Image credit: Zbynek Jirousek / Shutterstock Inc.

What 100% Cloud and Mobile Really Means

The 7 pillars of a cloud- and mobile-first strategy

okta

Introduction

Today's workplace is flexible, collaborative, and dynamic –allowing anyone to work anywhere, any time. Employees are working remotely on their own devices, often on insecure networks, accessing sensitive data through new and potentially unsanctioned applications. And an organization’s workforce now extends outside the company to contractors and partners, too.

These are just some of the challenges facing modern organizations as they scale for success in a quickly changing global economy.

A 100% cloud and mobile strategy allows companies to remain competitive and empowers greater productivity amongst their internal and external teams–all while decreasing costs and increasing security. Those attributes, in turn, extend to better customer service and experience.

An effective cloud-first approach shifts the IT team’s role from software installation, server set-up, and patching–mundane, back-office tasks–to strategic advisors and business enablers driving the company’s success.

Forward-thinking IT leaders know this, and we’re seeing more and more organizations adopt this mindset. But what does a 100% cloud and mobile organization really look like? It begins with a philosophy–a shift in the way IT teams think about openness, security, and employee trust–focused around seven core pillars.

Seven pillars of a 100% cloud and mobile organization

These seven pillars are the core attributes of being cloud- and mobile-first. They serve as vital, interlinking nodes that alone promote efficiency and progress, and together produce cloud-first transformation.

1. SaaS

Okta's 2018 Businesses @ Work Report[1] shows that organizations are investing more heavily in SaaS apps than ever before—in all regions and industries, and in companies of all sizes. From 2015-2017, the median number of apps per Okta customer grew 24%.

Instead of running apps themselves, IT teams in 100% cloud and mobile organizations offload that responsibility to best-of-breed cloud apps, such as Box, Office 365, and Slack. Cloud apps have inherently higher availability, better user experiences, are cheaper to maintain, and offer greater flexibility. Companies running legacy software can now comfortably move to the cloud, adopting newer protocols like SAML 2.0 or OpenID Connect in the process.

SaaS is also more secure than on-premises infrastructure. According to Alert Logic's 2017 Cloud Security Report[2], on-prem environments experience 51% more security incidents than their cloud-based counterparts. And, with cloud identity providers offering built-in SaaS integrations (with thousands of options), companies can securely connect their teams to the tools they need in minutes.

The fear of transitioning from legacy apps to cloud apps is unfounded. Cloud-first organizations leverage their access to vast libraries of SaaS applications for dynamic and scalable choice.

2. Distributed IT

Because SaaS apps have such an easy deployment model, the discovery and adoption of new apps in a cloud- and mobile-first organization is shared across the IT team and the departments who use them. This frees IT from acting as the gatekeeper of app adoption and empowers BUs to find and use the tools that make them most effective in the shortest time frame.

IT remains in an advisory role to ensure security standards, but each department can efficiently deploy the suite of SaaS tools it needs.

[1] 2018 Businesses @ Work Report, https://www.okta.com/businesses-at-work/2018-01/
[2] Alert Logic 2017 Cloud Security Report, https://www.alertlogic.com/resources/cloud-security-report-2017/

3. Distributed workforce

According to IDC's CloudView Survey[3], 40% of today's companies want to transition to a cloud-first strategy within the next 12 months because it affords them greater flexibility.

When companies are 100% cloud and mobile, they break down traditional office walls. They're agnostic to where their employees work. IT provides the right tools to the right people and access at the right time–even if it's beyond the firewall.

This also facilitates more productivity with outside contractors and global partners, particularly ones who require access to sensitive internal applications from unknown devices and insecure networks. A cloud- and mobile-first strategy gives all users secure access to internal resources without needing to jump through cumbersome hoops like firewalls and VPNs.

4. Security focused on apps & data

Companies are concerned with how their security measures up, and legacy infrastructure is vulnerable to increasingly sophisticated attacks. The firewall has been a traditional security mainstay to safeguard networks and infrastructure–and yet, for all their merits, even the strongest firewalls have been unreliable in securing sensitive data. Moreover, locking down devices and the network is heavy-handed and difficult to manage, especially if many of your users are outside the network.

