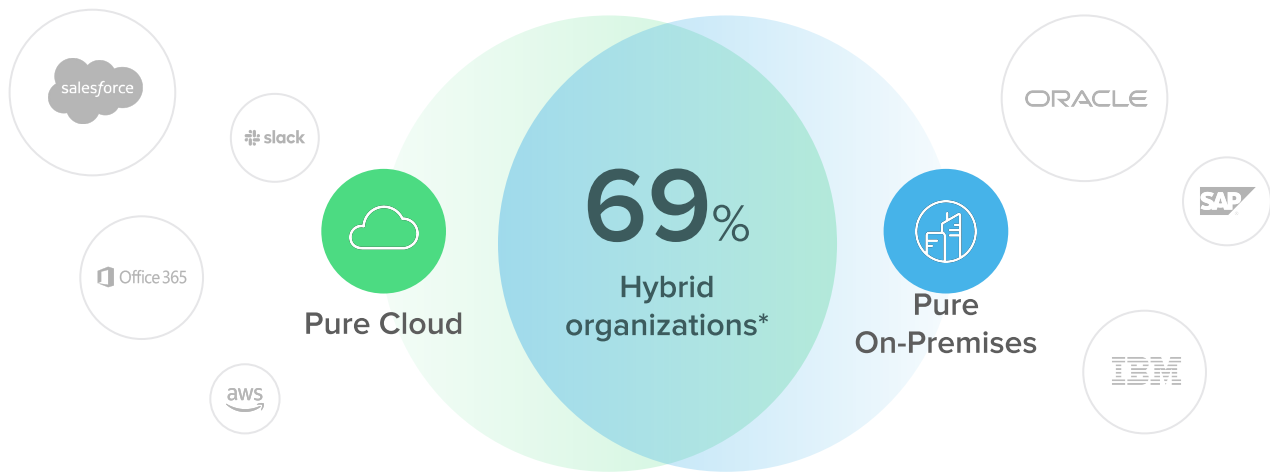




Business Value of Securing Hybrid IT with a Unified Identity

The proliferation of applications like Salesforce, Zoom, and Slack has enabled organizations to better serve their employees and customers while accelerating their cloud adoption. However, many companies adopting the cloud will still keep some of their mission-critical applications hosted on-premises, creating hybrid IT environments that require consistent security, identity, and access control.



*RightScale 2019 State of the Cloud Report <https://info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019>

To address this challenge, organizations traditionally utilize one of two approaches:

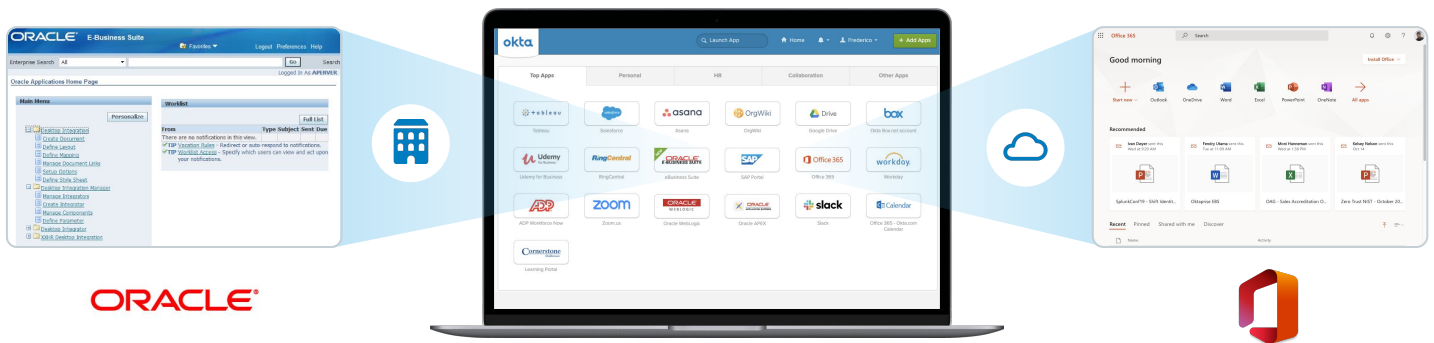
-  **APPROACH 1**
Adopt legacy web access management (WAM) solutions
Many organizations rely on legacy Single Sign-On (SSO) solutions hosted on-premises – also known as Web Access Management (WAM) – that are not built for cloud scale and to deliver unified access across the hybrid IT stack.
-  **APPROACH 2**
Secure on-premises applications individually
Other organizations expend valuable administrative resources to manually manage legacy IT with little to no automation.

