BUSINESSES @ WORK

JANUARY 2018

Businesses @ Work takes an in-depth look into how organizations and people work today—exploring employees, partners, contractors, and customers, and the apps and services they use to be productive.

Welcome to our January 2018 annual Businesses @ Work Report! Businesses @ Work does just what its name implies: it examines how organizations, along with the people who work for and with these organizations, get work done. We analyze our data and identify key trends on an annual basis; you can also find the most popular apps and fastest growing apps charts updated quarterly on our **Businesses @ Work Dashboard.**

You're probably wondering, what's changed in the last year? Turns out, quite a lot. When we dug into our data for 2017, we discovered: there's more than one way for an app to be "popular," companies are heavily investing in security apps (and they need to be!), stringent password policies *and* high assurance second factors are crucial, and the dev tools marketplace continues to grow. Learn more below.

How did Okta create this report?

To create all our Businesses @ Work reports, we anonymize Okta customer data from our network of thousands of companies, applications, custom integrations, and millions of daily authentications and verifications from countries around the world. Our customers and their employees, contractors, partners and customers use Okta to log in to devices, apps and services, and leverage security features to protect their sensitive data. Our customers span every industry and vary in size, from small businesses to enterprises with tens of thousands of employees. As you read this report, keep in mind that this data is only representative of Okta's customers, the applications we connect to and the ways in which users access these applications through our service.

Unless otherwise noted, this report presents and analyzes data from November 1, 2016 to October 31, 2017, which we refer to as “this year,” “this past year,” “today” and “in 2017.” Similarly, when we refer to “last year” or “in 2016”, we are referring to data from November 1, 2015 to October 31, 2016. 2015 refers to the same period in its respective year.

KEY FINDINGS

The Most Popular Apps of 2017

Today, there are hundreds of unique, category-defining apps for businesses to choose from. Organizations and IT departments would be hard-pressed to test them all. Popularity matters. This year, we not only looked at apps by popularity (number of organizations that deploy that app), but also by usage (number of monthly active users) within an organization. Office 365 has led the pack of most popular apps based on number of customers since January 2015. Office 365’s lead becomes even more notable when you consider their number of monthly active users, which grew 92% in the past year. That said, the email race is never over. In our network, Google has been adding G Suite customers faster than Microsoft has been adding Office 365 customers over the past 3 months, 6 months and even the last 12 months. Notably, among Okta customers, G Suite grew its customer base 49% this past year, compared to Office 365 which grew 40%. In other news, wall-to-wall business apps like Workday and ServiceNow are much more “popular” based on number of monthly active users (2nd and 3rd most popular apps, respectively) than they are based on the number of customers using these apps. Conversely, AWS and DocuSign are the 3rd and 9th most popular apps in our network respectively, based on number of customers, yet they don’t make the top 15 based on number of monthly active users. This is likely because they are often accessed by a limited number of departments with an organization.

Tear down this wall—organizations are going borderless for security and collaboration

Our fastest growing apps chart makes one thing abundantly clear: companies are investing in security and collaboration tools.

SECURING A BORDERLESS WORLD

7 of the 15 fastest growing apps in our network this past year (Jamf, KnowBe4, DigiCert, Cisco Umbrella, Mimecast, Sophos and CloudFlare) are security tools or have security use-cases. Jamf, which provides software for managing and securing Apple devices, is a notable newcomer to the list and the fastest growing app in our network with 389% year-over-year growth. Security awareness training company, KnowBe4 grew 290% in the past year, indicating organizations’ increased focus on training employees around security best practices and ways to combat social engineering attacks.

THERE’S NEW BLOOD IN THE COLLABORATION RACE

For the first time since we began publishing Businesses @ Work, Slack competitors have achieved fastest growing apps status. Cisco Spark is the second fastest growing app in Okta’s network, with 377% growth this past year. New, innovative features like Spark’s **virtual office assistant** seem to be driving some of that traction. Meanwhile, another relatively new entrant to the collaboration space, Workplace by Facebook, was the 5th fastest growing app this year, with 163% growth. Workplace by Facebook has made some critical product improvements, forged partnerships with compliance companies, and built key integrations with Box, Dropbox, Microsoft and others. You may be wondering where Slack is on this list for 2017. With staggering growth the past few years, Slack was most recently featured on both the most popular and fastest growing apps lists in our

2017 report. They were the only app ever to be featured on both lists in the same report, and this year Slack graduated to 7th on the most popular apps list (based on number of customers).

Plenty more where app came from

In When it comes to the number of apps enterprises use, organizations are stepping on the gas. Customers across all industries in our network continue to add more apps to their environments each year. The tech industry uses the most distinct apps at 1,910, followed by consulting/business services (1,611 distinct apps) and finance/banking (1,545 distinct apps). And companies aren't just using different apps, the average organization is also increasing the number of apps they use. Over the past two years, the median number of apps across our global customer base has grown 24% from 2015 to 2017. The biotech/pharma/healthcare industry saw the most app growth from 2016 to 2017 at 36%, followed by the finance and banking industry, which grew 33%. And it's not just off-the-shelf apps that customers are connecting to. 87% of customers in Okta's network have at least one custom integration, and 64% have more than four custom integrations.

Have apps, will travel (and read and bank and more)

In past Businesses @ Work reports, we have always closely examined how employees are getting work done. We know what email, HR, document storage and collaboration tools are most popular in the enterprise. But in today's global economy, we were curious: what *else* do modern workers care about when it comes to their jobs? We looked at travel, banking, e-learning and news apps to find out. Here's what we learned: Southwest and United Airlines are the top two travel apps in our network, by a significant margin. (Everyone wants that **Southwest Companion Pass**!) CNN and *The Wall Street Journal* are the top two news sources, but *The New York Times* and ESPN are close behind. PayPal is the most popular banking site. And, as many of today's hottest job skills aren't taught in school, elearning is on the rise. 31% of Okta customers accessed online learning courses in 2017, with Lynda.com being the most popular.

All your tools are belong to us

The dev tools marketplace continues to grow as more organizations start off cloud-first, or commit to building their digital footprint. Today, 47% of our global customer base is using at least one developer tool. JIRA is, far and away, the most popular developer tool among our global customers who are using dev tools. 48% of these Okta customers are using JIRA. Our data also shows that organizations across *all* industries are adopting developer tools, building their own apps and moving to the cloud. While the technology and media/entertainment industries are leading this charge (with 69.4% and 68.7% using dev tools, respectively), the insurance and finance/banking industries had the most significant increases from 2016 to 2017.

It's not just China—identity attacks originate worldwide

It's well known that 81% of hacking related breaches are caused by compromised credentials[1]—but what else do we know about attacks against identities? We took a look at the identity threat landscape and found that while we may see China in the news for hacking, the real threats are coming from, well... everywhere. Yes, 48% of all threats are coming from IPs geolocated in China. But that means 52% are coming from elsewhere, including 7.7% from the United States, 4.5% from France, 3.4% from Russia and 2.6% from the Netherlands. We may not hear about them because more than 50% of global attacks we analyzed do not have prior intel from the open source community. Of these attacks with no prior intel, 36% are coming from Europe, including 19% from France, 12% from the Netherlands, 11% from Russia and 10% from Germany. But the real non-starter for most businesses? The 23% of attacks coming from Tor exit nodes (more commonly described as the dark web). Unless you have a reason to interact with Tor, we'd suggest just blocking those IPs.

1. Verizon's 2017 Data Breach Investigations Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Beyond the 8 character minimum

Threats are coming from everywhere: how well are you protecting against them? We took a look at the average Okta password policy (as passwords are rightly encrypted in Okta so we can't see them) to see first what companies are doing to protect against identity focused attacks, like brute forcing (trying a large list of passwords against one account), password spraying (trying a small number of general passwords like 'password123' against a targeted list of accounts) and phishing (tricking you into giving up your credentials). We compared this analysis to a list of publicly-exposed passwords and discovered that (surprise, surprise) the average person isn't making good choices about their passwords. However the good news is that companies of any size can mitigate many password based attacks by enforcing longer credential length and MFA.

Not all factors are created equal

Passwords aren't a silver bullet to protect your apps and data. They're just one piece of what should be a much more sophisticated puzzle. MFA adoption among Okta customers continues to grow, as does the average number of factors they deploy. Nearly 70% of Okta customers are offering three or more factor options to their users today (compared to 62% last year). While implementation is a good first step, there's more you can do. Our data shows our customers continue to use less secure factors like SMS and security question. The infamous security question is the most popular factor we see deployed and adopted, and it's growing. 38% of MFA users are using security questions today, compared to 30% last year.