A 100% cloud and mobile approach places security directly on the apps and devices through strong identity and access management processes. Multi-factor authentication (MFA) plays a huge role in securing apps and data. According to Verizon's Data Breach Investigation Report[4], 81% of data breaches involved weak or compromised credentials. MFA acts as the gate before the front door, increasing security by requiring additional factors–such as SMS, push notifications, or email–from a user before he or she logs in. By layering on an adaptive policy that takes into account access attributes like device type, IP address, and user privileges, IT can ensure an even higher level of security that wasn't possible before.

5. A mixed Mac and PC environment

In modern organizations, employees are able to access apps and data using the devices and operating systems they choose. But that freedom presents unique challenges. For example, Mac OS devices have become favored among employees, but have never played well with Microsoft AD.

When everything was behind a firewall, end points were seen as the weakest link and had to be locked down. A 100% cloud and mobile organization focuses on identity and authentication instead, which enables access to apps from any endpoint.

It no longer matters, then, if an employee is using a Mac or a Windows device. They have the freedom to work on the devices that make them feel their most comfortable and productive. In fact, many cloud- and mobile-first organizations now start entirely on Mac devices.

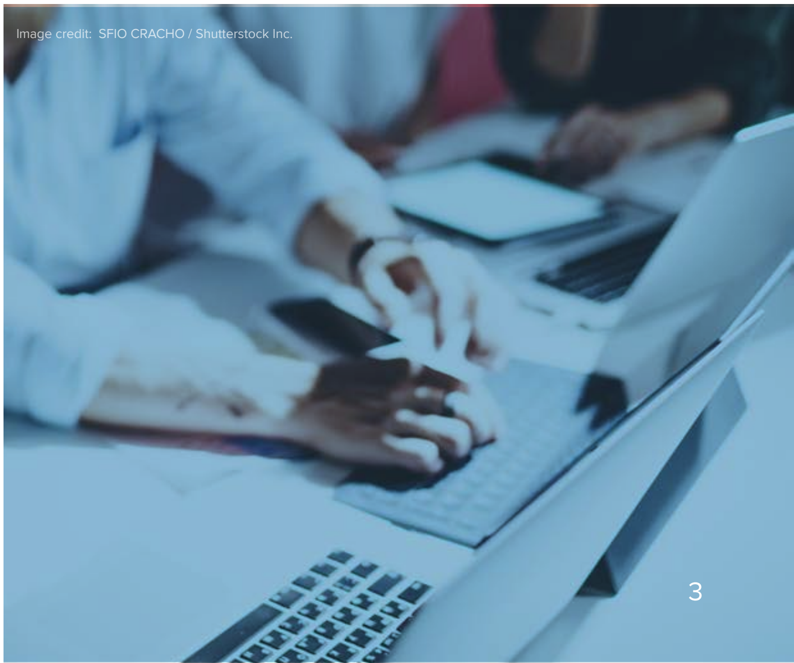


Image credit: SFIO CRACHO / Shutterstock Inc.

[3] IDC 2017 CloudView Survey, https://www.idc.com/
[4] Verizon's 2017 Data Breach Investigations Report, http://www.verizonenterprise.com/

Image credit: Ditty_about_summer / Shutterstock Inc.

6. BYOD

Modern businesses understand the importance of flexible BYOD policies, which improve productivity and increase collaboration among employees. Yet despite this, many organizations state security as a top concern and remain shy to adopt BYOD policies. A 100% cloud and mobile organization focuses on protecting access to apps through identity and authentication rather than the device. When IT teams have visibility into who has access to what data, and with the added security of MFA across all devices, companies can empower their teams to work on any device they choose.

This pillar is instrumental in orchestrating effective workflows with contractors and partners who most likely have their own devices. Cloud- and mobile-first organizations trust the end-user to work on their own personal device without compromising company security.

