie anpassen, damit Sie sich flexibel an neue Business-Anforderungen anpassen können

Unternehmen stehen nicht still, also sollten es IAM-Lösungen auch nicht tun. Die Kontrolle der Mitarbeiterzugriffe ist ein wichtiges Thema, und die Wünsche von Verbrauchern ändern sich ständig. Eine strategische IAM-Lösung sollte jeden Benutzer (Mitarbeiter, Kunden, Partner und Lieferanten) über den gesamten Identity-Lifecycle hinweg im Blick behalten, und zwar sowohl die Mitarbeiter als auch die Kunden. Ihr Unternehmen sollte sich Gedanken darüber machen, wie Identities dazu beitragen können, den Fokus auf die Kunden zu maximieren, ohne den Betrieb zu behindern.

Stellen Sie bei der Evaluierung einer IAM-Lösung sicher, dass diese folgenden Anforderungen gerecht wird:	**Ihre Vorteile im Überblick:**
• Möglichkeit zur No-Code- und Low-Code-Individualisierung • API-zentrierte Architektur mit umfassend erweiterbarem Framework • Dynamische Workflows für eine einfache Automatisierung der User-Lifecycles und der Access-Policies • Transparenz über alle Device-Identities, um kontextbasierte Security-Policies entwickeln zu können • Leistungsfähige Policy-Engine für die Erstellung dynamischer Access-Policies, die auf einzelne User, Use Cases, Devices und mehr zugeschnitten sind • Expression Languages, mit denen die Entwickler Attribute aus unterschiedlichen Systemen referenzieren, transformieren und kombinieren können, um sie in einer Single Source of Truth zu konsolidieren	• Schnelle Bereitstellung neuer User-Experiences (z. B.: schnelles Onboarding neuer Mitarbeiter, schnelles Deployment neuer App-Integrationen und mehr) • Stärkung des Security-Standings • Geringerer Entwicklungsaufwand für neue Workflows • Höhere Effizienz im Betrieb (z. B.: ‚Mit weniger mehr ereichen', indem die verfügbaren IT-Ressourcen und Budgets optimal ausgeschöpft werden) • Bieten Sie Ihren Kunden eine hochwertigere Customer-Experience, um sie langfristig zu binden

Um einzuschätzen, wie wichtig flexible Individualisierungsoptionen für Ihr Unternehmen sind, stellen Sie sich die folgenden Fragen:

- Wie viel Zeit und Geld wenden wir auf, um neue Workflows zu entwickeln und bestehende Workflows zu pflegen?
- Wie viel Entwicklungszeit investieren wir in individuelle Automatisierungsfeatures?
- Wie viele Ressourcen bindet es, individuelle Landing Pages für Kundenanwendungen und B2BV-Partnerportale aufzusetzen?
- Wie viel Zeit brauchen wir, um regulatorische Vorgaben, Compliance-Bestimmungen und Audit-Anforderungen umzusetzen (z. B.: DSGVO, FedRAMP, SOX, CCPA, u.a.)?
- Wo stehen wir mit Blick auf die Umsetzung einer Zero-Trust-Security-Strategie? Was müssen wir tun, um unsere nächsten Meilensteine bei diesem Projekt zu erreichen?

> “
>
> Wenn uns ein Fehler nicht auffallen sollte und er im SOX-Audit bemerkt wird, müssten wir ihn an die US Securities & Exchange Commission melden. Das ist für jedes Unternehmen ein großes Risiko.
>
> Curtis Salinas, Senior Director,
> Strategic Planning & Operations, Slack

Faktor #3: Bedienfreundlichkeit

Ihre IAM-Lösung sollte benutzerfreundlich sein, um Ihren Mitarbeitern, Kunden und allen anderen eine hochwertige Experience zu bieten.