However, neither of these approaches is ideal leading IT with a conundrum. Not only do these approaches result in high financial and productivity costs but they're also hamstrung by disjointed end-user experiences where cloud applications have a different login than custom and on-premises applications. This leads to a situation where IT and business leaders feel stuck.

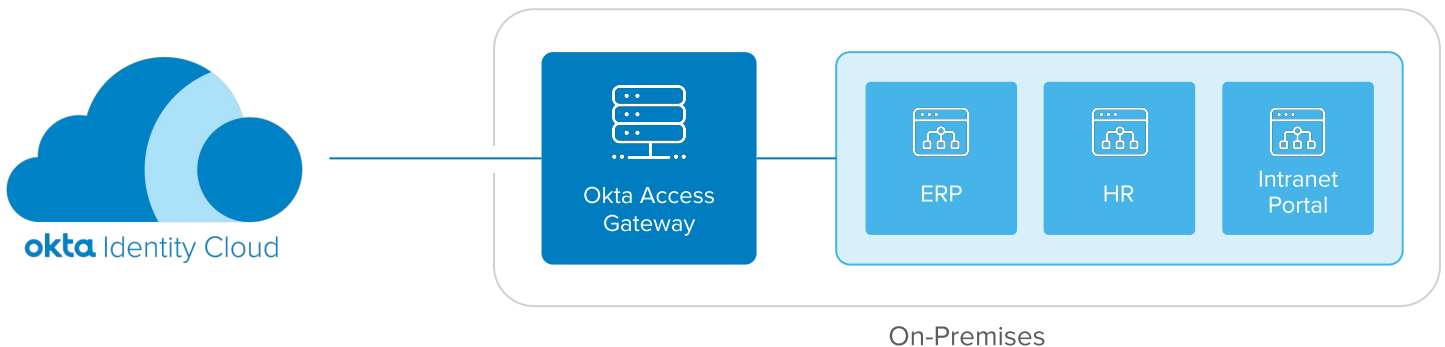
 According to Forrester Research, legacy on-premises IAM solutions typically carry 60% to 80% higher costs of maintenance and development labor.^[3]

Okta Access Gateway Overview

Organizations can use Okta as a single identity provider to maximize the return of investment for securing access to systems both on-premises and in the cloud. Okta enables that by combining the Okta Identity Cloud Single Sign-On (SSO) – to secure cloud applications – with Okta Access Gateway (OAG) – to secure on-premises applications:



Okta Access Gateway delivers the Okta Identity Cloud to on-premises applications without changing how those applications work. Access Gateway acts as a reverse proxy, integrating with Okta as a SAML Service Provider, securing user access to on-premises web applications that do not support cloud Single Sign-On (SSO) and Adaptive Multi-Factor Authentication (MFA) natively.



After authentication, Okta Access Gateway leverages the authentication data from the cloud to validate user access and authorization.

With Okta Access Gateway, users get consistent login and MFA to access applications regardless of their deployment mode: from SaaS, to mobile, custom applications, and on-premises applications. This is not only great for users but enables streamlined management with Okta's IT Admin console wrapping all administration into a single console.