What are the most popular apps?

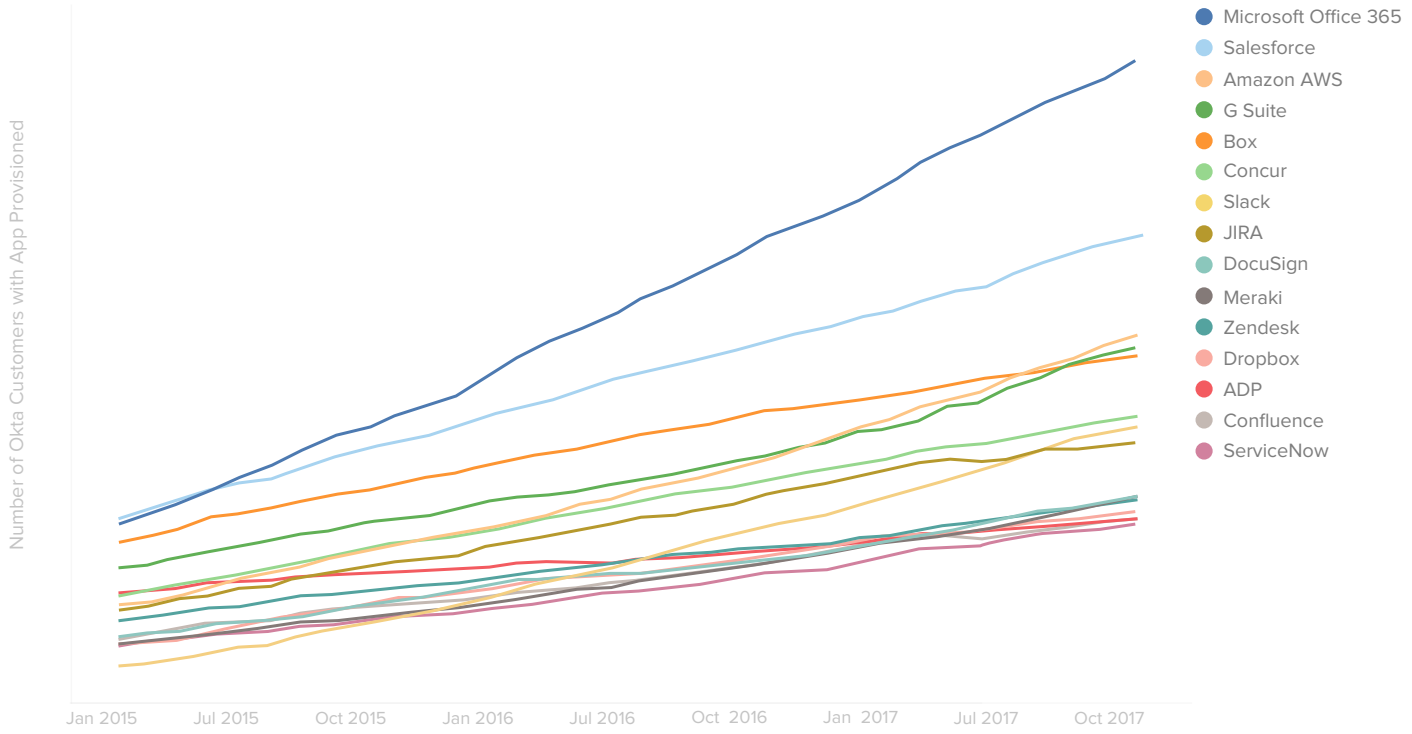
Many organizations have developed a best of breed cloud app strategy, meaning they select the best app in each category for their business needs. But what does a best of breed app strategy *really* mean? Do enterprises test out every app in a category—HR, messaging and collaboration, document storage, etc.? Or, do they often choose the most popular app in a particular category, the one that is getting the most buzz? Popularity matters. Our most popular apps chart has been featured in Businesses @ Work since the very **first report**. To date, we've defined the most popular apps as those with the largest number of customers with the application provisioned.

But is that methodology the only proxy for popularity? This year, we're *also* analyzing most popular apps based on the number of monthly active users (defined as users who have logged into an app, via Okta, at least one time in the past 30 days).

When comparing the two graphs, here's what we found for 2017:

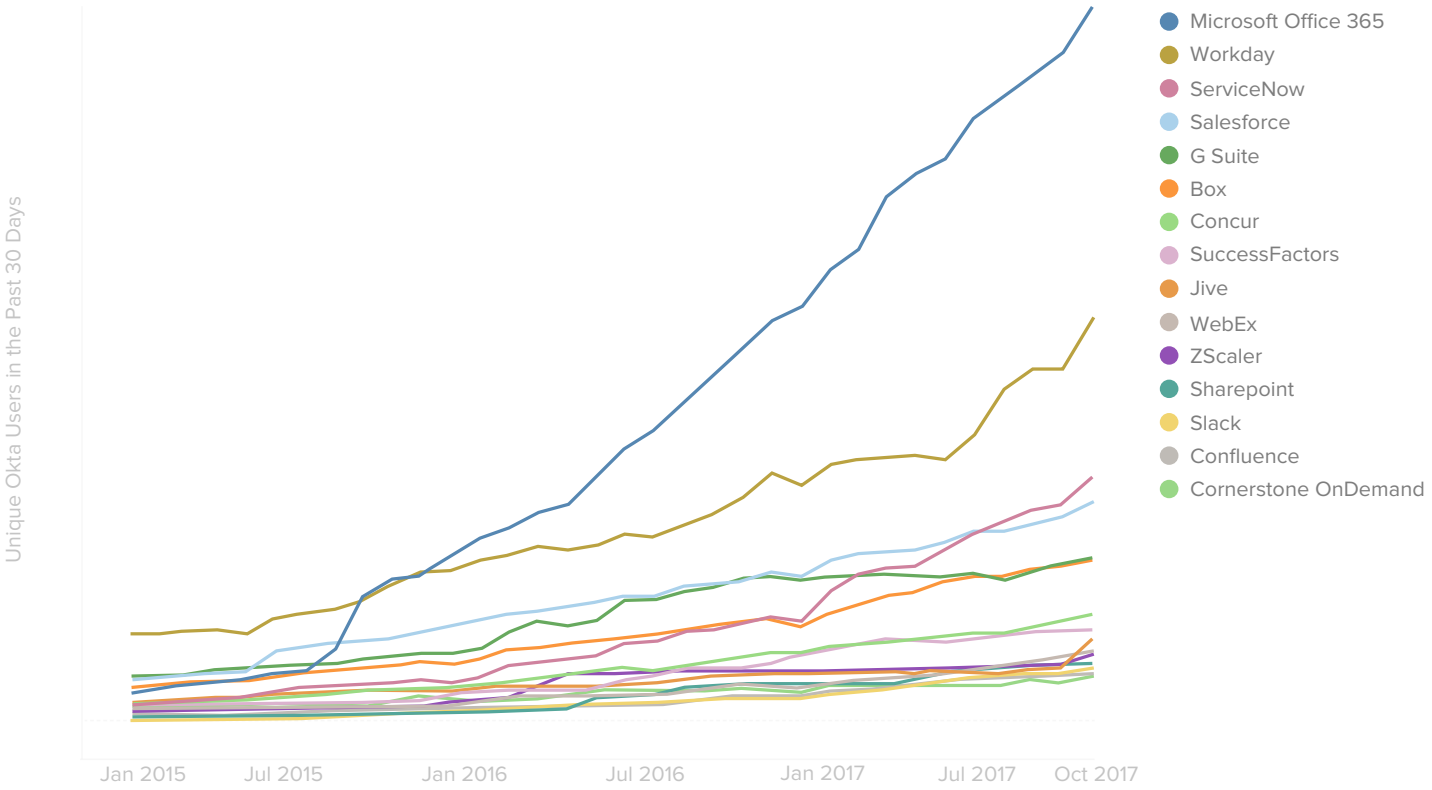
- Office 365's lead as the most popular app is even more notable when considering the number of monthly active users.
- Workday is number 2 based on number of monthly active users, but isn't in the top 15 based on number of customers with the application provisioned. Workday's core HR functionality make it a company-wide business app, compared to other apps that are department specific. The same is true for ServiceNow, which is the 3rd most popular application based on the number of monthly active users, compared to 15th based on number of customers with the app provisioned.
- Department specific apps like AWS and DocuSign continue to be actively deployed in organizations (with 56% and 51% year-over-year customer growth, respectively), but not as widely used.

