Buyer's guide

Your guide to getting C-suite buy-in for Okta IAM

Your guide to productive IAM conversations with security, IT, and finance teams

You did your research, tracked down all the information you needed, and decided that Okta's Workforce Identity Cloud is the best Identity and Access Management (IAM) solution for your organization.

Now comes the next step: getting buy-in across teams. Consider this your secret weapon. Read on for a comprehensive guide to pitching Okta to leaders of the teams it will impact most: security, IT, and finance.

Quick links by team

CISO or security teams

CIO or IT teams

CFO or finance teams

Getting buy-in from your CISO and security teams

Cybersecurity is a board-level initiative — one that informs top-level risk management and mitigation strategies. Modern, unified IAM will strengthen your company's security posture by ensuring secure access to sensitive corporate resources.

The CISO POV

A Chief Information Security Officer (CISO) is chiefly responsible for protecting the company or organization's intellectual property, proprietary data, and information assets. CISOs and the security teams they lead manage and oversee all information security needs within an organization and are responsible for both proactive and reactive security.

Teams that fall under CISO orgs

- Offensive Security
- Governance, Risk, and Compliance (GRC)
- Infrastructure and Data Protection
- IAM
- Network Security
- Security Operations Center

Why CISO teams need Okta for IAM:

- Stay ahead of Identity threats (phishing, password spray, cred stuffing, etc.)
- Build customer trust and protect brand reputation
- Do more with less

> "Okta is the center of our Zero Trust universe."
>
> Steve Williams, Enterprise CISO, NTT Data

Why IAM matters across security teams

IAM lays the foundation for strong, integrated security across the organization.

Offensive Security: Identify and correct deviations from corporate access standards (roles, policies, permissions, etc.) across infrastructure and applications.

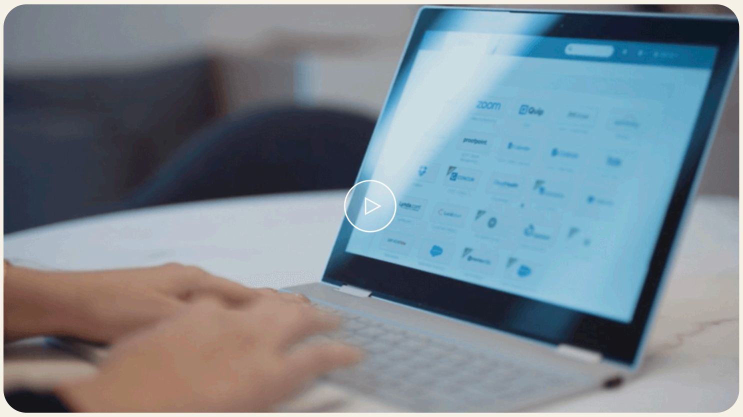
Governance, Risk, and Compliance: Define and manage roles across resources (entitlements), run access certification campaigns, and simplify evidence collection for audits.

Infrastructure and Data Protection: Define and manage access requirements (e.g., SSO, MFA, etc.) to any infrastructure or data app and manage privileged access to highly critical infrastructure.

Network Security: Set customizable requirements for network access based on device health, geolocation, past login patterns, and risk levels.

Security Operations Center: Quickly pinpoint a user login and account context (e.g., whether MFA was required on login, where the login was initiated from) and identify gaps in security policies to share back to IAM team.

Without Okta / Current State of IAM	With Okta
You’re locked into a vendor that slows down or prevents new (and much-needed) security integrations like EDRs, SIEMs, MDMs, SASEs, etc.	Leverage best-in-class tools with a neutral, cloud-native IAM platform that integrates easily with every component of your security stack. **40% reduced security risk by leveraging signals from third parties.**
You’re leveraging MFA, but inconsistencies in policy enforcement across device platforms create security gaps.	Enforce phishing-resistant MFA on all major platforms, for all users (including partners and contractors).
You’re relying on different vendors for IAM, PAM, and IGA, which creates administrative friction across products.	Improve employee UX with a unified platform for all Identity use cases (including IAM, PAM, and IGA).
Manual, decentralized provisioning creates orphaned guest accounts (for past contractors and partners, for example) that lead to avoidable vulnerabilities.	Centralize provisioning for any user type (including management of roles and entitlements) and leverage automation tools that save time and improve security posture.
You’re experiencing up to 8 eight hours of report latencies when using the next leading Identity provider.	Get real-time reports with user and device context via Okta’s Syslog.