Benefits of Okta Access Gateway and Okta SSO

Modernizing your hybrid IT stack with Okta Access Gateway and Okta SSO delivers benefits across the following value buckets:



**Lower
TCO**



**Improve
Productivity**



**Reduce
IT Effort**



**Enhance
Security**



**Accelerate
Modern IT**



Significantly Lower TCO

The overall cost for Okta is dramatically lower than WAM or manually managing hybrid IT for a variety of reasons. Its reduction in infrastructure footprint and complexity lowers hardware and maintenance costs. Okta's centralized console reduces IT administration friction, boosts efficiencies, and simplifies user access management and SSO policies for all enterprise cloud applications, on-premises web applications, and mobile applications. Unlike the complex and multiple layers of hidden costs with WAM or manual solutions, Okta licensing costs are transparent and predictable with no perpetual hidden costs, making budgeting easier for organizations.

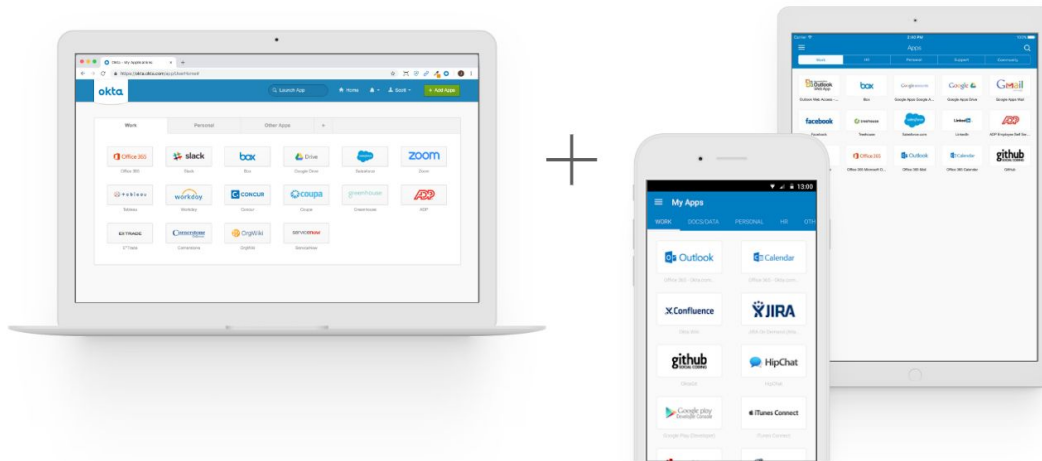
Okta further reduces costs while accelerating application rollouts with over 6,000 pre-configured integrations. This includes native integrations for the most popular cloud applications – from Office 365, to Salesforce, to Slack, to Amazon Web Services – as well as complex on-premises web applications, such as Oracle eBusiness Suite, Peoplesoft, JD Edwards, SharePoint, and Qlik. Okta also provides integration wizards to facilitate connecting to applications that do not have pre-built connectors and on-premises integration patterns to make it easy to integrate with web applications without changing any backend source code.

Okta also takes the worry out of patching and upgrade downtime, while delivering continuous releases and innovation. As a cloud service, Okta transparently manages all patching and upgrade efforts for the cloud components – Okta SSO and MFA – without any impact on a large organization's users. Patching for Okta Access Gateway is fast, seamless, and low cost. Organizations can easily keep their environment secure with proactive security upgrades and standards from Okta.



Improve Productivity with a Seamless, Unified User Experience

Consolidating hybrid IT access control in Okta gives users consistent sign-on experiences to all their applications, whether in the cloud, mobile, or on-premises. Optimizing the end-user experience increases productivity from Day Zero. Okta Access Gateway also increases scalability with rapid and simple service upgrades. This reduces outages that can be frequent occurrences in WAM or manually managed environments.



Reduced IT Effort

Okta Access Gateway increases operational efficiency while reducing strain on the IT organization. With Okta, we estimate on average 80% reduction in IT administration to manage users and policies. This is primarily driven by folding all identity management into a single console, but other areas of improvement include application rollouts. Applications can be configured with the Okta Access Gateway in less than 15 minutes. This is a significant reduction in time vs. legacy solutions, and leads to faster application roll-outs, accelerating end-user access, and improving productivity along the way.



