okta

Simpler, Smarter Authentication with Okta

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

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

Contents

2014: The Year of the Security Breach

2014 was a banner year for security breaches. According to the Identity and Theft Research Center, there were 783 reported US data breaches this past year, a 27.5% increase from 2013. Hacking was the number one cause of a breach, accounting for 29% of incidents.[1] On average, it took a company 205 days to detect a breach even existed.[2] Sony, Target, Home Depot, JP Morgan Chase and Anthem were amongst the many high profile victims of 2014. These breaches had profound (and lasting) financial and reputational effects. eBay, for example, was greatly impacted by its 2014 breach in which consumer passwords, names, birth dates, addresses and emails were revealed. Not only did eBay pay damages for this breach, but the company's balance sheet was also impacted, as consumers were hesitant to make marketplace purchases after the breach occurred. By July 2014, 85% of eBay consumers had reset their passwords, but account activity levels hadn't returned.[3]

Security is C-Level Issue

Security breaches are no longer "just ITs problem"; they've become a top concern for c-level executives. In a recent CIO survey conducted by Piper Jaffrey, security was listed as the number one area of increased investment in 2015. 75% of CIO's indicated they plan to increase security spending this year, compared to 59% in 2014.[4]

Yahoo Security Chief, Alex Stamos, suggests how both enterprise CIO's and CMOS's might think about security investments. He encourages CIO's to focus on "attack surface minimization", or finding the least expensive and easiest way to reduce their risk. Enterprises can begin by imagining what their business looks like from the outside to an attacker and addressing those vulnerabilities. Stamos also recommends that, for all functions where a business isn't running its own software, they should move to the cloud. CMO's, who are chiefly concerned with brand image and reputation, should invest in proactively talking about security (before there is any reason to).[5]

1 http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

2 http://www.itsecurityguru.org/tag/breach/

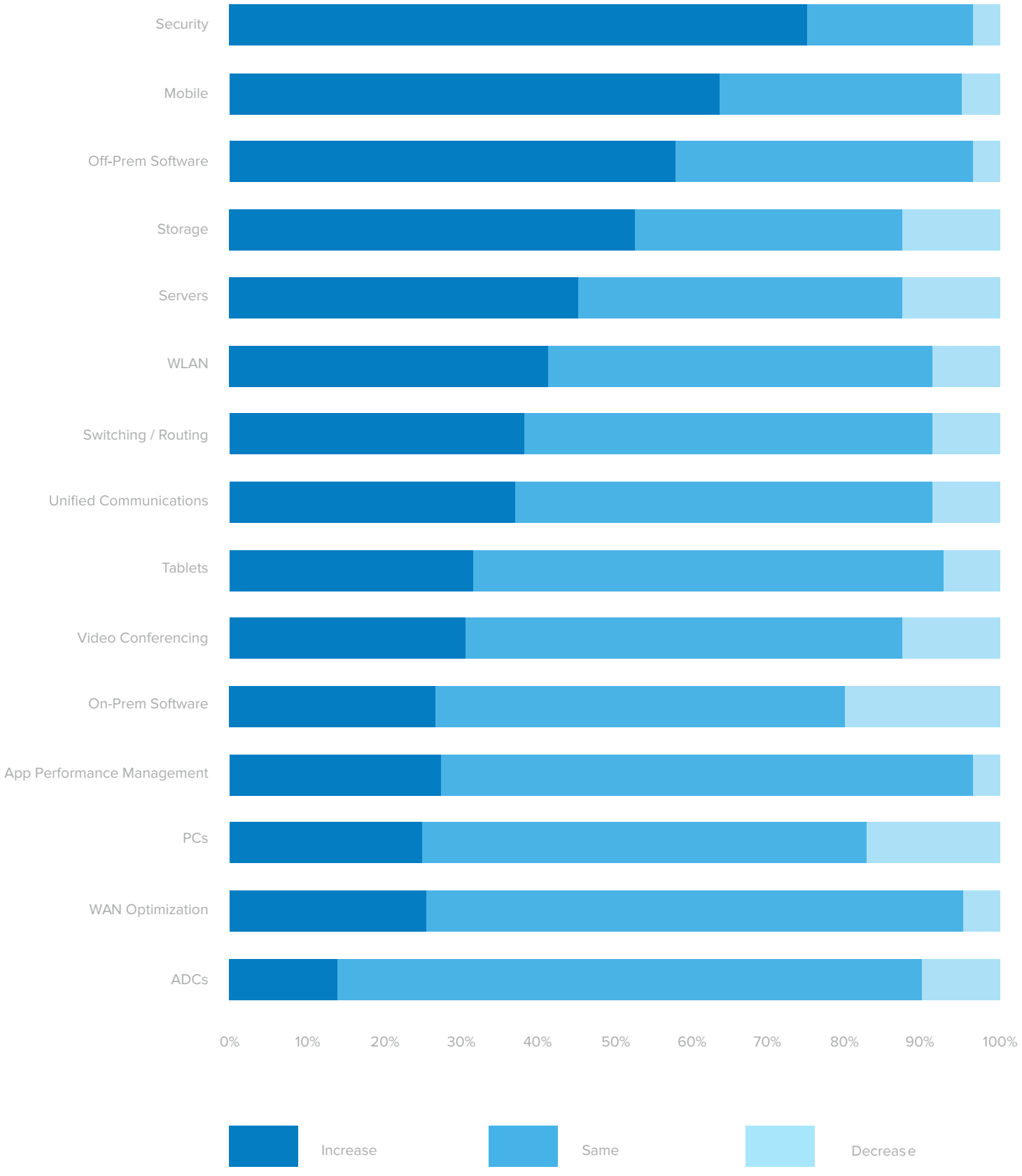
3 http://www.scmagazineuk.com/ebay-counts-the-cost-after-challenging-data-breach/article/361338/

