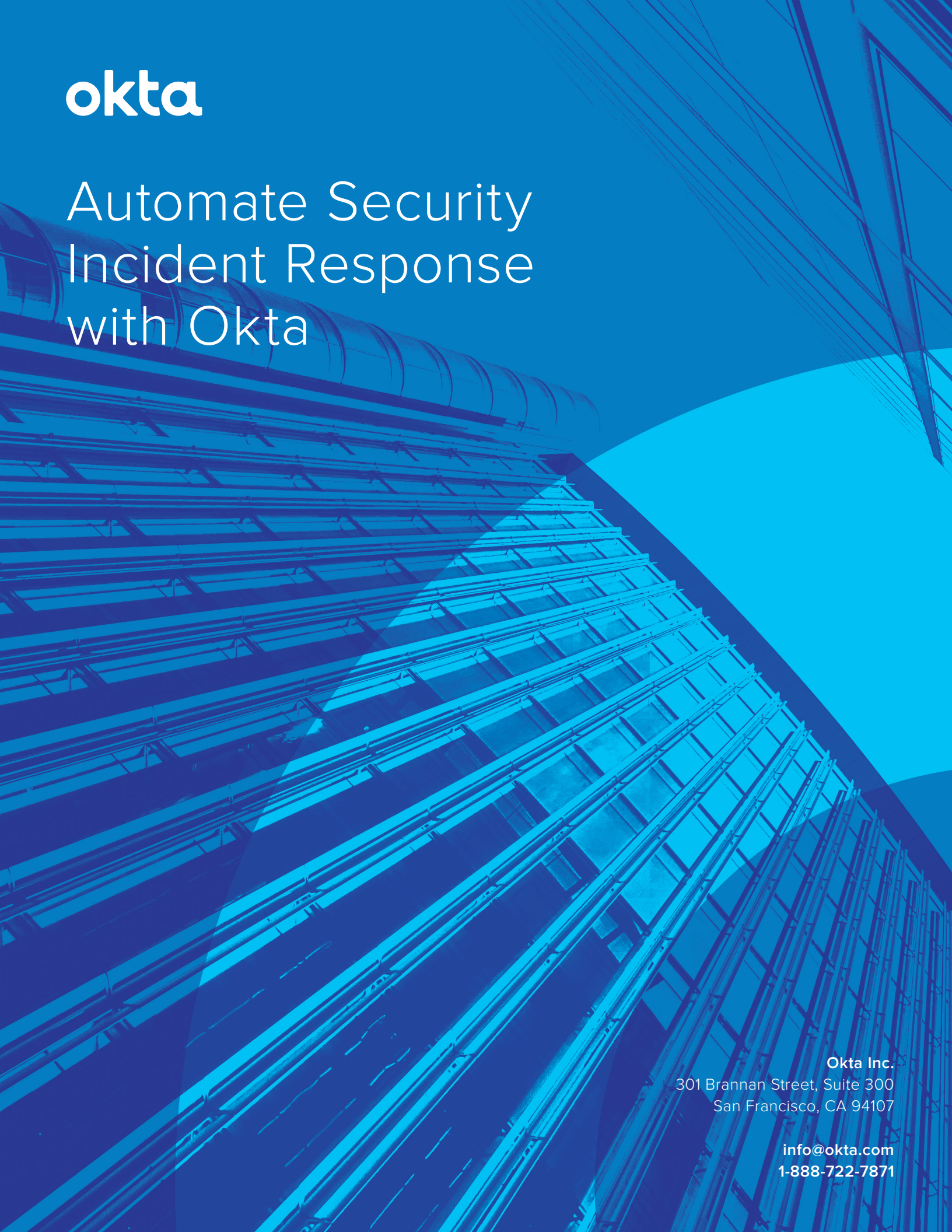
okta

Automate Security Incident Response with Okta



Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

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

Security threats require immediate response. Automation and improved security orchestration make that possible.

Security attacks can happen in an instant. For example, 30% of people who receive a phishing email open it, according to **Verizon's 2016 Data Breach Investigations Report (DBIR)**. On average, it takes them just 1 minute 40 seconds to open it, and 3 minutes 45 seconds to blithely click on its malicious link or attachments.

In less than 5 minutes, your network, apps, data, and users have gone from safe to compromised.

Because this common and devastating kind of hack can happen so quickly, companies must be prepared to take immediate action the moment a suspicious actor is identified. In fact, to stop a breach in progress before intruders get a chance to wreak havoc, security response needs to begin faster than humans can react. This means incidence response operating at maximum efficiency, and even fully automated where possible.