Centralize access management for IT admins

80% reduction in administration efforts



Accelerate secure application roll-outs

15 minutes on average to configure an application



Reduce impact of legacy service interruptions

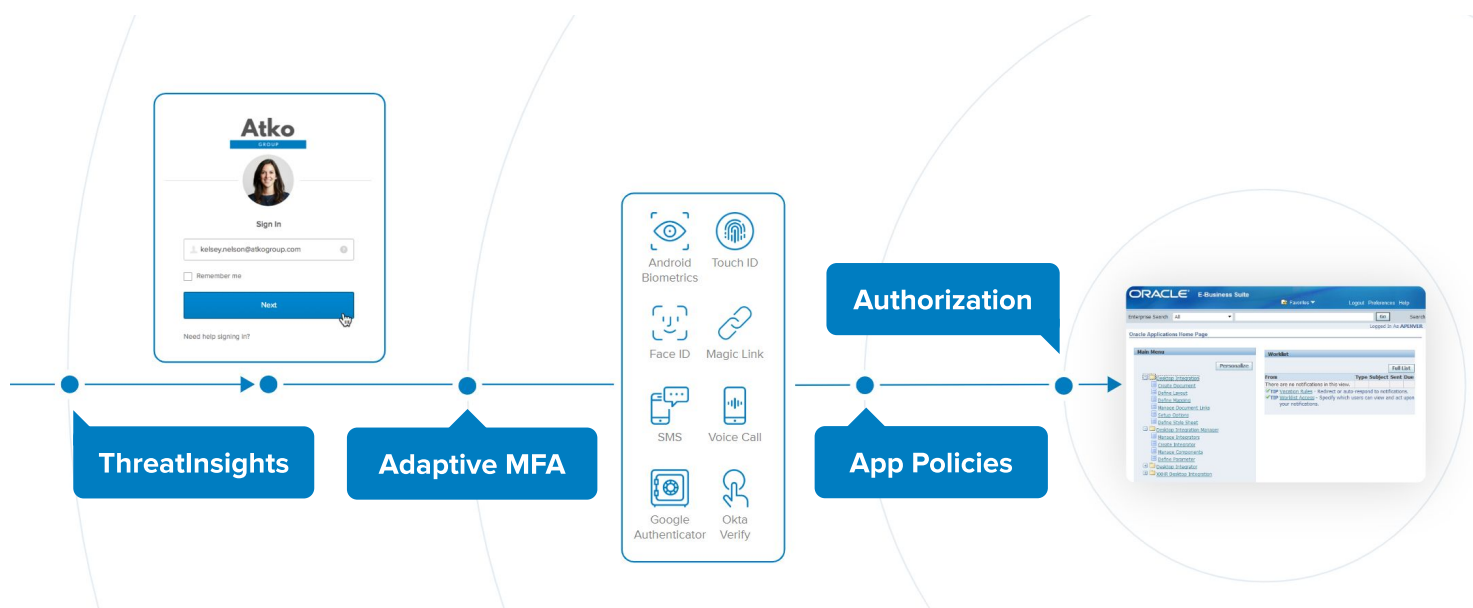
50% improvement in productivity for end-users



Enhanced Security Posture

Okta delivers best-in-class security using ThreatInsights®, Adaptive MFA, and Passwordless access. It enhances enterprise security with robust and unified access management, as well as native support for modern multi-factor authentication (MFA). The ability to view and manage all access management policies from a central administration console gives visibility to enhance an organization's security posture. Okta's build-from-the-ground-up approach simplifies upgrades and patching while strengthening the protection of both cloud and on-premises web applications.

As organizations move toward a Zero Trust posture, adopting modern open standards is crucial to maintain agility from a security perspective. Okta supports open integration patterns (OAuth, OIDC, etc.) that securely connect users to any technology while avoiding vendor-lock. As a result, companies can modernize with agility and reduce dependency on legacy vendors, which can be limiting in what they allow you to implement and provide no viable cloud strategy. For organizations that are manually managing on-premises application access, automating authentication and authorization closes multiple security gaps and applies consistent application security policies across the organization to secure the perimeter.



