# How to Choose an Identity Solution You Can Trust

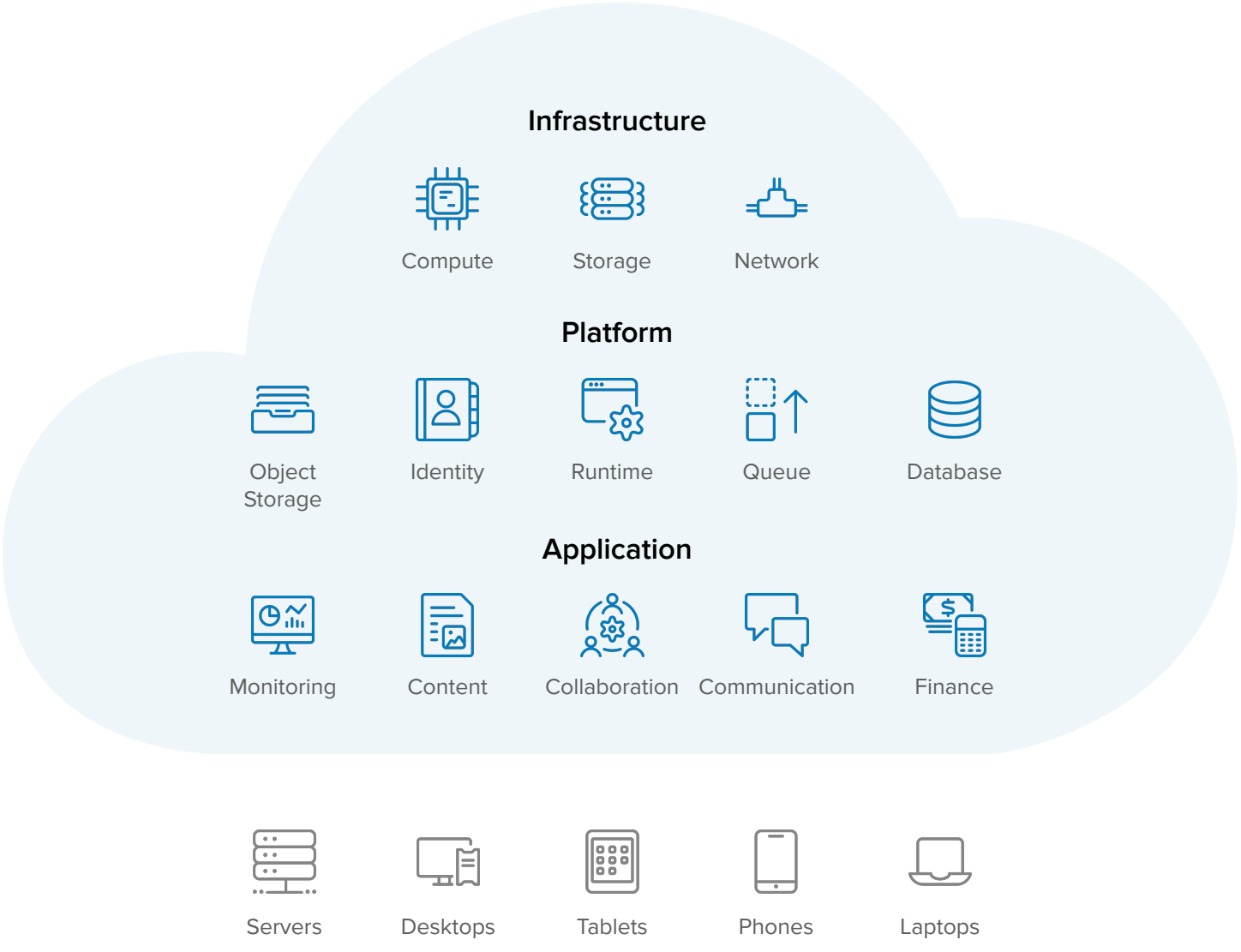
## 5 Ways to Pressure-test Identity Services

okta

# Index

# Not all technology services are built alike

To win in today's fast-moving digital world, companies are increasingly adopting innovative technologies. Solutions such as Infrastructure-as-a-Service, Platforms-as-a-Service, Software-as-a-Service, and hybrid multi-clouds offer greater flexibility and quicker time to value. These approaches help IT systems scale with self-service agility and adaptability, all while freeing developers' bandwidth to focus on building code for core business services.