4 Piper Jaffray 2015 CIO Survey, January 6, 2015.

5 Podcast: http://a16z.com/2014/12/03/a16z-podcast-securitys-wakeup-call/ December 3, 2014.

Which Technologies Will You Increase / Decrease Spending On In 2015?

Securitiy the top spending priority for 2015; 75% of CIOs expect to increase spending on Security.



Employee Mobility is Changing the Game

Employee mobility needs have changed, and businesses are increasingly challenged to meet those needs. Users are demanding increased flexibility with respect to when, where and how they access corporate information. This is forcing enterprises to re-evaluate bring your own device (BYOD) policies and the notion that you can only access corporate data behind the firewall. "By 2017, Gartner [estimates] that 90% of all organizations will support some aspect of BYOD."[6] And, according to Forrester, "nearly 60% of enterprises are re-architecting traditional or back-end applications to interface with mobile front-end apps."[7]

The Status Quo Isn't Good Enough

Typically, web applications are protected with single-factor authentication: a user name and password. These credentials, in addition to being difficult to manage, leave sensitive data and applications vulnerable to a variety of common attacks. Attackers are using increasingly prevalent and sophisticated techniques to steal passwords to consumer, banking, and enterprise applications.

Some security breaches are complex and sophisticated attacks that would be very difficult to prevent. But in many cases, instituting some basic security measures can go a long way. In the case of Anthem, for example, assailants stole personal records from Anthem's databases using compromised administrator credentials. With multi-factor authentication in place, requiring an additional piece of information beyond just a user name and password for access, these attackers may not have been successful. The Anthem breach affected up to 78.8 million people to-date, including anywhere from 8.8 to 18.8 million non-Anthem customers.8

Multi-factor authentication (MFA) is designed to protect against the range of attacks that rely on stealing user credentials. Organizations can use a variety of techniques, but all work by requiring the user to provide something in addition to their primary password— something the user is, has, or knows—before they can be authenticated to the protected service. With MFA in place, even if a user's password is stolen, his account is safe from unauthorized access.

But MFA has its challenges. First, MFA can be disruptive to end-users in a variety of ways. Hard tokens are a burden for end-users to carry, and soft token require them to type in a code from their phone. For businesses with strict MFA policies, end-users have to re-authenticate frequently throughout the day. A successful MFA product should prompt only when necessary; when additional verification is required, the verification process should be easy. MFA can also be hard for IT teams to implement because they have to integrate individually with each application or system, so establishing a universal standard is difficult. An effective MFA solution should integrate with everything, and should be deployable across an assortment of resources quickly and easily.