Accelerate IT modernization

Okta Access Gateway does not change the on-premises application source code, which offers enterprises a clear on-ramp to modernization. Organizations with hybrid IT environments can retire legacy solutions at their own pace. As companies adopt more best-in-breed cloud applications, Okta scales to deliver unified, secure, and modern access experiences across users and devices.

With a modern IT solution, Okta Access Gateway customers are empowered to sunset VPNs, deprecate server infrastructure and increase productivity across the entire enterprise.



Avoid data breaches to sensitive systems on-premises

Average cost of a data breach: \$3.9 M*



Eliminate VPN usage for non-System/Network Admins

Reduce the attack surface while saving on hardware costs



Reduce VPN helpdesk tickets

Save up to \$104 per ticket on IT & Network support costs**



Expand self-service password / MFA recovery to all applications

Reduce helpdesk time, on average 15 minutes per password reset



Unlock mobile workforce productivity

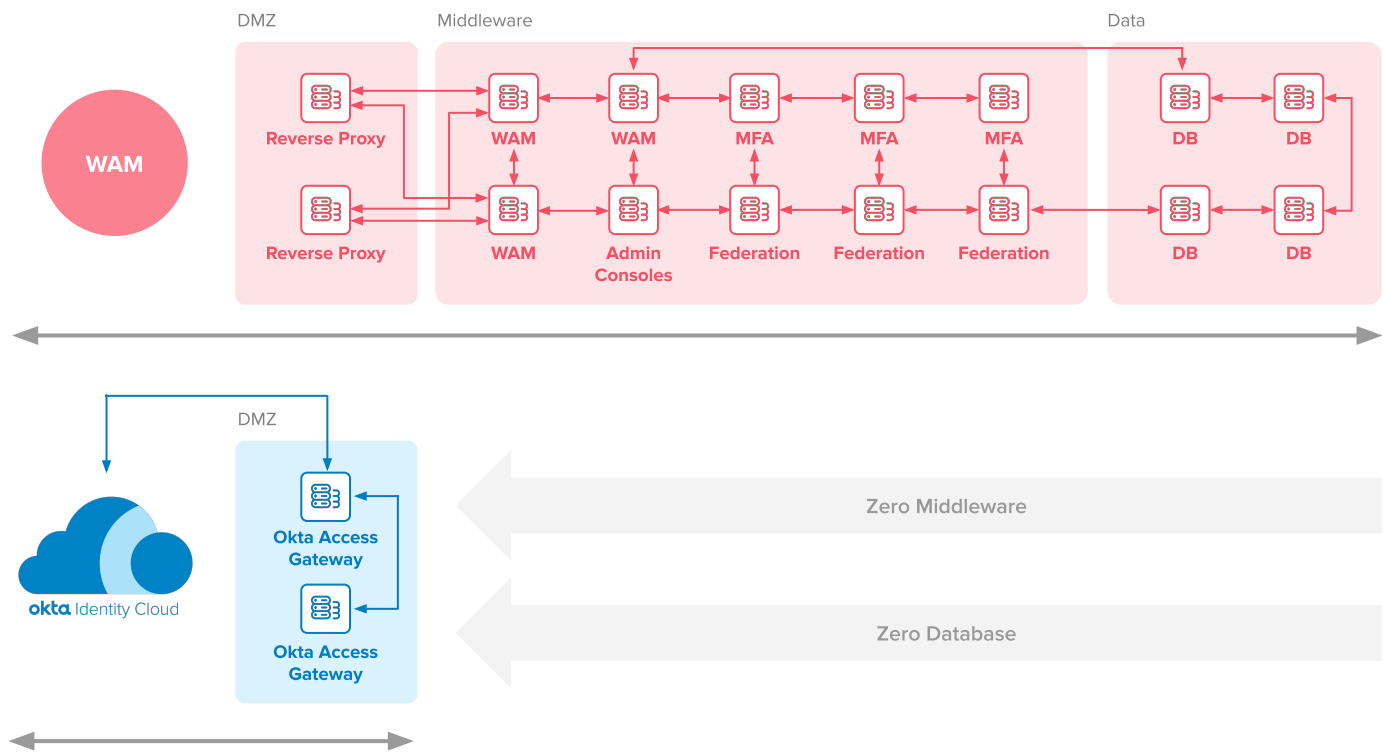
Any device, anywhere access. At a minimum, regain 5 minutes/week/user