But relying on outside services also brings inherent risks. No one wants to deal with that midnight call reporting that your mission-critical business application is down, or the typical follow-on scenario...waiting in limbo until the vendor finally gets their system back online, while your workforce loses days of productivity.

It gets even worse if one of these services fails to protect your customer data. A security breach can have devastating effects, since 92% of consumer victims either lose trust or stop doing business with the company entirely, 85% tell others about their experience, and 34% use social media to complain about having their information stolen. Organizations hit by data breaches lose an average of $3.92 million as a result of customer churn, regulatory fines, and more.

So, what can you do about all this? While it may be hard to trust an external vendor with your valuable data, home-grown platforms require a lot of time, cost, and effort to be spent on something that takes you away from driving innovation. It's simply not reasonable for most IT and security teams to deliver reliability or protection at the same level of sophistication as a large solution provider that supports billions of users. As you continue to leverage everything as-a-service and hybrid IT, there are several major considerations you should review in order to assess how trustworthy each technology service is, so you can select reliable partners.

### The impact of a security breach by the numbers

**92%**

of consumer victims either lose trust or stop doing business with the company entirely

**85%**

tell others about their experience

**34%**

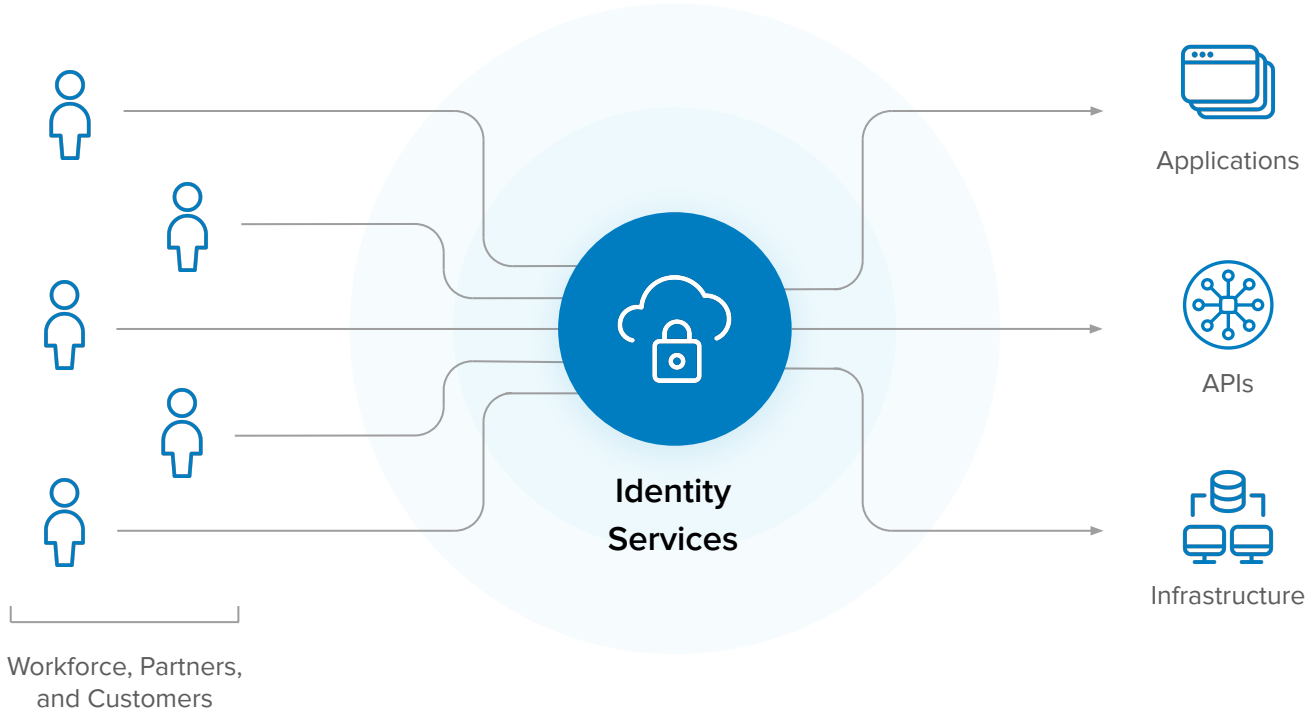
use social media to complain

**$3.92m**

Are lost on average by organizations hit by data breaches

## Protecting the keys to your kingdom with identity and access management

When you look at the services surrounding your company's most critical apps and data, there's no doubt identity and access management is mission-critical to your technology ecosystem. Businesses can't operate without the ability to securely authenticate employees, partners, and customers, so the impact of an identity outage or breach is more severe than with any other system. You're putting a lot of trust into this foundational layer of protection, and your solution's security and reliability are too important to compromise with 'good enough.'




Given this, it's paramount to carefully evaluate identity services. Rather than just accept the status quo, or jump hastily into a new solution, be cognizant of all of the benefits and disadvantages that come with various identity options—whether a home-grown system or one built by a software vendor, hosted on-premises, in a hybrid environment, by a managed service provider, or a cloud-native solution.


# 5 pillars of trusted identity

There are five primary aspects to consider when looking for an identity solution that you can trust with the keys to your kingdom. Recognizing where your provider stands on each of these important attributes could make the difference between gaining a robust service that powers secure, scalable, always-available experiences, or getting stuck with a non-proven vendor and software that breaks down unexpectedly.