Most Popular Apps (Number of Customers)



REFLECTS DATA THROUGH OCTOBER 31, 2017

Most Popular Apps (Number of Monthly Active Uniques)



In every Businesses @ Work report we've published to date, there is the inevitable comparison between G Suite and Office 365. While Office 365 has had the lead in terms of popularity, this year's report reminds us that the email race is never over. Notably, Google has been adding G Suite customers faster than Office 365 over the past 3 month time period, 6 month time period and even year-over-year. It appears G Suite's renewed focus this year on the enterprise is paying off. G Suite grew its customer base 49% this past year, compared to Office 365, which grew its customer base 40%. According to Prabhakar Raghavan, VP of Apps at Google Cloud, "Today, more than 3.5 million paying businesses, including companies like Verizon, Nielsen and Colgate-Palmolive, rely on G Suite's intelligent productivity and collaboration apps to transform the way they work. We're excited to see the uptick in G Suite's adoption among Okta's customers, and we look forward to seeing the momentum continue in 2018."

Customer Growth

	TRAILING 3 MONTH GROWTH	TRAILING 6 MONTH GROWTH	TRAILING 12 MONTH GROWTH
G Suite	9%	22%	49%
Office 365	7%	16%	40%

Note: As of October 31, 2017

What are the fastest growing apps?

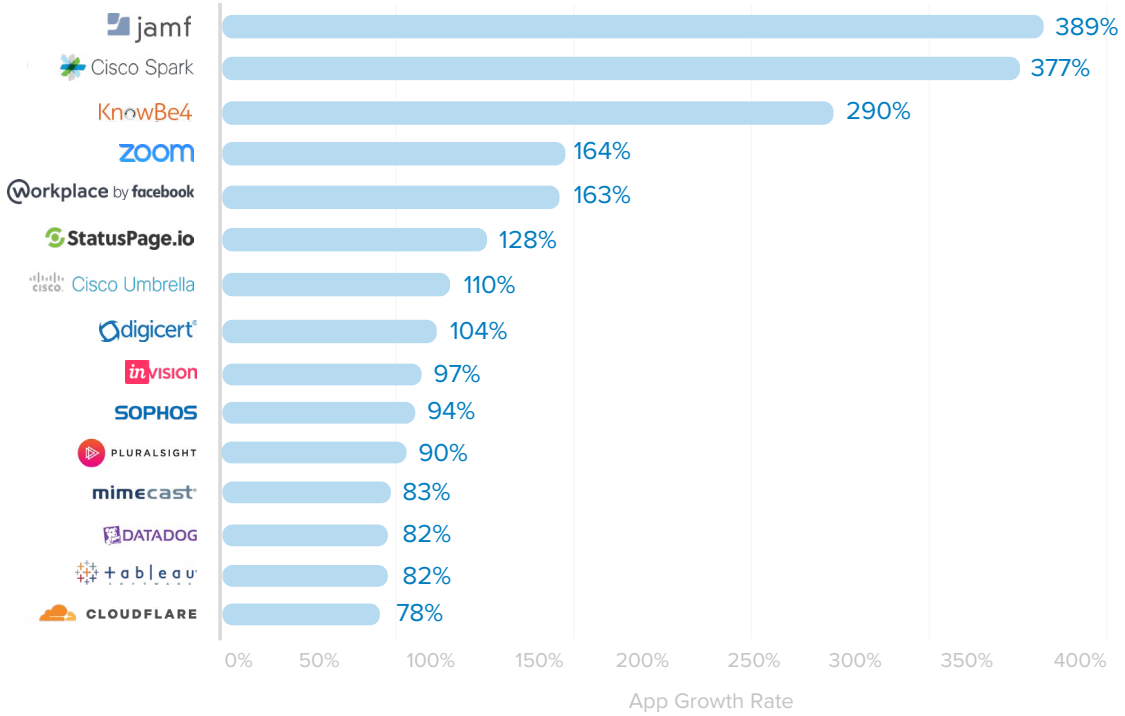
In today's world—where businesses can't always control the devices end-users work on, where they work from, or even the apps they use—security is a tremendous challenge. Businesses are eager to secure their apps and data. And our data is proof of that. *Seven* of the 15 fastest growing apps in our network this past year (Jamf, KnowBe4, Cisco Umbrella, DigiCert, Sophos, Mimecast and CloudFlare) have products with security use-cases. Jamf, which provides software for managing and securing Apple devices, was the fastest growing app in our network this past year, with 389% growth. Security awareness training platform, KnowBe4 was the third fastest growing company with nearly 300% growth. According to Gartner, in the security awareness training market, "growth projections for the next several years remain strong, with a Gartner forecast compound annual growth rate (CAGR) of 45% from 2016 to 2021, and revenue reaching over $1.5 billion in 2021."[2]

Our fastest growing apps chart also tells us the messaging and collaboration race isn't over! For the first time since we began publishing Businesses @ Work in 2015, Slack competitors are on the fastest growing apps chart. Cisco Spark is the second fastest growing app in Okta's network this year with impressive 377% growth. The product's new, innovative features like **virtual office assistant** seem to be intriguing enterprises. Workplace by Facebook, which just launched in October 2016, was the 5th fastest growing app and made some critical product improvements this past year (key integrations with Box, Dropbox, Microsoft and others; bots; partnerships with compliance companies). While Slack is not featured as one of the top 15 fastest growing apps in Okta's network for the first time in several reports, we believe this is primarily due to the scale they have achieved. (Slack is the 7th most popular app in our network based on number of customers and 13th based on monthly active users.) That said, the messaging and collaboration space remains hotter than ever, with competitors popping up on our fastest growing apps chart as they attempt to challenge Slack.

Zoom, which was the fastest growing app in our network in the last report, continues to show impressive growth as the 4th fastest growing app with 164% year-over-year growth.

2. Gartner, Inc., Magic Quadrant for Security Awareness Computer-Based Training, Joanna G. Huisman, 26 Oct 2017.

Fastest Growing Apps Year-over-Year



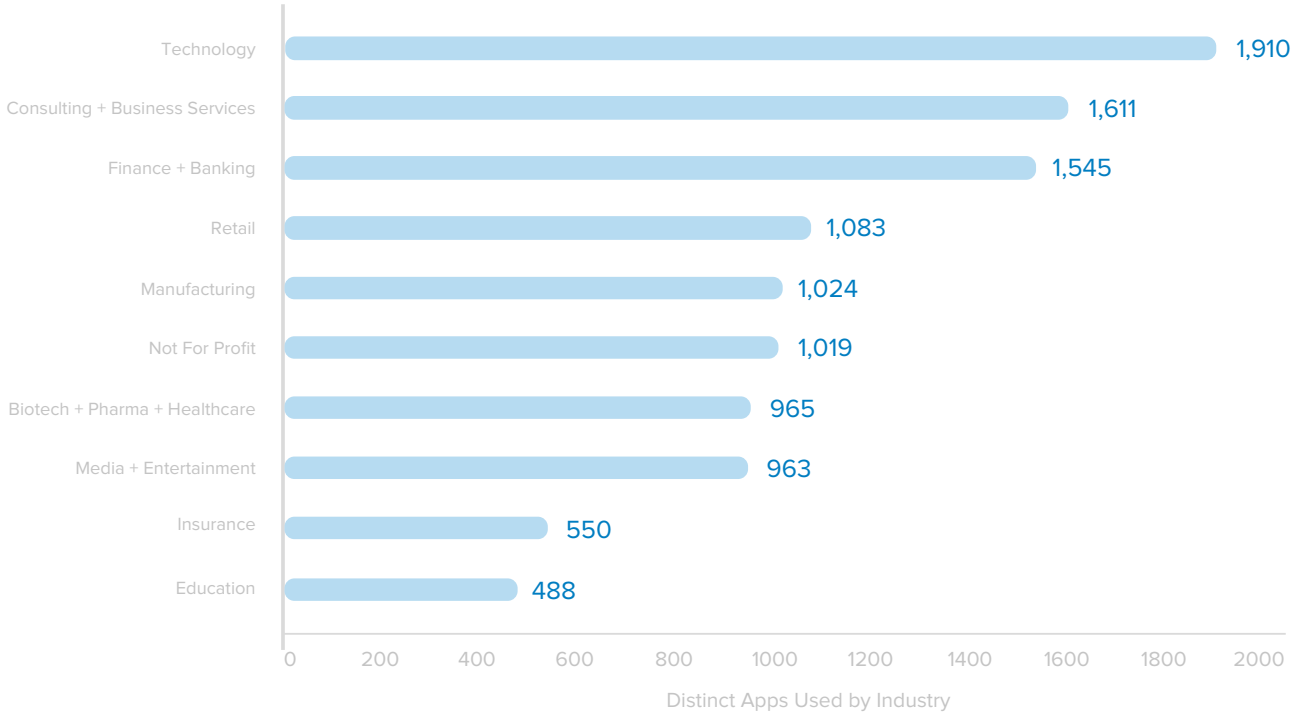
Note: This graph shows the change in rank of each app over time based on Okta's number of customers that make that app available to their employees, contractors, partners, and customers. All apps had at least 100 customers at the end of the period.