Infrastructure requirements

Legacy WAM solutions require a wide array of complex hardware and servers, including databases and middleware services to support SSO, enforce policies, store credentials, and more. In addition, these deployments often require expensive subscriptions to third party software that needs to be installed, maintained and patched on a regular basis on top of the underlying hardware.

WAM hardware requirements vary based on the number of infrastructure environments (i.e. QA, production, etc.), types of on-premises web applications being protected, and the number of users accessing each web application. Typically, legacy WAM requires at least 15 servers. That number can quickly double or increase even more in organizations that demand robust features like development and test environments, and global deployments and those that understand the importance of having an always-on, reliable service with high availability, load balancing, and disaster recovery.

In contrast, Okta Access Gateway requires minimal infrastructure to protect on-premises web applications by collapsing the environment with fewer servers, consistent policies and a single identity provider for all users and assets. Combined with Okta SSO for cloud applications, the need for multiple servers and multi-tier infrastructure is reduced by up to 90%.

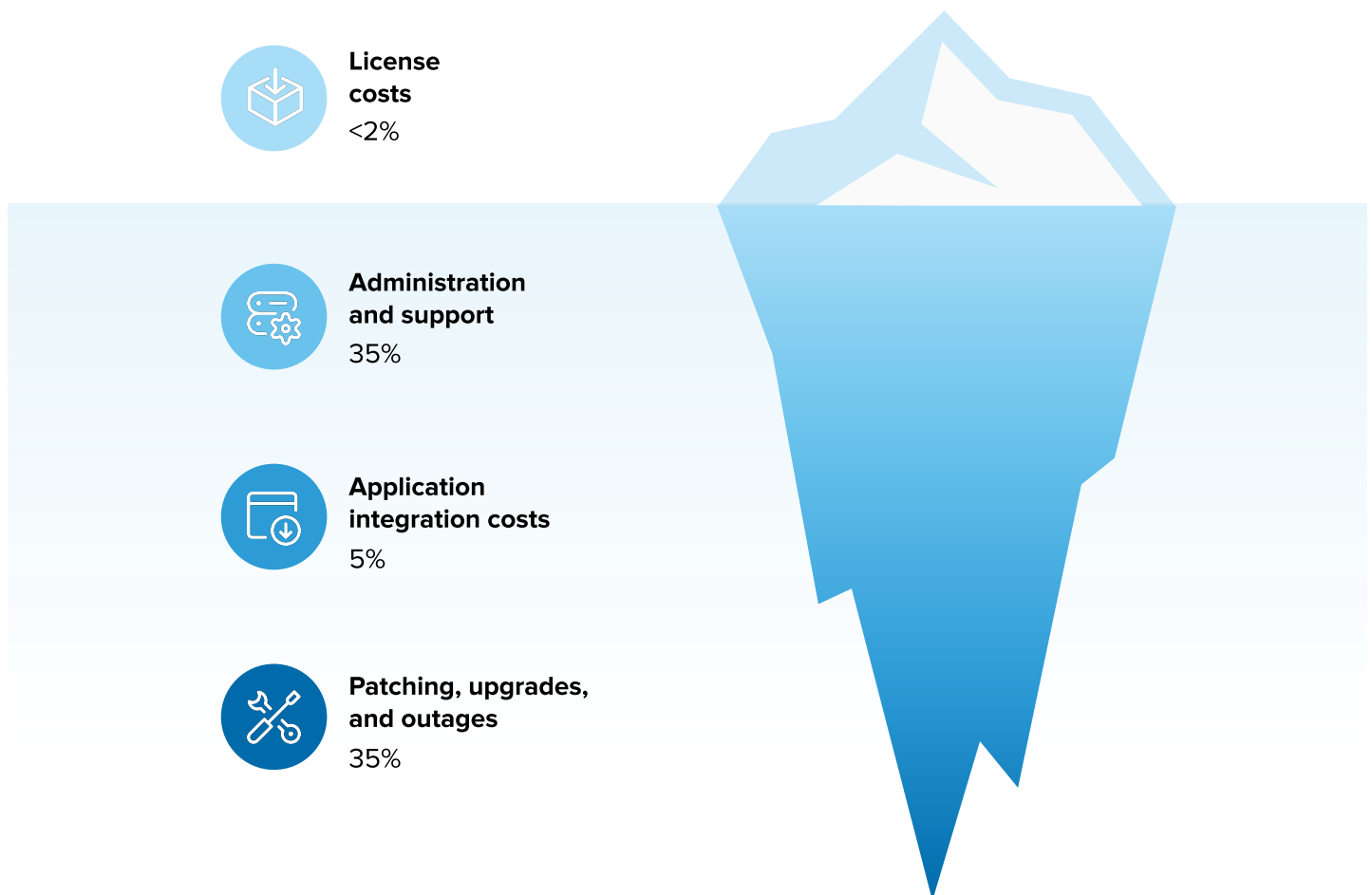


Full Migration to Modern IT

Now that we've covered benefits, how do we fully migrate to a modern IT infrastructure for a hybrid IT environment.

When evaluating the right identity management solution, organizations must assess the full costs to purchase, deploy and maintain the technology over its lifecycle, a calculation typically captured by total cost of ownership (TCO). For many on-premises identity management services, the TCO often goes beyond the upfront licensing costs. For example, licensing costs for legacy WAM solutions typically represents less than five percent of the TCO. In addition to licensing recurring costs for legacy WAM place significant expenses and efforts on businesses, especially as continuous patching, upgrades, and innovation are required over time. These additional costs typically fall into four main categories:

WAM TCO



Let's dive deeper into each of the above cost categories for legacy WAM solutions.