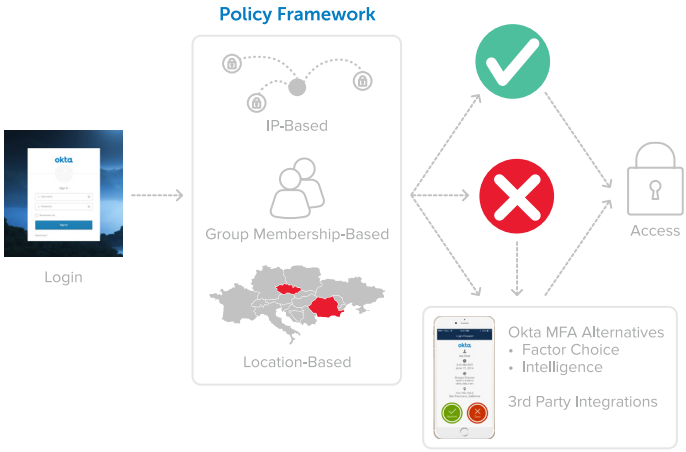
6 http://www.gartner.com/newsroom/id/2909217

7 Forrester: Latest IT Trends For Secure Mobile Collaboration

8 http://www.reuters.com/article/2015/02/24/us-anthem-cybersecurity-idUSKBN0LS2CS20150224

Okta's Solution for MFA

Okta is an integrated identity management and mobility management service that securely and simply connects people to their applications from any device, anywhere, at anytime. Okta offers a comprehensive MFA solution—running entirely in the cloud—that keeps users safe without getting in their way. Okta provides its own MFA mobile app, Okta Verify, which allows users to authenticate using several convenient methods. Okta has also integrated with all major MFA providers; if you have an existing MFA solution, it can serve as your second factor.



Seamless Verification for the End-User

Many well-intentioned security professionals roll out MFA to end-users, but fail to increase enterprise security. If MFA is cumbersome to end-users, they will either find ways around it or elect not to work while away from their desks. But it doesn't have to be that way. With Okta, MFA is an extension to its core identity service. Okta not only provides the mechanism for additional verification, it also controls when and why users are asked to verify. So Okta MFA has the ability to combine information about a specific application with identity data and environmental context to make an intelligent determination of risk. Users must provide verification only when a particular access request is deemed high risk. Okta puts second factors where and when they are needed, so that end users are not prompted too frequently.

Best-in-Class Factor Support

Okta Verify with Push allows end users to provide second-factor authentication with a tap of their phone instead of transcribing rotating codes. Okta also supports multiple other options for authentication: security questions, Okta Verify OTP, SMS, and integration with 3rd party MFA providers. This broad support allows Okta to support a wide range of use cases. See below for more about our factor support.

Security Question		Okta MFA provides an in-browser second factor by allowing an authenticated user to answer a security question. This allows you to support users who can't be expected to use a phone as a second factor.
SMS Verification		For those users who need something stronger than a security question but don't have a smartphone, Okta's MFA also offers a text message option which will delivers an OTP code via text message to any SMS-enabled phone. Like the other MFA options, it is built into the service; no additional third party services are required—it just works.
Okta Verify		Okta Verify is a mobile app that generates authentication codes on a rotating basis, which users can use to provide secondary verification in Okta. Because the apps are pre-registered with the Okta service, the attacker would have to possess the user's phone to know the code. This method does not require a text plan or a connection to the Internet.
Okta Verify with Push		Okta Verify with Push is the easiest way to provide second-factor authentication. Okta will send a notification to a user's smart phone or tablet, and a single tap will provide the proof of ownership that Okta needs to allow or deny access to an application. If a user receives an authentication request that they don't expect, they can simply deny it and prevent any invalid access.

Built and Run in the Cloud

Okta is an enterprise-grade identity and mobility management service, built from the ground up in the cloud. With Okta, MFA is not installed, configured, and maintained on premises across one or more servers and software components; it's a zero-downtime service with a 99.9% uptime guarantee that can be consumed on-demand. When major multi-national corporations choose Okta to be their MFA provider, they get a veteran team that they trust. This helps organizations get off the ground quickly and stay up and running consistently.