PLENTY MORE WHERE APP CAME FROM

How many different apps are industries, and the average company, using?

When it comes to the apps an organization uses, every enterprise is truly unique. We looked at the number of distinct apps used by the top 10 industries in our network. The numbers were staggering! Tech companies lead the pack, with 1,910 distinct apps, followed by consulting/ business services with 1,611 distinct apps. Even more traditional industries (finance and banking, insurance and education) use hundreds, even thousands of distinct apps.

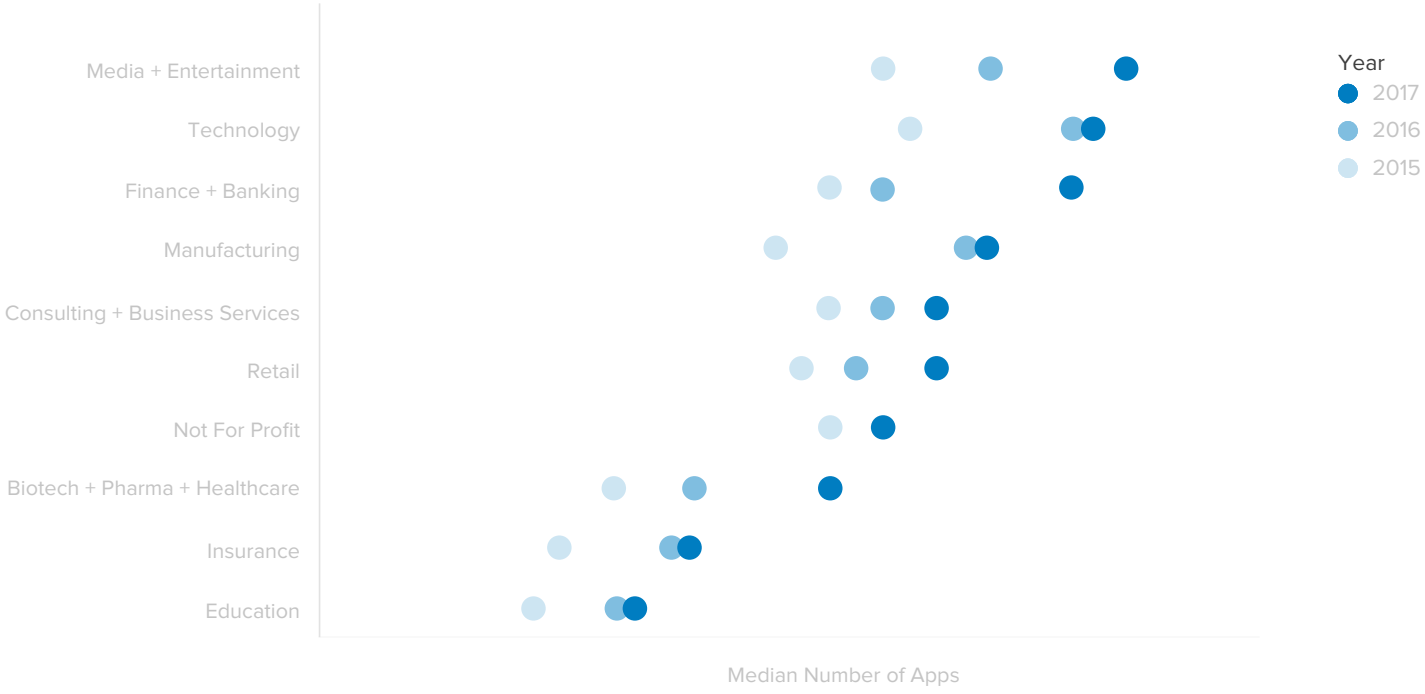
Distinct Number of Apps Used, By Industry



And companies aren't just using different apps, the average organization is also increasing the number of apps they use. Over the past two years, the median number of apps per customer has grown 24%. In fact, customers across all industries continue to add more apps to their stacks each year:

- From 2015 to 2016, manufacturing and technology customers went all in on cloud apps, with growth of 41% and 27% respectively.
- However this past year, two traditionally regulated industries have played catch up. The biotech/pharma/healthcare industry saw the most growth from 2016 to 2017 at 36%. Jason Bush, Chief Information Security Officer at Magellan Health, offers the following to consider for this dramatic increase. "For a long time, healthcare clinicians often dictated what would or wouldn't happen as it related to information technology; it was their practice. However, increased risk to protected health information and increased regulation have prompted regulators and leaders in the industry to now require compliance with current information technology and security standards. Subsequently, healthcare institutions with which these clinicians are affiliated are now more actively influencing and even dictating adherence to such standards. This is one reason we're seeing the most significant growth of application adoption in healthcare."
- Customers aren't just connecting to off-the-shelf apps in Okta's network. Today, 87% of customers in Okta's network have at least one custom integration and 64% have more than four custom integrations.

Median Number of Apps by Industry, Over Time



What are the most popular apps for the modern worker?

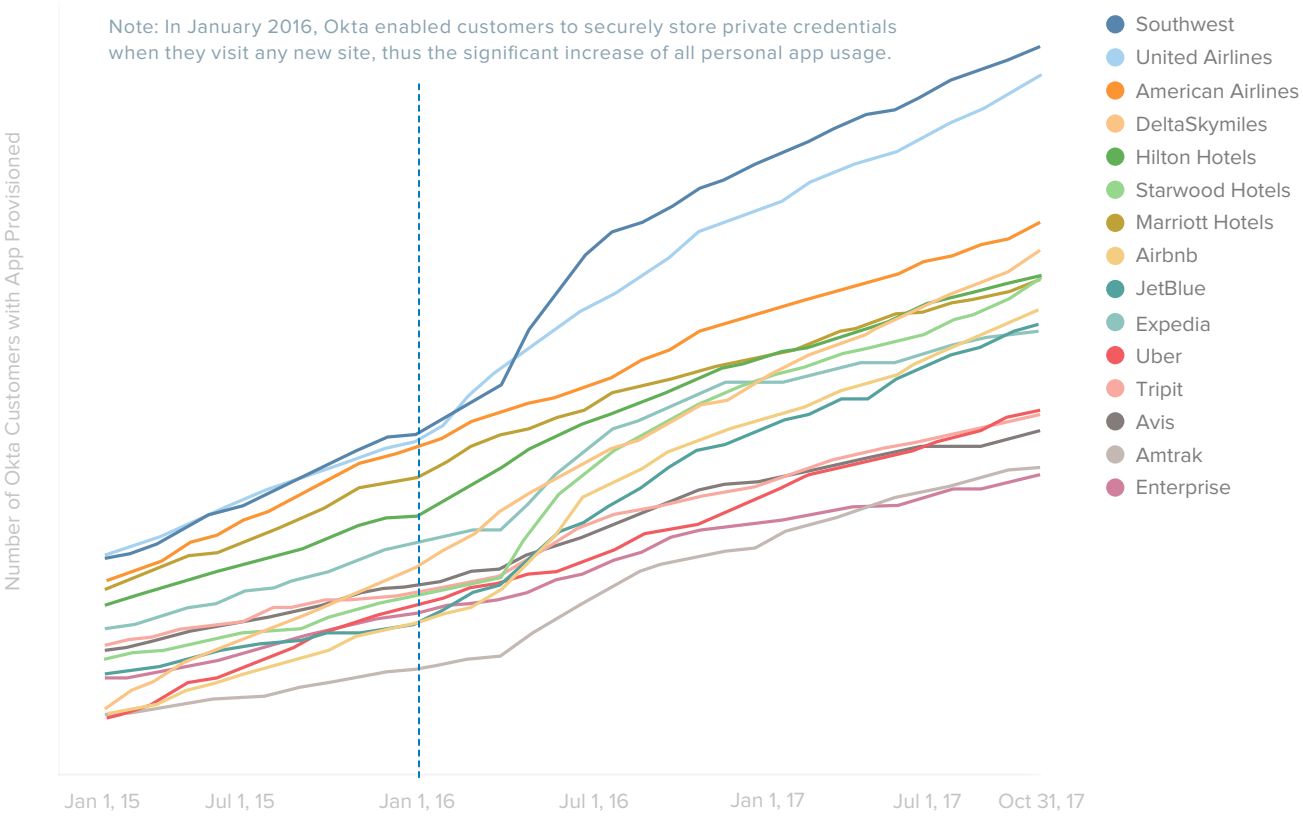
Millennial. Gig economy worker. Remote employee. Whatever phrase you want to use, they're all part of a transformed workplace that doesn't exist solely in the four walls of a business of time's past. Today's workers are increasingly global, and as such they've also brought in a new set of tools that aren't quite what you'd call work apps.