The faster a security team can take meaningful action against a threat, the safer a company will be.

Data Breaches by the Numbers

Cybercrime isn't new—but increasingly, exploitable user credentials are the target.

$1.33B
Financial losses due to cybercrime for US companies in 2016[1]

$3.62M
Average cost of a single data breach[2]

30%
Portion of phishing attacks in which the recipient opened the message[7]

1 MIN 40 SEC
Average time it takes for a recipient to open a phishing email[8]

9,576
Number of reported phishing incidents in 2016[3]

91%
Percentage of phishing attack in which the attacker stole the recipient's credentials[4]

74%
Percentage of data breaches in the first half of 2017 that involved identity theft[5]

3 MIN 45 SEC
Average time for a recipient to click on a malicious link or attachment[9]

Sources:
1. https://www.statista.com/markets/424/topic/1065/cyber-crime/ 2. https://www.ibm.com/security/data-breach/index.html /
3, 4, 6, 7, 8, 9. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
5. https://www.statista.com/statistics/329593/frequency-share-incident-classifiaction-patterns/

How Do You Address the Threat?

The first step is to make credentials as secure as possible. A main way to protect credentials is to implement multi-factor authentication (MFA). With MFA, a company can create more secure authentication policies without overburdening users. MFA is a critical part of protecting credentials and is a first line of defense against threat actors.

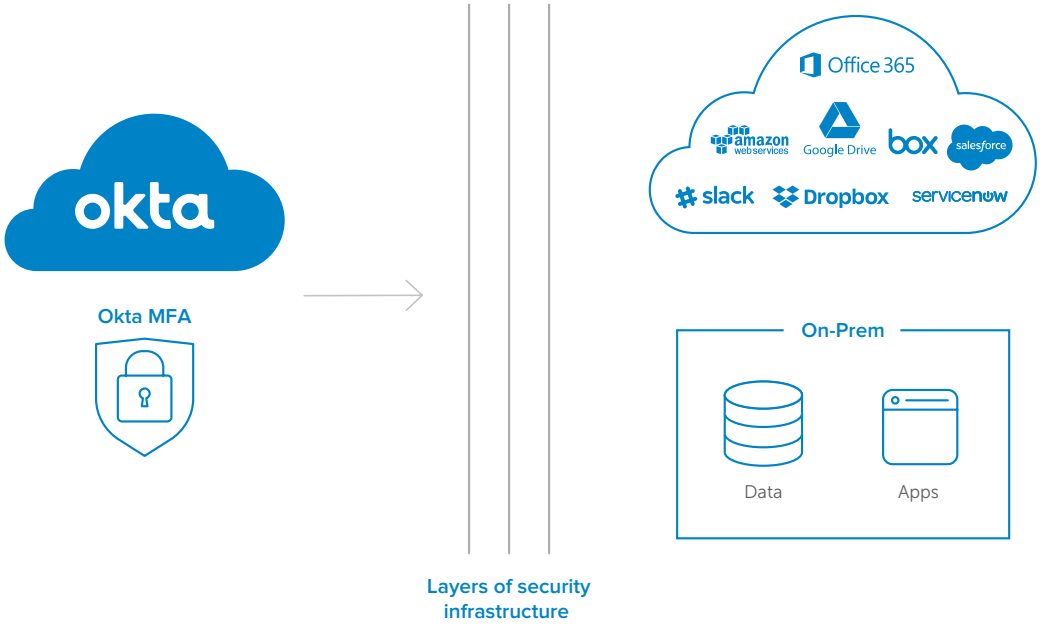
An additional security layer behind credentials is for companies to have visibility into user activities to detect suspicious behavior. When someone logging into a system is identified as suspicious or malicious, the system should rapidly alert security analysts to take immediate action. Better still, where possible and appropriate, a policy-based automatic response can instantly force a step-up authentication or even suspend the suspected user. In either case, the attacker is stopped before any harm is done to the enterprise.

With attacks happening so frequently and quickly, it's impossible to manually safeguard a complex environment. It takes sophisticated tools for identity management, analytics, and security automation to keep your enterprise safe. Protecting identity is a key part of elevating your security posture.

That's where Okta comes in.

Okta provides the secure authentication and MFA to offer to companies an identity-based security perimeter around cloud and on-prem infrastructure. And beyond that, Okta's security partnerships help security companies achieve the degree of automation necessary to keep an enterprise safe.