Another major cost category organizations often overlook are in administration and support. This category is broken into three cost areas:



Vendor support fees

On WAM solutions, vendor support fees are anywhere from 20% of the initial license cost and only go up. Additionally, these perpetual fees don't change based on your actual usage. So even if on-premises web applications usage drops due to reasons including modernization efforts, the support fee is owed in perpetuity.



IT Operations

Operational costs on WAM solutions are associated with the number of full-time employees (FTEs) required to maintain the solution up and running securely. Organizations typically hire two to three full-time specialists or more depending on the deployment complexity and the variety of skills required for maintaining the WAM database, middleware, network, and supporting servers. Due to the WAM complexity, infrastructure specialists are in short supply and demand high compensation rates. For service operations, this often raises questions, "Should we employ and train our IT staff to maintain and patch proprietary WAM servers? Or should we instead enable our high-paid resources in new skills, such as enabling access to the cloud, adopting modern standards, and supporting our Hybrid IT at scale?"



Helpdesk Support

Helpdesk operations are yet another significant cost area related to WAM maintenance. WAM solutions lack seamless self-service user interfaces and mobile access natively available in modern access management solutions. The increase in helpdesk tickets that result from poor user interfaces quickly add up, becoming increasingly costly for organizations.

Okta Access Gateway minimizes total helpdesk calls and users' frustrations for password resets by granting quick and seamless access to business-critical applications.



50% of all IT help desk costs are for password resets^[1] and each call costs a company up to \$70.^[2]



WAM solutions don't offer preconfigured integrations for the most of the applications they protect. As a result, enterprises must invest heavily in consulting services, developers, or IT specialists to manually integrate applications with their WAM infrastructure. As organizations continue to adopt more cloud applications—leveraging out-of-the-box integrations is table stakes. Unfortunately, integrating WAM and cloud solutions is expensive and difficult due to the lack of preconfigured app catalogs and integration wizards.