## Transparency

First and foremost, trust starts with transparency. It's hard to know whether you can trust your vendor if they don't offer public resources and third-party validation detailing their security, reliability, or scalability efforts. Look for identity providers that take this very seriously and demonstrate their commitment to trust and transparency. They should provide accurate, real-time specifics about their service record with key performance indicators like outages, root cause analysis, and legal or regulatory compliance. For example, their security and privacy documentation should be easy to find and their service-level agreement (SLA) should include simple language about exactly what it covers or excludes.

It's not a good sign when your solution provider points you to clauses buried in a jumble of unrelated documentation. Expect clear, concise security details that are specific to the identity system itself, as opposed to other products and tools in their portfolio. Choose a vendor that has demonstrated this kind of transparency consistently over several years, and maintains a large customer base across different use cases, integration complexities, identity user volumes, industries, and special event handling.

But relying on outside services also brings inherent risks. No one wants to deal with that midnight call reporting that your mission-critical business application is down, or the typical follow-on scenario...waiting in limbo until the vendor finally gets their system back online, while your workforce loses days of productivity.

### Questions to ask identity solution providers:

1. How long has the company been around?
2. How many customers are publicly referenceable? How diverse are their use cases and scale requirements?
3. Do you have a single trust portal with all the security, compliance, and availability information I need readily available?
4. Will you give us the ability to test the security and performance of your service?
5. Who leads your security team and where do they fall in the reporting structure of the organization? How often do they meet with customers?
6. Do you operate under a shared security responsibility model with customers, and are the expectations clearly delineated somewhere?

## Security

In the current threat landscape, breaches happen every day—making world-class security a non-negotiable essential when selecting an identity partner. Their security measures should be far-reaching across all their services, but pay special attention to their data cryptography (at rest and in transit), credential hashing, and software development lifecycle practices. For example, since the most secure credential hashing methods consume a ton of computing power, some vendors purposely take shortcuts or rely on older algorithms not suitable for the modern world, like SHA1 and MD5, instead of more powerful and secure methods like salted Bcrypt. This could be a warning they're not well-equipped to handle complex database and architectural requirements, which puts your critical user credentials at risk in the event of an attack.

Another crucial area is your solution provider's privileged access management controls, their approach to Zero Trust principles, and how they help you implement security best practices. Make sure they have policies and procedures in place that verify all users based on their identity and device in order to limit who can access the system's critical infrastructure and platforms.