Okta provides unified monitoring and automation that starts at the identity layer and works with other parts of a company's security infrastructure. This is so security analysts have the intelligence they need at their fingertips to contain any attack and protect their organization's assets.



Okta MFA integrates with your security infrastructure to protect cloud and on-prem apps and data.

How Okta's Identity-Driven Security Works

A security infrastructure includes many types of solutions to monitor traffic, detect suspicious activity, and access/correlate data to generate alerts. These systems detect suspicious and unauthorized log-in attempts, as well as suspicious post-login activity, like a user trying to access sensitive information or download every contact from a CRM.

Okta works with these systems to ensure that once a threat is suspected or identified, immediate action is taken; such as prompting the user for a step-up authentication, or suspending their account while the suspicious activity is investigated.

These responses can be part of a semi or fully-automated security workflow—the choice is yours. Whichever approach you choose, Okta is user friendly, easy to incorporate, and flexible in the degree of automation and types of incident responses it supports.

How Does Okta Help Automate the Security Response?

Okta has an expanding security partner ecosystem and integrates with analytics systems, security orchestration, firewalls, VPNs, and cloud access security brokers (CASBs). Each piece of your security infrastructure provides a different path to automating a response, and Okta can fit seamlessly into any of those workflows. If it's part of the existing infrastructure, Okta can work with it.

There are many different ways to block a user who's intent on mischief. Okta doesn't prescribe one way to do things; choose a workflow, a degree of automated response, a type of software, a software provider, and Okta will work with that choice. Okta offers flexibility in the degree of automation it enables, the partners it works with, and the types of security systems with which it interacts.

When a security system detects a suspicious actor, Okta can enforce any number of policies from asking the user to re-authenticate all the way to suspending the user's access. This can happen automatically or if specifically directed by a security analyst. Okta integrates with your existing security infrastructure to make enforcing security policies faster and more efficient

Here's a deeper dive into some of the ways Okta can help.

1. Analytics Systems

Many organizations manage and review security alerts through a security analytics engine like IBM Qradar, Preempt, Splunk, or Sumo Logic. In these situations, Okta integrates with these and other analytics engines to discover and route a potential identity-based threat event to security analysts who can further investigate.

Once they choose an appropriate response, security analysts can complete the cycle and prompt Okta to take action such as force a step-up authentication on the user, or suspend access altogether.

Okta works with analytics systems to collect, monitor, understand, and analyze data from throughout the IT and security infrastructure; data that comes from a firewall, a VPN, a cloud-based app, or other piece of hardware or software.

Together, Okta and the analytics system aggregate and correlate all the relevant data from across your security ecosystem to better identify suspicious activity on your network, and directly alert authorized responders.