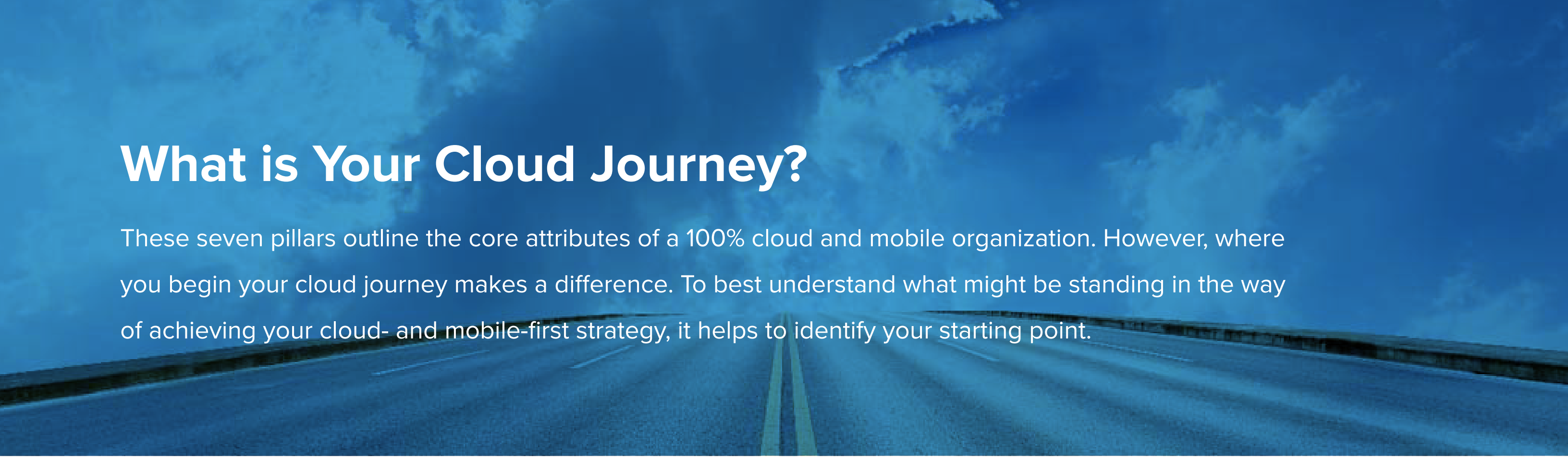
7. Automation focus

As the number of users, apps, and devices increase, IT organizations need to streamline workflows for greater efficiency. Manually provisioning every employee, contractor, and partner is unsustainable; the costs (and risks of errors) are simply too high.

Instead, pre-integrated applications, automated group licenses, and flexible delivery options modernize legacy Active Directory systems and allow once-manual processes to scale. This ensures employees, contractors and partners have the correct level of access to the data and tools they need.

Likewise, access should come to an end when their engagement does. In cloud- and mobile-first IT organizations, automation allows on- and offboarding processes to take place smoothly through centrally managed policies that meet security and compliance requirements. Automation also prevents IT from being a bottleneck through the provisioning process.

Once an employee's identity is established with automated lifecycle management, it is easy to update or tweak access either individually or across wider groups, regions, roles, or territories. Through lifecycle management, businesses can embrace flexible scalability, dynamic responsiveness, and a pay-as-you-grow model where costs are more granularly linked to measurable usage.



What is Your Cloud Journey?

These seven pillars outline the core attributes of a 100% cloud and mobile organization. However, where you begin your cloud journey makes a difference. To best understand what might be standing in the way of achieving your cloud- and mobile-first strategy, it helps to identify your starting point.

Cloud Native

A cloud native organization was born in the cloud with no on-premises infrastructure. Its main challenge is quickly scaling its IT infrastructure to keep up with a rapidly expanding and distributed organization. These organizations want to prevent the redundancy of apps, shine a light on shadow IT, and automate manual processes.

Is this your organization?
Download our Cloud Native Checklist for tips to scale in the cloud.

Cloud Aggressive

A cloud aggressive organization has on-premises infrastructure traditionally rooted in AD or LDAP. These organizations are committed to moving to the cloud to increase IT agility to meet new business needs. Challenges include a need to modernize workflows with SaaS apps and the improvement of their security stance.

Sound like your organization?
Download our Cloud Aggressive Checklist for steps to more quickly migrate to the cloud.

To learn how Okta can help you on your 100% Cloud and Mobile journey:

- **Visit our website**
- **Contact us to speak with a representative.**

About Okta

Okta is the leading independent 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 over 5,000 integrations, 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 revenu,e 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.