Identity vendors should also follow security best practices throughout their internal development process, including extensive quality testing and assurance, rapid deployment of fixes and patches, and the ability to revert changes if needed. Consider the breadth of their penetration testing program, and whether they provide you with tools to help improve your security posture, such as your own environment for security testing.

When it comes to security, keep in mind that some multi-tenant cloud architectures can create very helpful network effects as the service learns and evolves based on various use cases across billions of users. Your identity solution should uncover recurring threats from suspicious IPs against one or more customers for the benefit of all, and then use that valuable risk analysis to inform authentication decisions. In addition, solution providers should partner and tightly integrate with other best-in-class tools for capabilities, such as bot detection, identity proofing, and security information and event management (SIEM)—ensuring end-to-end protection. These robust security capabilities are rarely found in home-grown solutions, on-prem services, managed cloud services, or from vendors that ported on-prem software to the cloud.

## Questions to ask identity solution providers:

1. What type of Zero Trust controls do you employ internally to support access management?
2. What role does security play in your software development lifecycle? How many development tests do you run per release?
3. What kinds of pen testing do you perform? Just internal, or third-party and customer testing as well? Do you have a public bug bounty program?
4. What credential hashing methods do you use, and how well do they scale?
5. What type of encryption do you use for data in transit and data at rest? What type of redundancies have you built in to ensure reliability and business continuity?

## Questions to ask yourself about an identity solution:

1. Are its security capabilities a few steps ahead of my current needs, so we'll be able to keep advancing our security posture?
2. Does the vendor offer tools and pragmatic guidance to help us keep up with emerging security trends, such as DevOps, DevSecOps, and Zero Trust?

# Reliability

In technology, things break. It's inevitable that there will be unexpected problems, but this doesn't mean you have to tolerate interruptions due to vendor-related issues. There's never a good time for your critical identity service to go down, so identity should be built and operated with the expectation that it must always stay on no matter what occurs behind the scenes. Avoid solution providers that blindly consume IaaS, PaaS, or SaaS services without implementing their own controls to ensure redundancies, as this makes them susceptible to outages if those underlying platforms crash.

Aim to adopt an identity architecture that supports this redundancy at every layer of the stack so it remains reliable, resilient, and highly available. This is another area where multitenancy brings important benefits, since all customers use the same environment, and service providers can focus on making this shared infrastructure extremely robust. Your vendor should employ dedicated engineering teams who monitor, detect, and resolve issues quickly, hopefully before they become visible to any customers.

As we mentioned above, it's also helpful to look closely at the system's SLA. Some can be misleading, as many service providers still require planned downtime for maintenance and patching activities, but carefully remove those from their SLA metrics and availability reports. Others use vague language, such as "does not include downtime that results from a Customer Cause or a Force Majeure Event." Dig into exactly what these terms mean, so you can more accurately estimate how much downtime to expect throughout the lifetime of your solution.

## Questions to ask identity solution providers:

1. What does your SLA encompass? How much planned downtime should we expect?
2. Do you have a website where we can view current and historical uptime and service issues? Does the site report publicly planned outages?
3. Do you have dedicated engineering teams focused on performance monitoring, detecting and resolving issues, as well as introducing new reliability innovations?
4. What is your average mean time to respond (MTTR) to incidents?
5. How does your underlying architecture support reliability and resiliency?
6. Does the service run on multiple availability zones that are geographically separated?
7. Is there built-in auto-failover or do customers have to manually recover systems?
8. How fast can you perform disaster recovery in a worst case scenario?
9. Do you ensure redundancy by using multiple DNS providers, routers, load balancers, cache, telephony, etc.?

### Questions to ask yourself about an identity solution:

1. How far back does their public outage data go?
2. Is it consistent with third-party reports, like those from StatusGator?
3. Do they regularly provide root cause analysis? If so, are there any recurring themes?

## Scalability & Extensibility

Many organizations experience spikes and dips due to seasonality, general business growth, or geographic expansion. For example, e-commerce companies want their customer identity solutions to run at the volumes of Amazon Prime Day at a moment's notice. Your identity system should be architected for massive scale so it can support authentication and authorization bursts without any service disruption—which would erode the customer experience and compromise employee productivity.