Extend Protection to the Most Critical Components

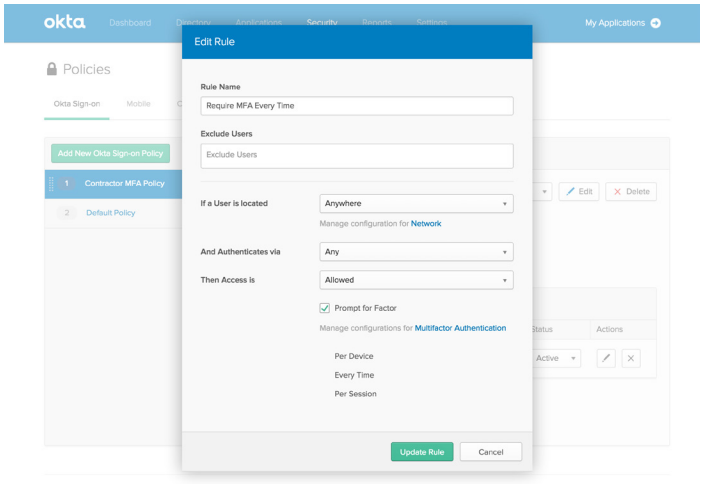
Okta's RADIUS agent allows organizations to integrate Okta with any RADIUS-enabled device that uses the PAP protocol, including VPNs, servers, and other network hardware. Some of these components are the most critical to protect. As such, Okta embedded its MFA solution into the authentication flow—even on the command line. Privileged and unprivileged users can authenticate to protected infrastructure components using a username/password, plus any configured MFA factor for extra security.

Embeddable MFA with RESTful APIs

MFA has traditionally been difficult for companies trying to build their own software products, such as Independent Software Vendors (ISVs). Okta's MFA service provides a RESTful API layer that facilitates enrollment, revocation, and authentication, allowing developers to add strong authentication into custom applications of all types. The APIs also allow business to fully brand the MFA experience so they gain the benefit of Okta's MFA while preserving their own look and feel.

Security through Intelligence

Okta knows that user adoption is critical to the success of any IT initiative, so balancing security with a non-disruptive user experience is critical. Okta employs authentication intelligently by assessing the risk associated with an authentication event and prompting only when needed. Okta allows admins to configure policies to prompt users based on authentication metadata, including: IP address, location, device, application, group membership and more. This capability can flexibly enforce MFA for authentication requests that deviate from expected patterns, so we can deny malicious requests and permit legitimate ones.



Okta's Policy Engine allows admins to configure granular access control to integrated applications

End-to-End Solution

MFA is only effective if it's a universal standard in your organization. If there's an unprotected server or application, attackers will exploit it. Okta integrates with all of an enterprise's most important applications and resources with its comprehensive application network. Okta is the first place end-users login every morning; it serves as the portal to most of the services users consume. This central positioning uniquely equips Okta to enforce MFA across your entire organization, wherever it's needed. Instead of implementing a second-factor into each individual resource, simply extend Okta to enforce this protection.

The importance of a comprehensive, end-to-end solution was highlighted in the JP Morgan breach this past year. While JP Morgan had 2-factor authentication in place, the bank's security team "had neglected to upgrade one of its network servers with the dual password scheme, [leaving] them vulnerable to intrusion. Once inside, hackers managed to gain high level access to more than 90 bank servers."[9] If JP Morgan had a fully integrated MFA and identity management solution in place, they would have been able to ensure MFA was appropriately applied across each system. Because they didn't, over 83 million households and small businesses were compromised.

Summary

In today's world, security cannot be ignored. All enterprises need to think about strengthening authentication, and multi-factor authentication is the best way to do that. But, not just any solution will suffice. A managed solution that is both easy to administer and low-friction for end-users will ensure that MFA is successful in the enterprise.

9 http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/?_r=1

About Okta

Okta is the foundation for secure connections between people and technology. By harnessing the power of the cloud, Okta allows people to access applications on any device at any time, while still enforcing strong security policies. It integrates directly with an organization's existing directories and identity systems, as well as 4,000+ applications. Because Okta runs on an integrated platform, organizations can implement the service quickly at large scale and low total cost. More than 2,500 customers, including Adobe, Allergan, Chiquita, LinkedIn, MGM Resorts International and Western Union, trust Okta to help their organizations work faster, boost revenue and stay secure.

For more information, visit us at www.okta.com or follow us on www.okta.com/blog.