We've closely examined how end-users are getting work done. We know what email, HR, document storage and collaboration tools are most popular in the enterprise. But in today's global economy, we were curious what else is important to a person's success in business? What do modern workers need to be productive, grow their careers, travel and pay their bills?

So we started digging into work-related app categories. That is, the apps employees frequently use that aren't technically considered "business apps." What are their go-to news sources? What sites do they use to book travel? Are they continuing their education? If so, what e-learning tools are they using? And what banking sites are most common? Here's what we found:

Southwest and United Airlines are the top 2 travel apps in our network, by a significant margin. (Everyone wants that **Southwest Companion Pass**!) Hilton, Starwood, and Marriott are the top hotel apps. But, industry disrupter Airbnb isn't far behind, as the company's new focus on business travelers has paid off. According to **Forbes**, more than 250,000 businesses use Airbnb for travel today, compared to just 250 in 2015. (Airbnb usage grew 39% in our network year-over-year.) While Airbnb doesn't offer reward points, they do offer new business-centric perks such as self service check-in, one-click expensing, and the ability to easily rent an entire home for your entire team.

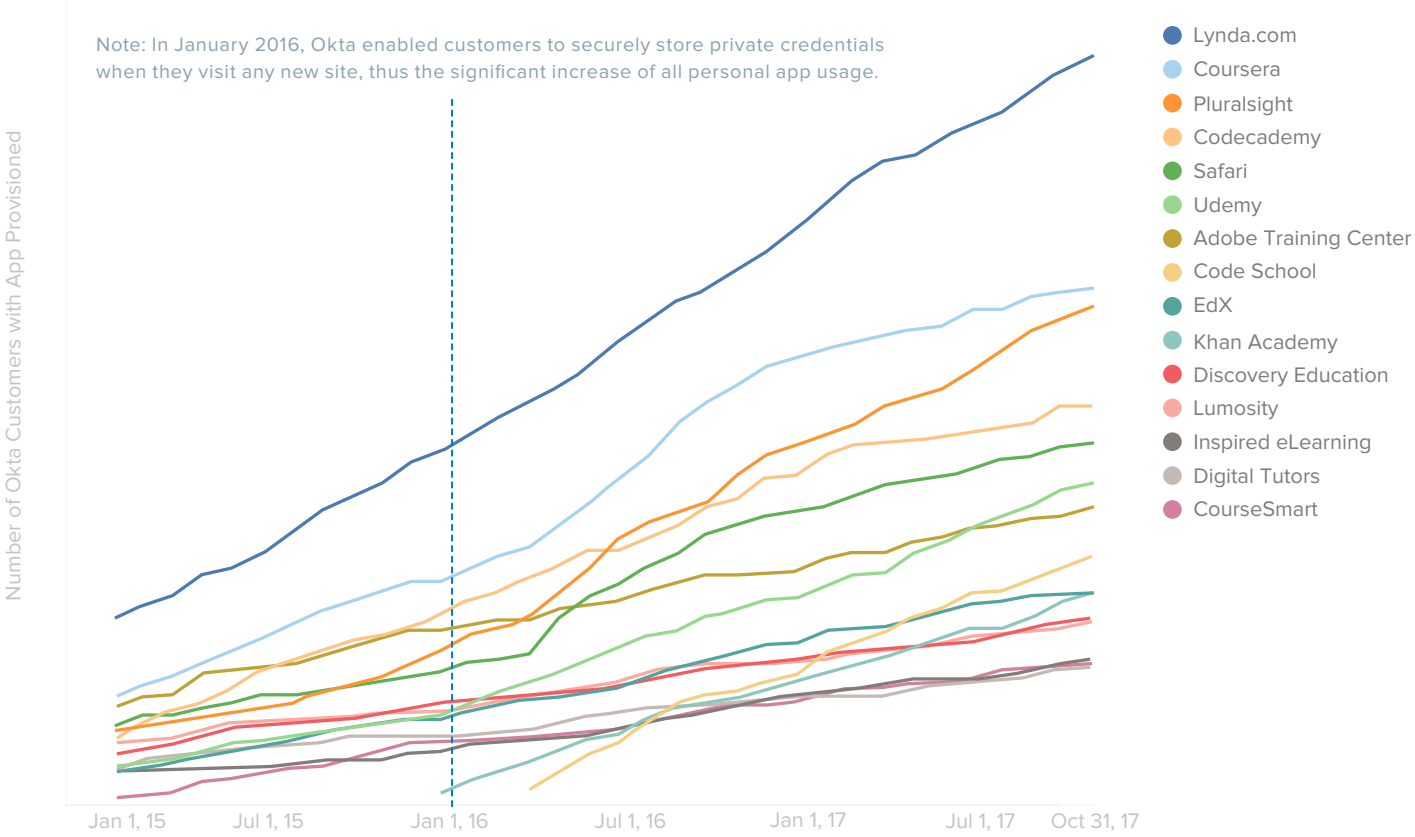
Most Popular Travel Apps Over Time



Note: Graph includes both personal and corporate app usage.

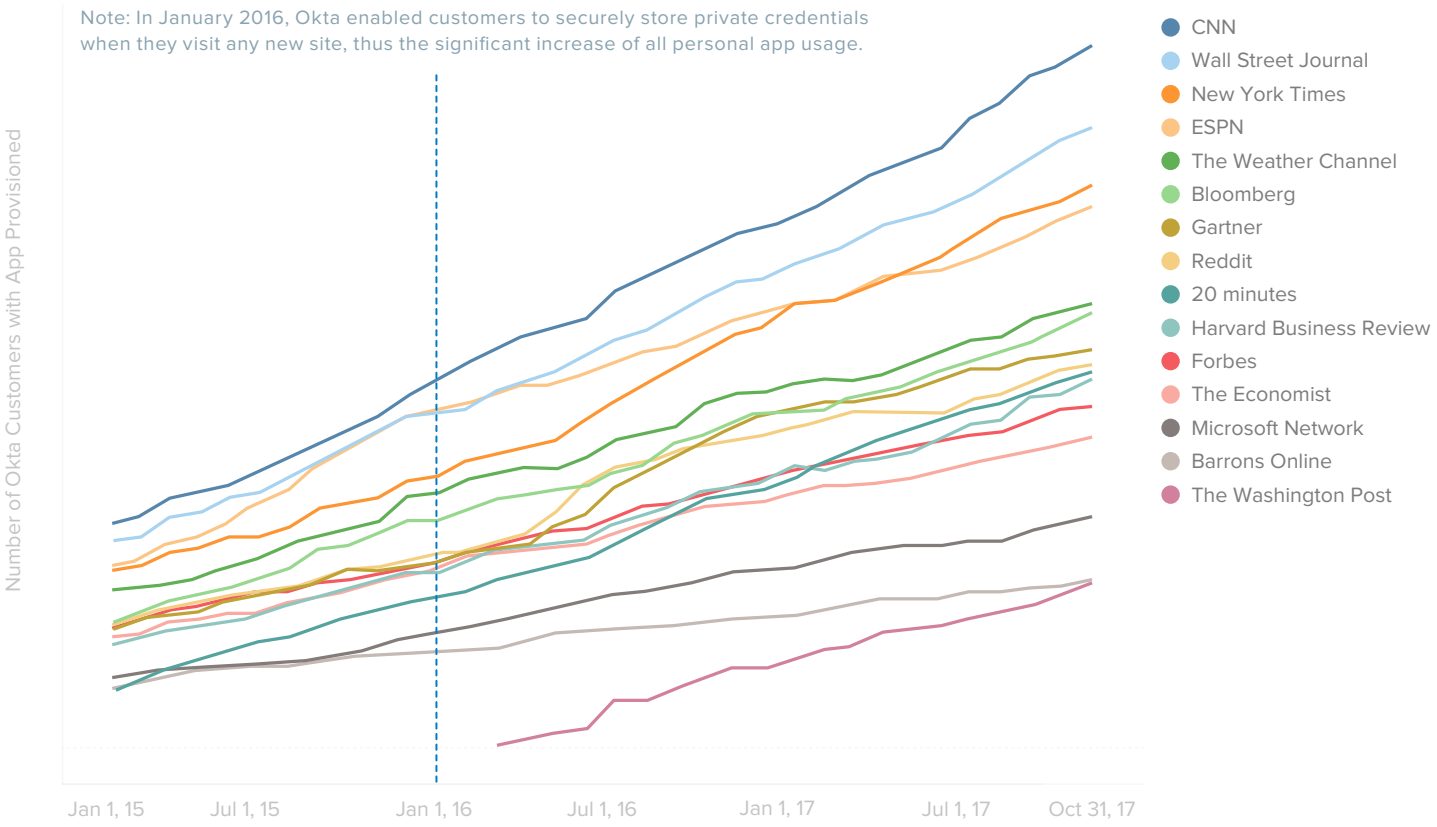
There's a gap between the skills people have and the jobs that they want—especially given that many of the **hot jobs** (machine learning, data scientist, dev-ops engineer, etc.) require hands-on training. Both individuals and businesses are prioritizing lifelong learning. 31% of Okta customers accessed online learning courses in 2017, either for corporate or personal use. Lynda.com, which was **acquired by LinkedIn** in April 2015, is the number one elearning app in our network. Lynda focuses more on courses for individuals—adding skills (via certificates) to their resumes—whereas the number 2 player in the space, Pluralsight targets enterprises first. Pluralsight's adoption within our customer base grew 22% in the 6 months ending October 2017, and is closing in on Coursera, which only grew 9% in this same period.

