okta

5 Arguments to Justify Your Identity Spend

Okta Inc.
100 First Street
San Francisco, CA 94105

info@okta.com
1-888-722-7871

Spending on secure infrastructure is vital to protect any company's plans for revenue generation and business expansion. But when increasing focus and budget for security initiatives, CIOs and CISOs are faced with competing revenue-generating priorities across the business. And when it comes to identity spend—which today make up less than 9% of the average security budget, despite its potential to prevent the 80% of data breaches caused by compromised credentials —there's often a communication gap between the value of security infrastructure and key business initiatives.

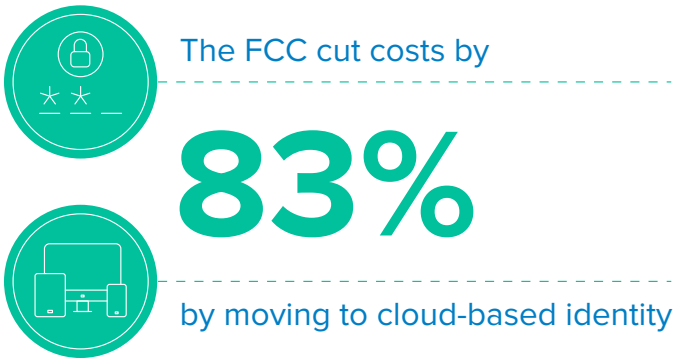
Armed with an understanding of the following five key business drivers and how identity feeds into them, technology leaders can better shift the balance in their favor and make a stronger case for increased identity spending organization-wide. By connecting security with each business driver, the organization as a whole is better positioned to succeed.

1 Do more with less: Identity-driven cost reduction

Companies are always looking to lower their operational costs, and one key way to accomplish this is by making teams, processes, and tools more efficient so that they can focus on their core competencies. By adopting cloud technologies, an organization can offload maintenance costs from expensive legacy systems as well as the time spent on addressing system outages. This also sets IT teams up with a regular schedule for updates and maintenance that they can prepare for, without disrupting their day-to-day work.

Implementing a single, cloud-based solution for identity can further reduce IT friction and lower costs. By automating authentication and using single sign-on (SSO), the system would eliminate password reset tickets, increasing the agility of IT teams. Lifecycle management and the use of a centralized directory would automate app provisioning and deprovisioning, granting access from an employee's first day and promptly deactivating an account when they leave the company. A comprehensive identity management solution will also be able to audit an organization's technology landscape, ensuring that there are no security blindspots that could drive up costs and providing insight into performance against security metrics.

When looking for a cost-effective, agile alternative to legacy, on-prem systems, the Federal Communications Commission (FCC) turned to cloud-based identity solutions like SSO, lifecycle management, and multi-factor authentication (MFA). These solutions helped the FCC automate processes, keep their users secure, and cut costs by 83% more than the organization's on-prem infrastructure.



2 Automate and simplify IT: Increase operational performance

Organizations continually strive to focus their teams on doing what they do best, rather than spending time and resources on less valuable tasks. Many of the operational challenges faced by enterprise IT teams, for instance, revolve around manual tasks, such as employee onboarding and offboarding. These can sometimes take weeks to complete, posing challenges for newly hired staff and creating a security risk from users that aren't deprovisioned quickly enough. These tasks can also bog down a team and leave very little time for operational excellence and innovation. Manual tasks

also compromise the efforts of security teams, who need comprehensive insight into who has access to what systems and data. This approach is prone to human error, creating a greater risk of data breaches.

By modernizing their enterprise IT infrastructure, organizations can improve their operational performance across the board. Adopting an identity management platform that streamlines access to information can improve the productivity of your IT team by as much as 83%, while optimizing performance across other teams. When News Corp rolled out SSO and automated their provisioning and deprovisioning processes, the company saved thousands of hours that are now dedicated to more strategic work. On top of saving time, automated and simplified functionalities like single sign-on (SSO) and lifecycle management also reduce the security risks associated with manual password resets, provisioning, and deprovisioning.