These WAM capability gaps can add days to weeks of integration efforts and costs, requiring organizations to engage with SaaS and SAML integration specialists. Due to the legacy and proprietary nature of WAM solutions, the integration costs and challenges are expanded to any modern resource: from SaaS, to mobile, to modern custom applications.

To avoid integration challenges, some enterprises invest in multiple access management providers to manage SSO for cloud, mobile SSO, and on-premises SSO, and Multi-Factor Authentication (MFA) creating identity siloes. This redundant approach increases operational costs and burdens, increases the threat surface, and frustrates users with inconsistent experiences.

Using Access Gateway with Okta SSO to consolidate access for all applications removes the identity silos, enhances operational efficiency, and creates a consistent experience for all end-users.



WAM solutions lack preconfigured integrations, resulting in additional time and costs to secure new applications

Oracle E-Business Suite

Microsoft Office 365

With Okta, users can access on-premises and cloud applications from the same place



Legacy WAM solutions require continuous maintenance, testing, and patching for every single component across multiple servers and environments. These activities can take several weeks of planning and execution. Most organizations will carry four or more patches in a year, exhausting key resources. Patching also requires taking systems offline. In today's always-on business environment, outages can cause massive work disruptions and revenue losses even if they are after hours or on weekends. To avoid such outages, organizations may delay or skip patches, an unwise but common misstep increasing their security risk.

WAM vendors recommend system-wide upgrades every two to three years. These upgrades are extremely costly and can take several months to over a year to fully deploy. They also often need consultants or professional services, adding to in-house developer and IT admin efforts for internal implementation and testing. Consequently, these upgrades can easily add up to a multiple of the initial WAM license and implementation costs on a recurring basis, comprising over 30% of the TCO for WAM.

To learn more about how migrating from WAM to Okta Access Gateway can lower your total cost of ownership, increase operational efficiency, enhance security postures, and accelerate IT modernization creating friendly end-user experiences, visit www.okta.com/products/access-gateway.

[1] Gartner Group

<https://www.okta.com/blog/2019/08/how-much-are-password-resets-costing-your-company/>

[2] Forrester Research

<https://www.linkedin.com/pulse/does-password-reset-service-desk-cost-us-money-yes-wake-vijay-shankar/>

[3] Forrester Report August 2018: Making the Business Case for Identity & Access Management.

<https://www.okta.com/resources/analyst-research-forrester-report-august-2018-making-the-business-case-for-identity-access-management/thankyou/>

Sources:

* Costs of a data breach in 2020: Ponemon/IBM

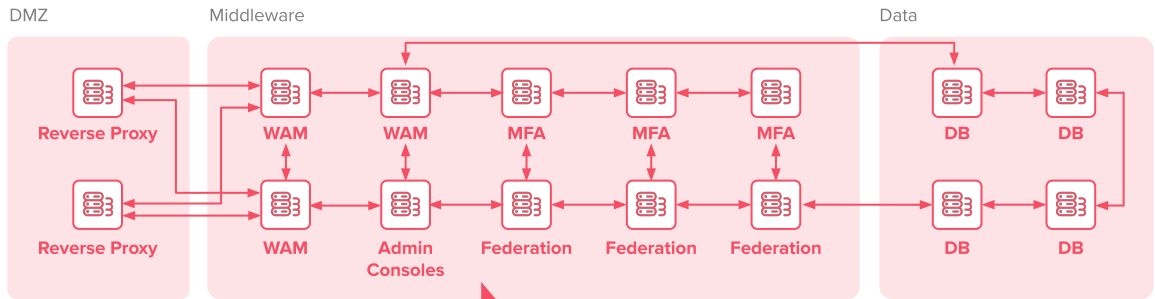
<https://www.ibm.com/security/data-breach>

** Metric of the Month: Percent Resolved Level 1: HDI

<https://www.thinkhdi.com/library/supportworld/2018/metric-of-month-percent-resolved-level-1-capable.aspx>

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 applications, the Okta Identity Cloud enables simple and secure access from any device. Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe 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.



WAM requires continuous patching and upgrades on every server and component