WATCH

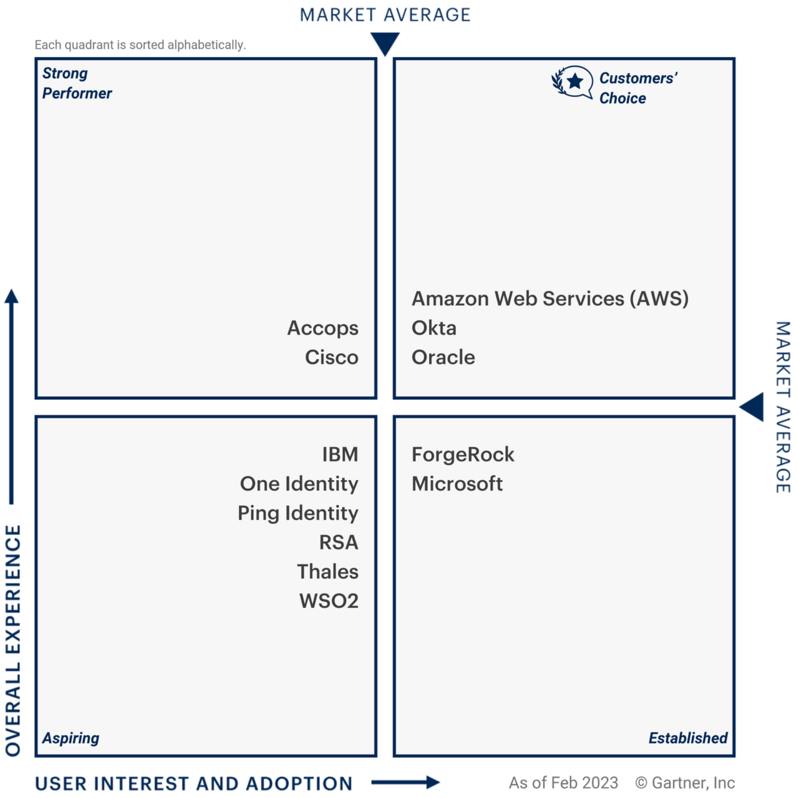
CISO case for choosing Okta in 3 minutes.

Okta is recognized as a Customers' Choice in Access Management in Gartner's Peer Insights Report, performing better than several prominent IAM providers, including Microsoft.

Did you know?

Only 34% of admins using Microsoft's Entra ID (formerly known as Azure AD) have MFA enabled on their accounts, while **90% of Okta admins actively use MFA.** Okta takes a "secure by default" approach to protecting all administrator accounts.

Gartner Peer Insights "Voice of the Customer" Access Management



As of Feb 2023 © Gartner, Inc

Gartner

Getting buy-in from your CIO and IT teams

IAM is a key business differentiator that connects the IT team to core goals like driving productivity and agility. Modern IAM enables secure and seamless customer experience (CX) for employees, partners, and customers, further aligning the organization’s tech stack with its business objectives.

The CIO POV

Chief Information Officers (CIOs) are responsible for driving innovation and growth through technology. Alongside their IT teams, they define how the organization can use its technological expertise to improve CX, accelerate speed to market, and hone the competitive edge that sets them apart from the competition. This involves working cross-functionally with development, product, security, and finance teams to build a clear, tech-empowered vision for the organization.

Teams that fall under CIO orgs

- Infrastructure / IT Administration
- Digital Innovation and Strategy
- Enterprise Architecture
- IT Procurement
- IT Service Management / Help Desk

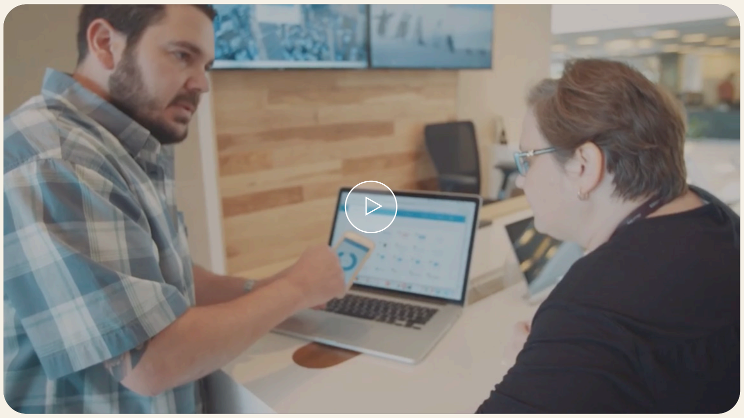
Why CIO teams need Okta for IAM:

- Drive innovation with a flexible platform that scales with the business (global expansion, M&A, etc).
- Deliver better digital experiences across the entire organization (e.g., self-service for employees)
- Empower IT to do more with less (more automation)

> “We wanted a solution that would play with everybody. We didn't want it to be overly tied to a particular vendor because we wanted to continue to be able to choose from the best solutions possible.”
>
> Tim Nall, CIO, Brown-Forman