IAM-Lösungen, die sich über den gesamten Identity-Lifecycle hinweg nahtlos mit Ihren Anwendungen und Devices integrieren lassen, sind oft aufwändig zu entwickeln, kostspielig zu warten und kompliziert zu nutzen. Eine strategische Identity-Lösung sollte für Entwickler, Administratoren und Endanwender gleichermaßen einfach und intuitiv zu bedienen sein. Andernfalls riskieren Sie, knappe IT-Ressourcen zu vergeuden und/oder die User-Experience zu beeinträchtigen, was Ihrem Umsatz oder Ihrem Ruf schädigen könnte.

Stellen Sie bei der Evaluierung einer IAM-Lösung sicher, dass diese folgenden Anforderungen gerecht wird:	**Ihre Vorteile im Überblick:**
• Zentralisierte Konsole, mit der Ihre Admins alle User, Apps und Policies verwalten können • Self-Service-Tools wie Quickstart-Guides und Integrations-Wizards für Ihre Admins • Widgets, APIs & SDKs für die gesamte User-Authentifizierung, die Konfiguration Ihrer Ressourcen und die Steuerung der Zugriffe • Ihre Entwickler erhalten Zugang zu einer Vielzahl von Ressourcen, die ihnen helfen, Identities schnell und effizient in jedes Entwicklungsprojekt einzubinden • Möglichkeit, Identity-zentrierte Prozesse ohne Code zu automatisieren • Einfache Integration in die Apps und Systeme Ihres Unternehmens • Möglichkeit zur No-Code- oder Low-Code-Individualisierung • Social Login für eine besonders komfortable Anwendung • Passwortlose Authentisierung • Volle Transparenz über alle sicherheitsrelevanten Prozesse – mit Monitoring und Reporting über alle User, Apps und Devices hinweg	• Geringere Betriebs- und Wartungskosten • Bessere Workforce-Experiences • Schnellere Integration mit Best-of-Breed-Security-Lösungen • Hochwertige digitale Experiences für Ihre Endanwender • Höhere Akzeptanz in Ihrem Unternehmen • Höhere Kundenzufriedenheit und Kundenloyalität • Stärkeres Security-Standing

Um einzuschätzen, wie wichtig Benutzerfreundlichkeit für Ihr Unternehmen ist, stellen Sie sich die folgenden Fragen:

- Wie viel Code erfordert die Individualisierung unserer Dienste?
- Wie integrieren wir neue Apps und Systeme?
- Wie hoch ist der manuelle Aufwand für die Entwicklung und das Management Identity-zentrierter Prozesse?
- Haben wir lückenlose Transparenz über alle User, Apps und Policies?
- Wie viele Ressourcen bindet die Entwicklung unserer Identities?
- Wie wirkt sich unser Stack von Business-Anwendungen auf die Produktivität unserer Mitarbeiter aus?

> “
>
> Die Einführung einer durchgängigen Identity-Ebene hat uns sehr geholfen, neue Kunden zu erreichen, neue Nutzer schneller einzubinden und die Customer-Experience nachhaltig zu verbessern.
>
> Emnet Gossaye, Security Software Engineer, Kensho

Faktor #4: Zuverlässigkeit und Sicherheit

Sie müssen sich auf Ihre IAM-Lösung verlassen können. Sie muss zuverlässig und sicher sein.

IAM ist ein geschäftskritischer Dienst, der auf Vertrauen aufbaut. Eine strategische IAM-Lösung verbindet Menschen sicher mit Technologien – und managt zuverlässig die wertvollsten Daten des Unternehmens: die Benutzeridentitäten. Vertrauen ist alles, und wenn sich Ihre Kunden aufgrund planmäßiger oder außerplanmäßiger Ausfälle oder aufgrund von Sicherheitsrisiken nicht auf Sie verlassen können, ist das ein Problem. Ein Problem, das zu sinkenden Einnahmen und steigenden Kosten führt – und damit in jeder Hinsicht eine Katastrophe.