Most Popular eLearning Apps Over Time



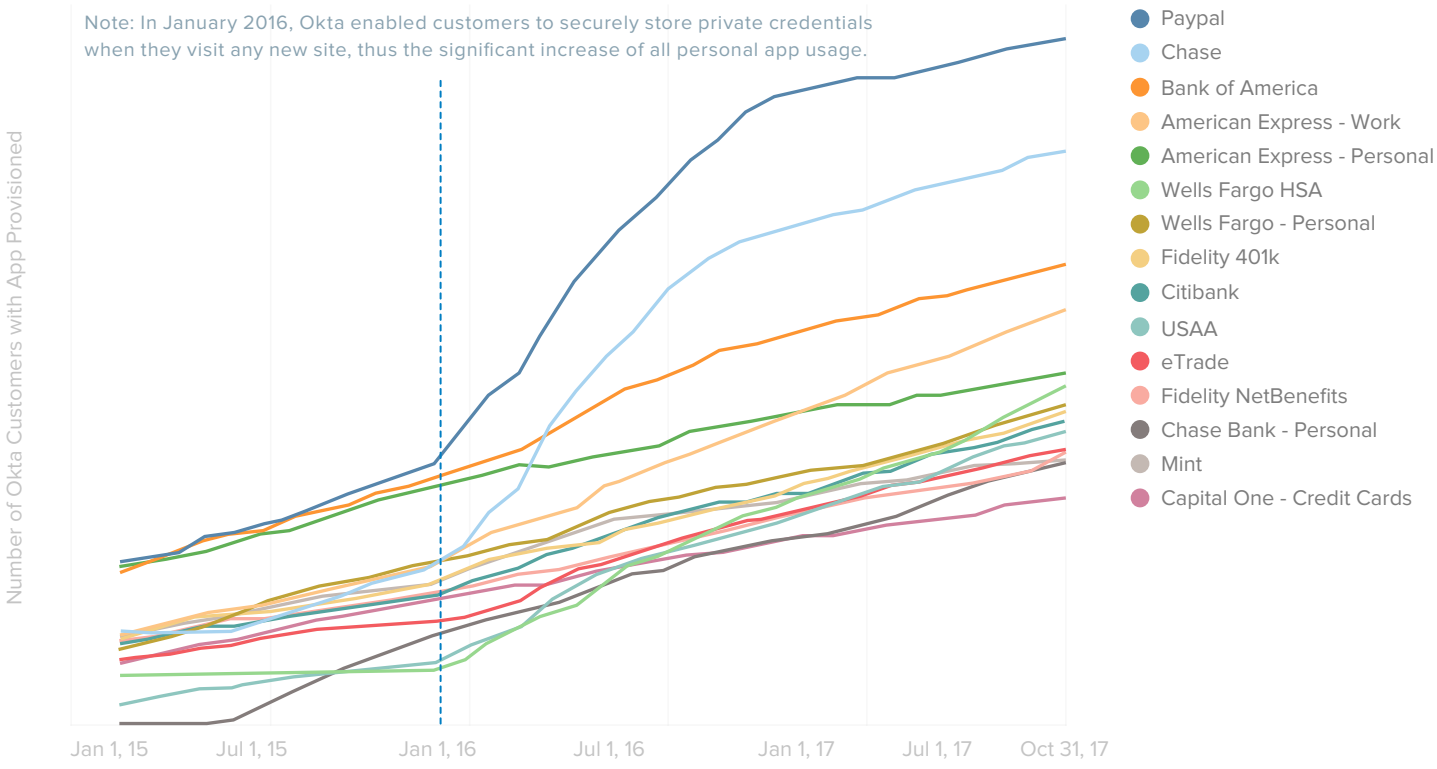
Note: Graph includes both personal and corporate app usage.

Most Popular News Apps Over Time



Note: Graph includes both personal and corporate app usage.

Most Popular Banking Apps Over Time



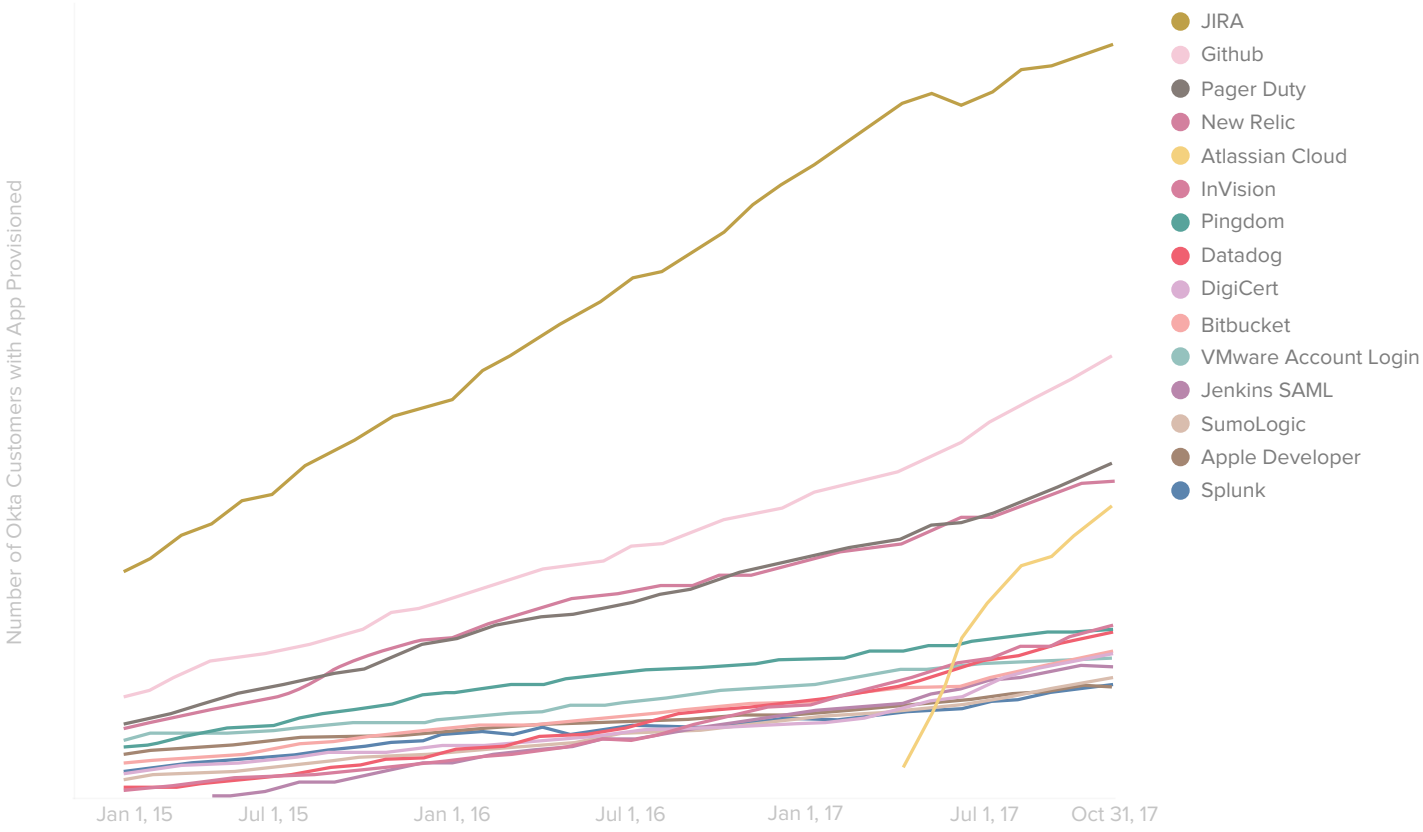
Note: Graph includes both personal and corporate app usage.