Accomplish key business goals with the help of modern IAM

Before Okta	After Okta
M&As and divestitures are hitting obstacles related to complex Identity integrations.	Provide business and IT teams with day-one access to all corporate resources during M&A and easily sync users across Active Directory domains. **Improve productivity by 30% by speeding up or avoiding domain consolidation of an acquired organization.**
Your IT teams need to manually provision and deprovision users from corporate apps, leading to tedious busywork and potential security gaps (e.g., a contractor mistakenly retaining access beyond the length of a business relationship).	Automate joiner, mover, and leaver processes to save time and improve security. **Reduce time spent on building and maintaining custom provisioning flows by 90%.**
Your company's Identity needs are being managed across multiple portals and vendors, leading to siloed IT and business functions that hinder collaboration.	Unify your approach to IAM, Privileged Access Management, Identity Governance, and automations with a centralized platform. **Increase IT admin productivity by 90%.**
Disjointed management of app ownership and a lack of integrated offerings are placing limitations on innovations that could improve employee and customer CX.	Leverage a suite of out-of-box integrations to SaaS apps, security integrations, HR integrations, and ITSM tools. **Increase IT productivity by 80% with out-of-box downstream integrations.**



WATCH

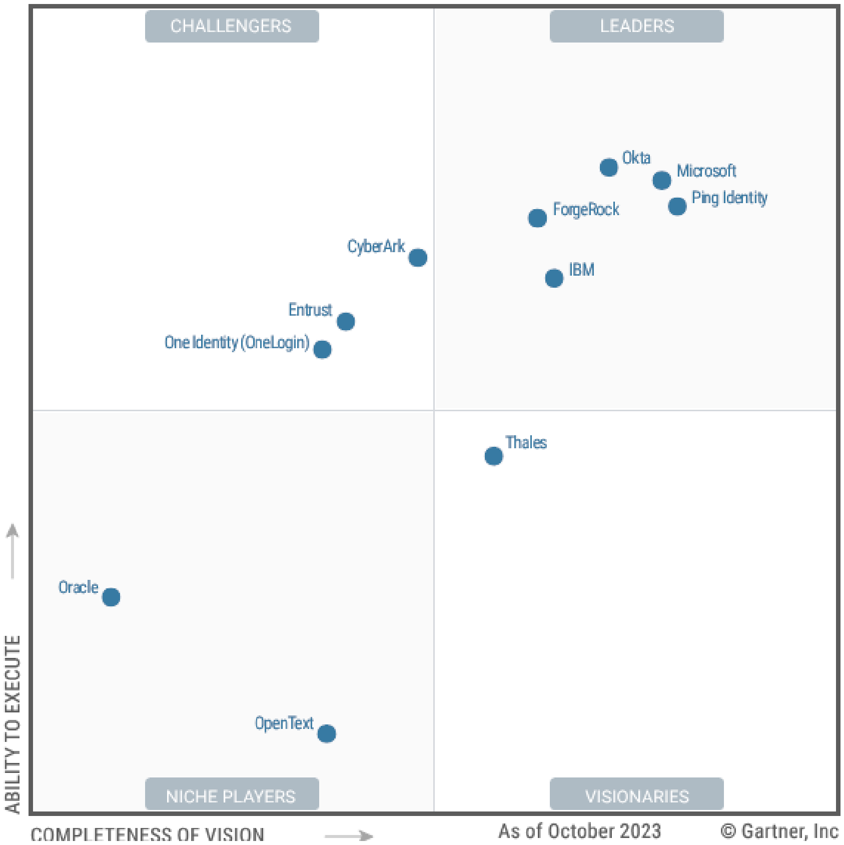
The CIO case for choosing Okta in two minutes.

In 2023, for the seventh year in a row, Gartner recognized Okta as a leader in the Magic Quadrant for Access Management, highlighting Okta's ability to execute over all other IAM vendors.

Did you know?

Microsoft customers still choose Okta for IAM needs. Here are six reasons why. Okta can integrate seamlessly with core Microsoft productivity tools like Office 365, Active Directory, Intune, and Windows.

Magic Quadrant for Access Management



Gartner

Getting buy-in from your CFO and finance teams

Modern IAM will save your company money. While it may seem like a large investment (especially in contrast to free point solutions), Okta eliminates hidden costs related to support, maintenance, and deployment — saving you money in the long term while empowering your IT teams to refocus their attention on more strategic business objectives.

“We already have a free IAM product. Why would we ever need to *buy* a new one?”

This is the primary form of pushback you’ll face from the finance and/or procurement teams in your organization. The short answer is that, in the long run, the costs incurred by these supposedly “free” IAM products vastly outweigh the cost of investing in a high-quality, cloud-native, vendor-neutral IAM platform like Okta.

In other words, your finance teams need to widen their view beyond the cost of an Okta license. They need to factor in the costs associated with deployment, maintenance, productivity losses due to low reliability, and more.