Many legacy on-prem products, or even identity vendors with hybrid or cloud models, require additional resources to handle user fluctuations or triage capacity issues because they scale infrastructure separately for each customer. As a result, these solutions often compromise performance, availability, and even security when attempting to meet scalability needs. To be sure you can trust your identity provider in a rapid growth scenario, ask whether they employ elasticity, automation, and self-healing to easily spin resources up and down. As with reliability, supporting this kind of scale requires ongoing management and monitoring, with a constant feedback loop and visibility across the tech stack.

A related consideration is the extensibility of your identity solution. Can it manage every user (employees, partners, customers) and resource type (apps, APIs, infrastructure) you might need with a single platform? Think about whether it is flexible enough to provide a single lens for all your users, along with access for each and every resource in your digital landscape as it evolves—both today and into the future. Extensibility is also key for developer productivity.  Adopt a partner that offers a full range of SDKs and APIs across the major technology platforms (e.g., Java, Node.js, JavaScript, PHP, C) and modern UI/UX tools (such as Angular, React, and others) your engineering teams use.

### Questions to ask identity solution providers:

1. What are the largest use cases you've handled?
2. How broad is your geographic reach?
3. Do you have data centers and referenceable customers in multiple regions?
4. Do you use automation to dynamically add, heal or remove servers on demand?
5. What is your built-in capacity to handle unexpected traffic?
6. How many API calls per minute can you handle without performance degradation? Do you have any delays on syslogs and reporting?
7. How broad is the ecosystem of best-of-breed apps you support?

### Questions to ask yourself about an identity solution:

1. Is there customer validation for high-volume use case claims, or do they expect me to take their word for it?
2. Will we end up needing a separate platform to support emerging external identities, such as customers, partners, or contractors?
3. What is their time-to-market for building connectors to new business apps or infrastructure we might adopt down the road?

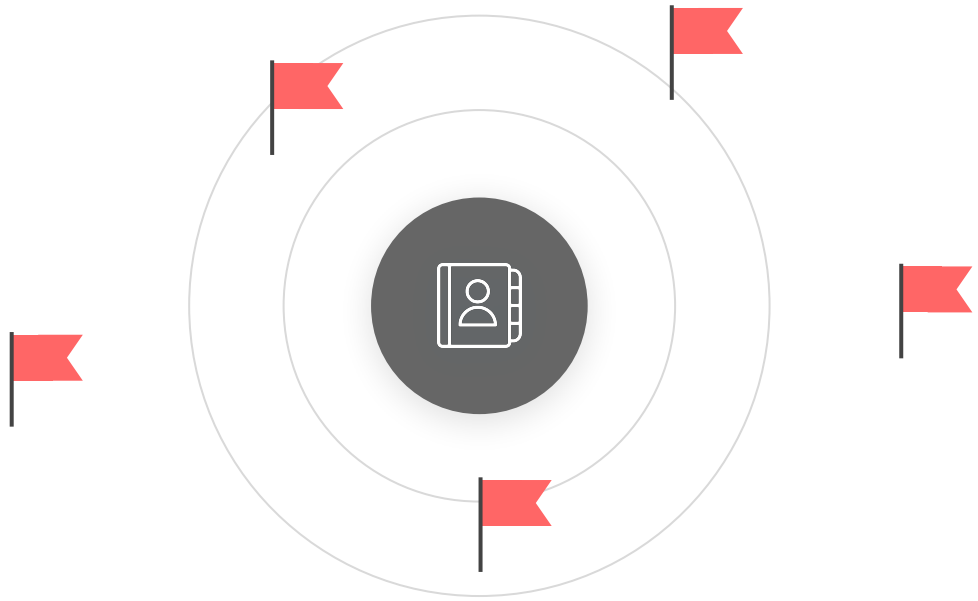
## Privacy & Compliance

All enterprises deserve an identity service that's designed to meet the rigorous requirements of even the most security-sensitive organizations and industries. Privacy is an essential driver of trust, especially as companies work to comply with tough privacy regulations, such as HIPAA, GDPR, and the new California Consumer Privacy Act (CCPA). You'll want to determine what methods your identity provider has in place to handle data privacy and tenant segregation. For instance, find out whether they keep tenant data separate and secure, and whether they can isolate user data in region-specific data centers.