What are the most popular developer tools and services?

The dev tools marketplace continues to grow as more organizations embrace a digital transformation and deploy best in class hosting, collaboration and monitoring tools to support their developers. According to Sami Hassanyeh, Chief Digital Officer at AARP, “For us, it’s all about tools that maintain privacy, security and compliance standards, and also fit with the agility and performance we need. That way, we can focus on what we're good at and differentiate our offering. We leverage the marketplace to achieve our architecture goals.”

As we reported in our **October 2017 EMEA Businesses @ Work report**, EMEA is the leader in the adoption of developer tools with 48% of customers using at least one dev tool, narrowly beating out APAC and North America with 44% and 47% usage, respectively. Today, 47% of our global customer base is using at least one developer tool, compared to 43% one year ago. JIRA is, far and away, the most popular developer tool among our global customers who are using dev tools. 48% of these Okta customers are using JIRA. GitHub is the clear number 2, followed by PagerDuty and New Relic.

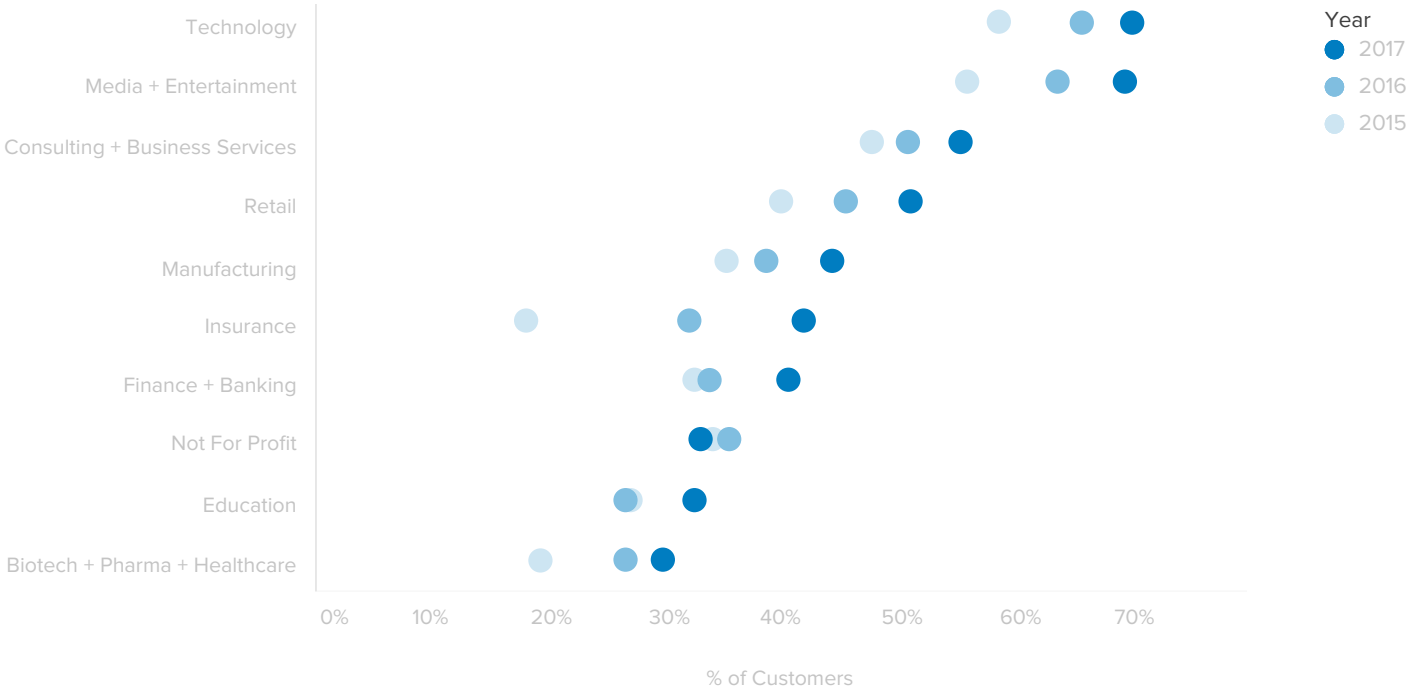
Most Popular Developer Tools Over Time



Note: Atlassian Cloud refers to the unified account identity across both Jira Cloud and Confluence Cloud products as **announced in May 2017**.

We also took a look at the usage of developer tools across industries. While the tech and media/entertainment industries lead the pack (with 69.4% and 68.7% using dev tools respectively), our data shows that slowly, but steadily, organizations across *all* industries are adopting developer tools, building their own apps and moving to the cloud. The insurance and finance/banking industries had the most significant jumps from 2016 to 2017, increasing the percentage customers using a developer tool by 9% and 6% respectively.

Change in Popularity of Developer Tools Over Time



Note: Includes customers that have at least one developer tool as of October 31, 2015, 2016 and 2017.

Where are threats coming from?

According to **Verizon's Data Breach Investigation Report**, 81% of hacking-related breaches leverage compromised credentials. As the leading independent provider of identity for the enterprise, we have unique insight into the threats against credentials. So, we explored our data to surface insights on these attacks.

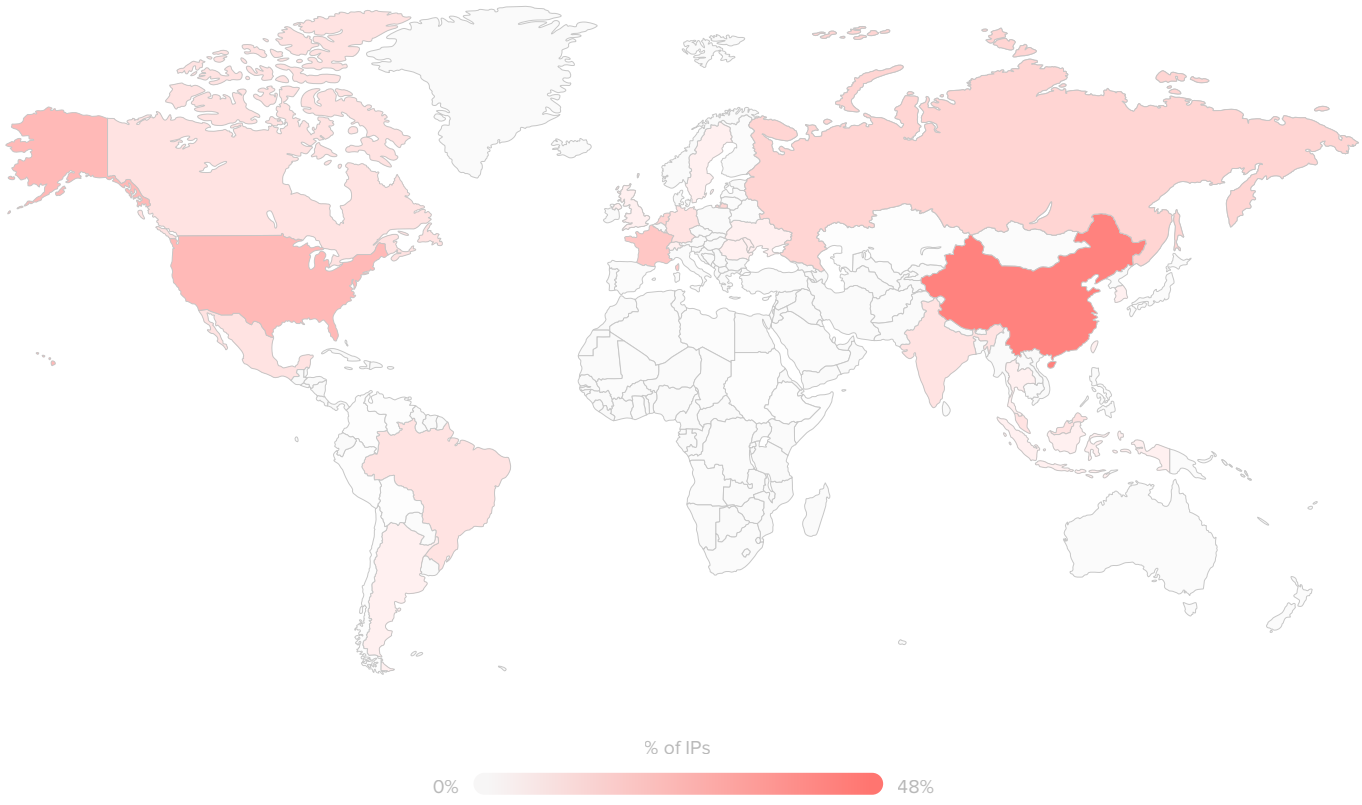
Using Okta's security data, paired with open source threat intel feeds[3], we were able to analyze attacks targeted at the cloud authentication layer.