Visible Costs

- Enterprise agreement
- Service-level agreement

Hidden Costs

- Deployment costs
- Third-party software costs
- Losses from outages (monetary and reputational)
- Maintenance costs
- Technical debt
- Business impact and user experience (lack of productivity)

A closer look: How Okta saves you money

Before Okta

Your reliance on a single vendor places immense pressure on your IT team and ramps up support costs related to custom integrations, etc.

Incidental and support-related outages lead to a meaningful strain on your bottom line.

Slow deployments that prevent your company from realizing value.

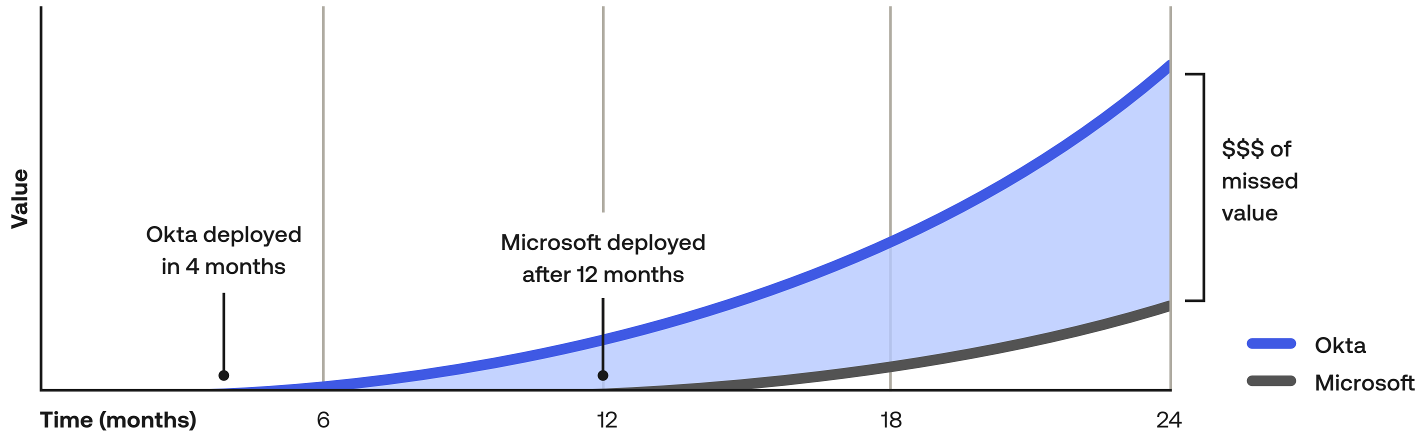
After Okta

Mitigate commercial and operational risk. Okta's vendor neutrality simplifies the task of connecting IAM to every part of your tech stack, **driving support costs down and allowing your IT teams to focus on more strategic initiatives.**

Increase reliability and uptime. Okta is extraordinarily reliable. From 2018 to 2023, the platform experienced **99.996% operational uptime,** translating to only 100 cumulative minutes of outages. Compare that to 1,500, the number of outage minutes experienced by another prominent Identity vendor from 2021 to 2023.

Deploy months faster than with other providers, so you start seeing value in a fraction of the time.

Realization of acquisition value



> "Microsoft was core to the original Identity strategy because it was free. But, we had to make a change after no progress was made after 5 years."
>
> Financial services company

Example cost-savings scenario:

The average Okta customer requires at least two user domain consolidations per year, equivalent to 400 hours of admin time. Using Okta saves these customers $40,000. Here's how:

400	×	2	×	$50	×	100%	=	$40K
hours needed to complete a domain consolidation project		domain consolidation projects per year		IT admin hourly wage (fully loaded)		improvement with Okta		total IT admin productivity saved by avoiding domain consolidation

Our current IAM infrastructure requires multiple solutions. Cost savings with Okta:

1	×	9	×	400	×	$50	×	90%	=	$162K
domain		IAM solutions		hours spent on administration per solution, per year		IT admin hourly wage (fully loaded)		improvement with Okta		total IT admin productivity saved by avoiding domain consolidation

See for yourself

Our ROI calculator gives you a quick breakdown of how much your company can save by switching to Okta.

Okta rated as "Best Value for Price" by TrustRadius for two consecutive years

Ready to take the leap?

As your company's resident IAM expert, you know that Okta's neutrality, high performance, and unmatched security make it the perfect fit for your organization's needs. With security, IT, and finance on board, you'll be up in no time, putting Okta's powerful functionality to use.

Your current reality

- Inadequate protection and security gaps
- Poor performance
- Costly ongoing admin that hinders growth

Your future with Okta IAM

- Robust security capabilities tailored to your needs
- Cloud-native efficiency and reliability (99.99% uptime)
- Scalable IAM that grows alongside your business

To learn more about the IAM platform or get in touch with an Okta representative, visit:

okta.com/contact

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements. Any products, features or functionality referenced in this material that are not currently generally available may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.