An Identity-First Strategy for IT Modernization

Datasheet
June 2022

okta

An Identity-First Strategy for IT Modernization

The modernization of IT has become an exercise in doing more with less. IT teams know they need to streamline the technology stack while mitigating security threats.

At the same time, empowering the workforce is one of the most critical functions of modern IT. Employees enjoy seamless digital experiences through their personal apps and now expect the same ease, access, and security from the organizations they work for.

Is there a way to support a best-of-breed ecosystem without complicating access, security, and user management? That's the ultimate question. And identity is the ultimate answer.

Key elements of an identity-centric strategy

- **Facilitate secure, flexible work** for employees by extending access management across both cloud and on-prem applications and integrating tools that enable productivity.
- **Facilitate efficient, scalable operations** by consolidating your view of all users, groups, and devices in the organization, centralizing policy management, and automating redundant processes.
- **Enhance security without compromising employee experience** by providing intelligent access to resources that monitor the context of every login request, ushering in verified traffic and stepping up authentication for suspicious attempts.

The top 3 challenges when modernizing IT

1. Maintaining agility while migrating legacy infrastructure

While moving to the cloud unlocks enormous opportunities, it's not always easy—or possible—to decommission existing on-prem resources. There's a balancing act to building a hybrid cloud environment that serves all the needs of the business and its employees, without creating needless complexity, siloed data stores, or new security vulnerabilities.

2. Facilitating employee productivity in a dynamic work environment

Flexible work environments are expected by today's talent. Providing a fully-equipped office space while supporting remote collaboration is all part of what we call dynamic work, but if it's not effectively managed, shadow IT—technologies used by staff without the approval of the IT team —can rapidly accumulate.

3. Reducing the attack surface without adding user friction

Security has never been more top-of-mind, yet many decision makers lack the resources to address the suite of complex challenges they face. They may maintain a perimeter-focused mindset, trusting a firewall to protect their organization's data—when in fact, users are the new perimeter. Security therefore revolves around identity-based access controls, and activating them in a way that maximizes their impact while minimizing user disruption.

The modernization of IT has become an exercise in doing more with less. IT teams know they need to streamline the technology stack while mitigating security threats. At the same time, empowering the workforce is one of the most critical functions of modern IT. Employees enjoy seamless digital experiences through their personal apps and now expect the same ease, access, and security from the organizations they work for.

Is there a way to support a best-of-breed ecosystem without complicating access, security, and user management? That's the ultimate question. And identity is the ultimate answer.