2. Security Workflows and Orchestration

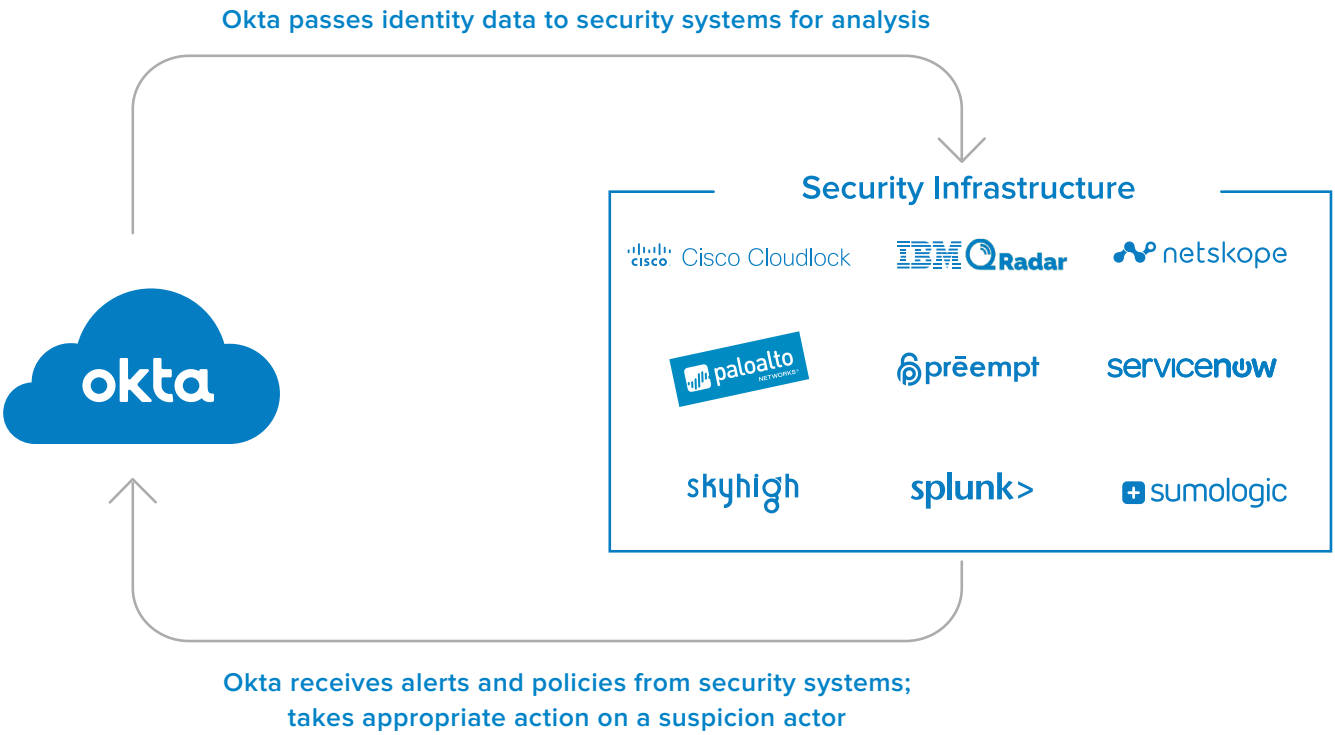
Okta integrates with workflow orchestration tools like ServiceNow to make the incidence response more efficient. When suspicious activity is identified in an analytics engine, ServiceNow takes that alert and routes it to the right security analyst, who can then go back into ServiceNow to enforce security policy in Okta. Incidence response can be customized based on desired degrees of automation, to strategically safeguard corporate apps and services at the identity layer.

Similarly, if a security platform like Palo Alto Networks discovers a threat, it can integrate to alert Okta as the user accesses the corporate network. If a CASB like Cisco Cloudlock, Netskope or SkyHigh detects suspicious activity, like someone trying to download every file from a content or collaboration system folder, it can also alert Okta to take action.

In these scenarios, Okta moves the suspect user to a high-security group and triggers one or several native actions, such as terminating all open sessions and forcing the user to log back in, forcing a multi-factor authentication challenge, or a different policy-based action.

These security policies can happen automatically, with the security system talking directly to Okta; or the alert can be routed to a security analyst who can then use Okta to enforce a policy.

When integrated into your existing security infrastructure, Okta vastly enhances your ability to accelerate, or even fully automate, security policy enforcement at the identity layer.



Benefits of Incorporating Okta into Your Security Infrastructure

Add Okta to an existing security infrastructure to:

1. Create additional layers of security through user context awareness
2. Provide identity data to security analysts
3. Create highly efficient security workflows
4. Automate incident response
5. Enforce a wide array policy-based security actions, from re-authenticating a user to suspending their access

Safeguard Systems from the Identity Level Up

Many security attacks today are coming from malicious actors using stolen or compromised credentials to hack into enterprise systems. Okta's easily-integrated security partnerships offer powerful tools to help address these threats quickly and decisively.

Added to the security infrastructure, Okta can enforce policy against a suspicious user by alerting security analysts to the threat, or even automatically implementing a policy-based response to stop the attacker in their tracks.

The Okta Partner Ecosystem

Okta works with a constantly growing and evolving ecosystem of leading security partners to provide the most complete, effective security response for any enterprise. Okta can integrate with many solutions that already play a key role in security landscapes, to speed the security response—or fully automate it—at the identity layer. Some of our partners include:

Cisco Cloudlock
IBM QRadar
netskope
paloalto NETWORKS
preempt
servicenow
skyhigh
splunk>
sumologic

Identity is the new security perimeter, and Okta is the guard that keeps that perimeter secure.

Okta integrates with your existing security infrastructure. Contact Okta today to find out how you can add identity data and identity-level threat remediation to augment your overall security posture.

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 5,000 apps, 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.

To learn more about Okta, visit:
http://www.okta.com

Subscribe to Okta's blog:
http://www.okta.com/blog

Follow Okta on Twitter:
www.twitter.com/okta

okta