Stellen Sie bei der Evaluierung einer IAM-Lösung sicher, dass diese folgenden Anforderungen gerecht wird:	**Ihre Vorteile im Überblick:**
• Keine planmäßigen Stillstandzeiten • Selbst-heilende Nodes • 99,99 % SLA in der Uptime • Modell der geteilten Security-Verantwortung • Security-Tools, die Ihr Security-Standing mit handlungsrelevanten Empfehlungen proaktiv verbessern • Definieren Sie eigene Security-Perimeter, an denen Zugriffe eingeschränkt oder reguliert werden können	• Gewinnen Sie das Vertrauen Ihrer Mitarbeiter und Kunden • Durchgängige Verfügbarkeit Ihres Unternehmens • Vermeidung rufschädigender Security-Vorfälle • Stärkung des Security-Standings

Um einzuschätzen, wie wichtig Resilienz für Ihr Unternehmen ist, stellen Sie sich die folgenden Fragen:

- Welche Folgen hätten regelmäßige oder langfristige Ausfälle Ihrer Systeme für Ihr Unternehmen? Würde die Produktivität leiden? Würden Sie Umsatz und Kunden verlieren?
- Wie viel Geld könnten Sie sparen, wenn Ihre Uptime bei 99,99 % oder höher läge?
- Ordnen Sie die Anbieter, die Sie in Betracht ziehen, nach ihren früheren Ausfallzeiten. Wer schneidet am besten ab?

> “
>
> Früher mussten Entwickler Code oft neu schreiben, weil er nicht sicher war. Heute funktioniert es gleich im ersten Anlauf, was für alle Beteiligten besser ist. Ihre Arbeitszufriedenheit steigt, da sie schneller einen Mehrwert schaffen können und keine Zeit mit der Behebung von Compliance-Problemen verbringen.
>
> Justin Moore, IAM Manager,
> NOV Inc

Fazit

Die Modernisierung der IT ist für jede IT-Abteilung ein langfristiges Projekt. Die vergangenen beiden Jahre haben die Taktung der Projekte spürbar erhöht, uns letztlich aber vor allem verdeutlicht, wie anspruchsvoll die Aufgabe wirklich ist.

Ungeachtet all Ihrer Vorteile bedeutet die Migration in die Cloud auch, dass viele Abteilungen zur Schatten-IT geworden sind: Sie integrieren auf eigene Faust neue Best-of-Breed-Lösungen, um ihre Technologie-Stacks so aufzubauen, wie es das Business erfordert. Dies macht viele Unternehmen anfällig für die steigende Zahl anspruchsvoller, Identity-basierter Angriffe. Hinzu kommt, dass wir alle von den Unternehmen, mit denen wir interagieren, immer mehr erwarten – sei es als Kunde oder als Mitarbeiter. Das richtige Gleichgewicht zwischen Security (und damit Vertrauen) und einer hochwertigen User-Experience zu finden, ist für Unternehmen keine leichte Aufgabe. Aber die richtige Identity-Lösung kann dabei helfen.

IAM ist der Klebstoff, der die vielen Technologie-Stacks zusammenhält. So können Unternehmen ihren Mitarbeitern und Kunden hochwertige Omnichannel-Experiences liefern, die gleichermaßen sicher wie zuverlässig sind.

Die Mindestanforderungen haben wir gerade definiert: Die IAM-Lösung sollte herstellerneutral, flexibel anpassbar, einfach zu bedienen und nicht zuletzt sicher und zuverlässig sein. All das – und mehr – bietet Ihnen Okta. Wir würden Ihnen gerne zeigen, wie wir anderen Unternehmen dabei geholfen haben, Zeit zu sparen, Risiken zu minimieren und die Kosten für das Identity- und Access-Management zu senken.

Um mehr über den tatsächlichen Mehrwert einer IAM-Lösung zu erfahren, besuchen Sie den ROI-Kalkulator und den Business-Benefit-Kalkulator von Okta.

Kontaktieren Sie uns noch heute, wenn Sie über Ihre konkreten Anforderungen sprechen möchten.