When evaluating an identity solution, check that it's routinely audited and has achieved certifications from trusted, independent firms. However, keep in mind that these reports can vary quite a bit. Some companies choose to limit the extent of the controls and processes they include in an audit, due to the significant due diligence, time, and cost it entails. A provider might say they have SOC 2 Type II certification, but it may only cover a portion of their services. Others may present reports from their underlying infrastructure providers and claim them as their own service certification. They could also say they offer a FedRAMP or HIPAA-compliant service, but without providing separate dedicated environments with enhanced audit controls and reports, or extended retention of personally identifiable information.

## Questions to ask identity solution providers:

1. Where is your privacy policy documented?
2. Which certifications are for your solution versus areas you'll help my company get compliant with?
3. What is the specific scope of each compliance certification you claim?
4. How do you support the requirements of the most prevalent data privacy regulations such as GDPR and CCPA?
5. Can you provide the full results from a recent penetration test by an industry-recognized third party, or allow our team to perform their own penetration test?
6. Do you offer a dedicated HIPAA and / or FedRAMP environment with enhanced security and audit controls?
7. What customer / tenant segregation measures do you employ to ensure privacy and performance?



# Red flags your provider might not be trustworthy

The five pillars above comprise just some of the many attributes IT security and development teams should review prior to entrusting their identity management to a new solution provider. To recap, here are some top indicators that a vendor won't deliver the high security and reliability your business requires:

1. Lack of a comprehensive and transparent trust portal for customers
2. Cutting corners on fundamental security practices and controls
3. Inconsistent (or missing) validation from industry analysts like Gartner and Forrester
4. Limited customer references or success stories across diverse industries and large-scale use cases
5. Planned downtimes and outages, or breach reports and claims that don't match third-party findings
6. Recurring patterns amongst root cause descriptions, such as MFA outages
7. Failure to provide customers with mechanisms to verify security for their own pen testing
8. Use of weak credential hashing with older cryptographic algorithms
9. Lack of (or limited) public documentation on company privacy and security policies
10. Lack of routine (or comprehensive) audits and certifications from multiple independent third parties

# How Okta drives continuous innovation

With identity management, any trust tradeoff can sabotage your efforts to protect people, data, and resources against vulnerabilities. To avoid breaches or outages that wreak havoc on your business, only partner with technology providers who embrace a continuous improvement culture around security and reliability. Your identity service should be more secure, reliable, and scalable than anything you could build and operate on your own. Cloud-native identity solutions like Okta uniquely address these requirements, while allowing companies to become more agile and nimble. As a result, you can accelerate modernization and digital transformation, while maximizing your return on investment (ROI) and reducing total cost of ownership (TCO).


At Okta, we adhere to the highest standards for security and reliability in all we do—from hiring, to the architecture and development of our software, to our data center strategies and operations. This is why each Okta code commit passes more than 60,000 tests before we release it to our master codebase. We also believe in the customer's right to conduct penetration tests on Okta, and so we provide them with test environments to do that.

Our highly redundant and resilient architecture is elastic, scalable, and uses automated health checks to ensure our solution stays up even when other, large platforms such as AWS go down.

In addition, Okta's security practices include multi-layered encryption to protect data at rest and over the wire, Zero Trust principles and segregation of duty controls to mitigate unauthorized user access, and next-gen architecture that lets us isolate customer data to ensure tenant privacy and performance. We even offer innovative security products such as Okta ThreatInsight, which uses global network intelligence across our thousands of customers to identify suspicious IPs and automate risk-based assessment and response prior to authenticating users.

Visit https://trust.okta.com/ to learn more about our system status, security approach, and many compliance attestations.

## About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 6,000 apps, the Okta Identity Cloud enables simple and secure access from any device. Millions of users and thousands of customers, including NASDAQ, Experian, Western Union, CNA Financial, Allergan, Albertsons, Nordstrom, Hertz, Priceline, and 20th Century Fox trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work. For more information, visit us at www.okta.com or follow us on www.okta.com/blog.