3 Fast, effective integrations: Business growth and M&A success

Organizations focused on growing their business—be it by geographic expansion, entering into different industry sectors, or making acquisitions—need supporting strategies that focus on people, funding, infrastructure, and more. This type of growth often manifests in new cloud-based applications that require a heavy investment in terms of regional compliance, provisioning, management, and connecting them to existing on-prem applications. Adding applications also means more credentials for employees and partners to remember, and a higher likelihood of password reset requests for IT.

According to US dealmakers, the most important factor for achieving a successful M&A transaction is effective integration, and adopting modern identity management is key to achieving that. A centralized identity platform will be able to consolidate and standardize user identities from multiple domains, reducing the time needed to collect users in a central directory and increasing IT's agility to provide day-one access to new employees and partners as they're onboarded. In 2015, Allergan merged with Actavis to form a global portfolio of leading medical brands and products. By adopting a centralized directory that integrated data from over 23,000 users across both companies, Allergan had a single source of truth that helped ensure a smooth transition and set the organization up for future success.

4 Going beyond enablement: IT as an innovation driver

As part of delivering future business impact, CIOs have indicated that focusing on digital, data analytics, and emerging technologies is vital. In an age when everyone is looking to be the unicorn of their industry, companies are focused on delivering original concepts. An identity management solution can foster innovation internally by eliminating the need to build a critical authentication and user storage layer, and instead increasing the time employees can spend on designing new products and processes.

Incorporating a modern customer identity and access management (CIAM) solution may allow an organization to focus on product differentiators, building value to customers, and investing time and effort in the things that make customers successful. Adobe experienced these benefits by incorporating a comprehensive authentication layer across Adobe Creative Cloud for enterprise, which led to additional growth in their customer base.

5 Protecting the business: Retaining customers

When designing new products and services, an organization needs to ensure that customers and their sensitive data remain protected. According to Ponemon's Cost of Data Breach Study, data breaches, which increased 75% from 2016–2018, cost organizations an average of $3.86 million. Part of the cost comes from the compromised trust of

existing and future customers, partners, and investors. If customers cannot trust a brand to protect their personal data, they simply won't continue to buy their products or services. The same goes for partners that have to share data and integrate with their services.

While delivering an optimal user experience is top of mind for most companies, it's important to pair this with security and privacy measures that protect user information. According to a recent Forrester study, powerful IAM can result in 46% fewer server and application breaches and 63% fewer cloud infrastructure breaches. As such, IAM can save your company up to 40% on your security spending, leaving further funds available for innovation, business growth, and more.

Identity tools like adaptive MFA add a robust security layer as they assess a user's login environment (e.g. location, network, device) and determine which authentication factors (e.g. security question, SMS, OTP) to use given the potential risk. By adding layers of security that align with a frictionless user experience, companies can foster customer and partner trust in their offerings, thus enhancing retention. 21st Century Fox took this approach when their Global CISO realized that its perimeter-based security was no longer the best way to secure and authenticate access for the company's 30,000 employees and thousands of partners. Now it uses a modern IAM environment to keep users—and their credentials—protected and secure, no matter where they're working.

Putting your security spend in action

By understanding how identity management contributes to an organization's business drivers, CIOs and CISOs can make a strong, reasoned case for security spending, and show the ROI boards and CFOs want to see.

Okta's solutions can offer support as you implement your identity management program, both for your workforce—including employees, partners, contractors—and for your customer-facing solutions. Our Workforce Identity solutions are used to secure and empower this extended workforce through products like Single Sign-On, Adaptive Multi-factor Authentication, and Lifecycle Management, that protect your employee data and support your team in optimizing performance and lowering overall costs. Our suite of Customer Identity products takes the same simple and strong authentication experience and puts it in the hands of developers, who can use Okta to build secure experiences for customers. With our extensive experience in helping our customers meet their business goals, Okta makes it easy to justify your security spend.

Learn which of these is right for you by browsing our solutions, or for a customized business value assessment, talk to our Sales team today.