While we're seeing significant diversity in threat origins, a high volume of attacks are from IPs geolocated as originating from China. When looking at the global threat landscape, 48% of all attacks are coming from IPs geolocated in China, followed by 7.7% from the US, 4.5% from France and 3.4% from Russia.

This threat geo landscape does not include attacks from Tor (dark web) exit nodes. The Tor network encrypts traffic to disguise user identity as traffic moves from one Tor server to the next. Tor nodes receive traffic on the Tor network and pass it along. We found 23% of all attacks were from Tor exit nodes.

3. Any data referring to external threat feeds is static, current in the moment it was pulled, as of November 29, 2017.

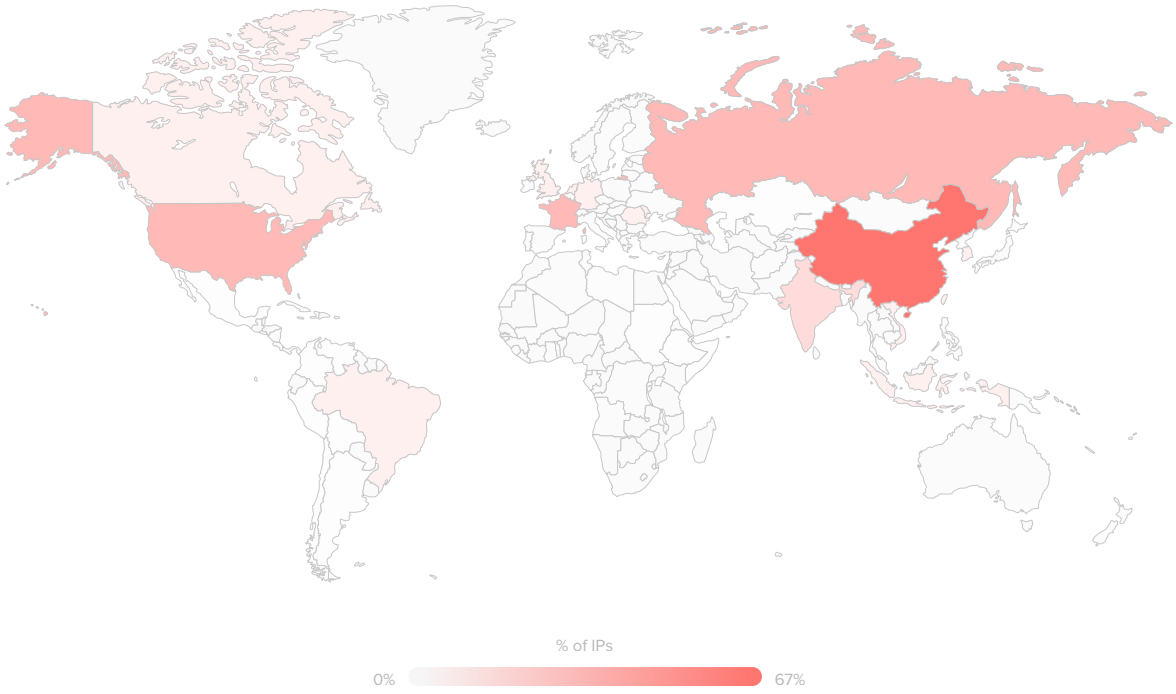
The Global Threat Landscape



Note: Includes all attacks - those that do and do not appear on open source threat intel.

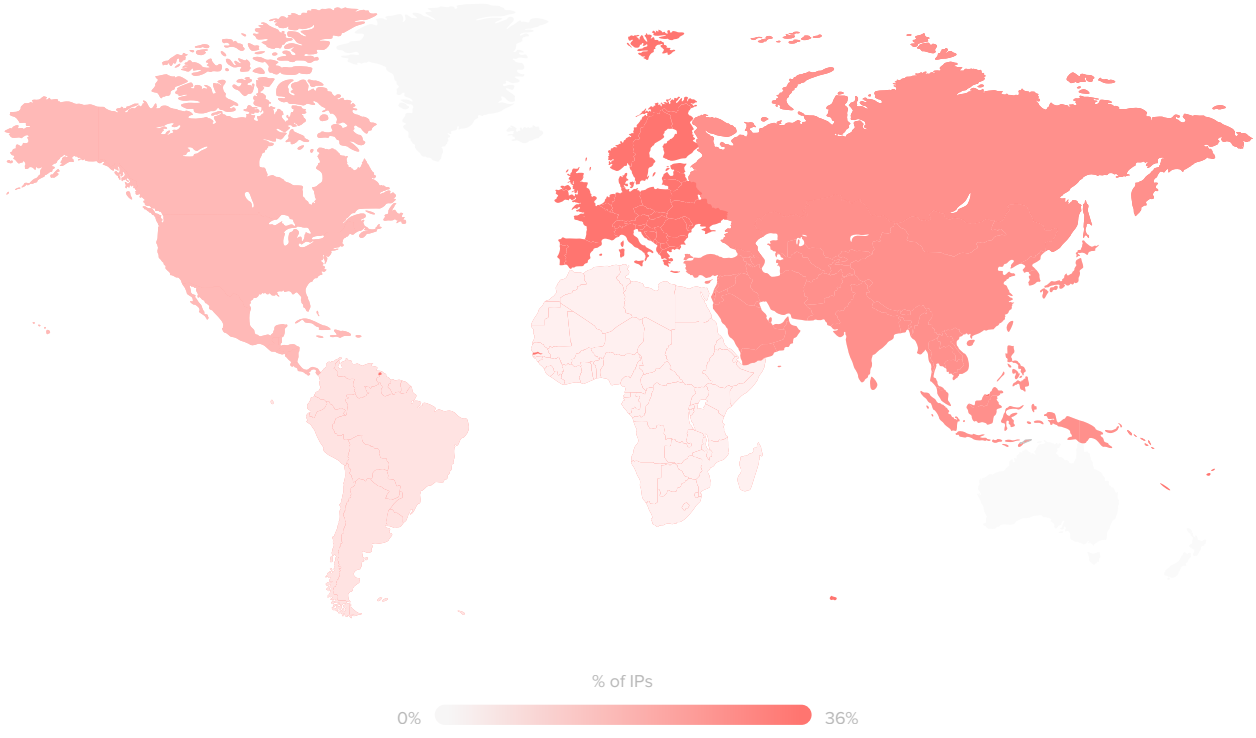
Attacks With Open Source Threat Intel

One way to slice the data is to compare the attacks on the cloud authentication layer with intel from open source threat feeds. According to our data, 47% of the threat actors that were involved in the attacks we see have hits on open source threat intel, meaning the security community was already aware of that IP as a possible threat. Of this group of "flagged" threats, we see the majority (67%!) coming from China. Russia, the US, and France have the next largest percentage of attacks, at 3% each.



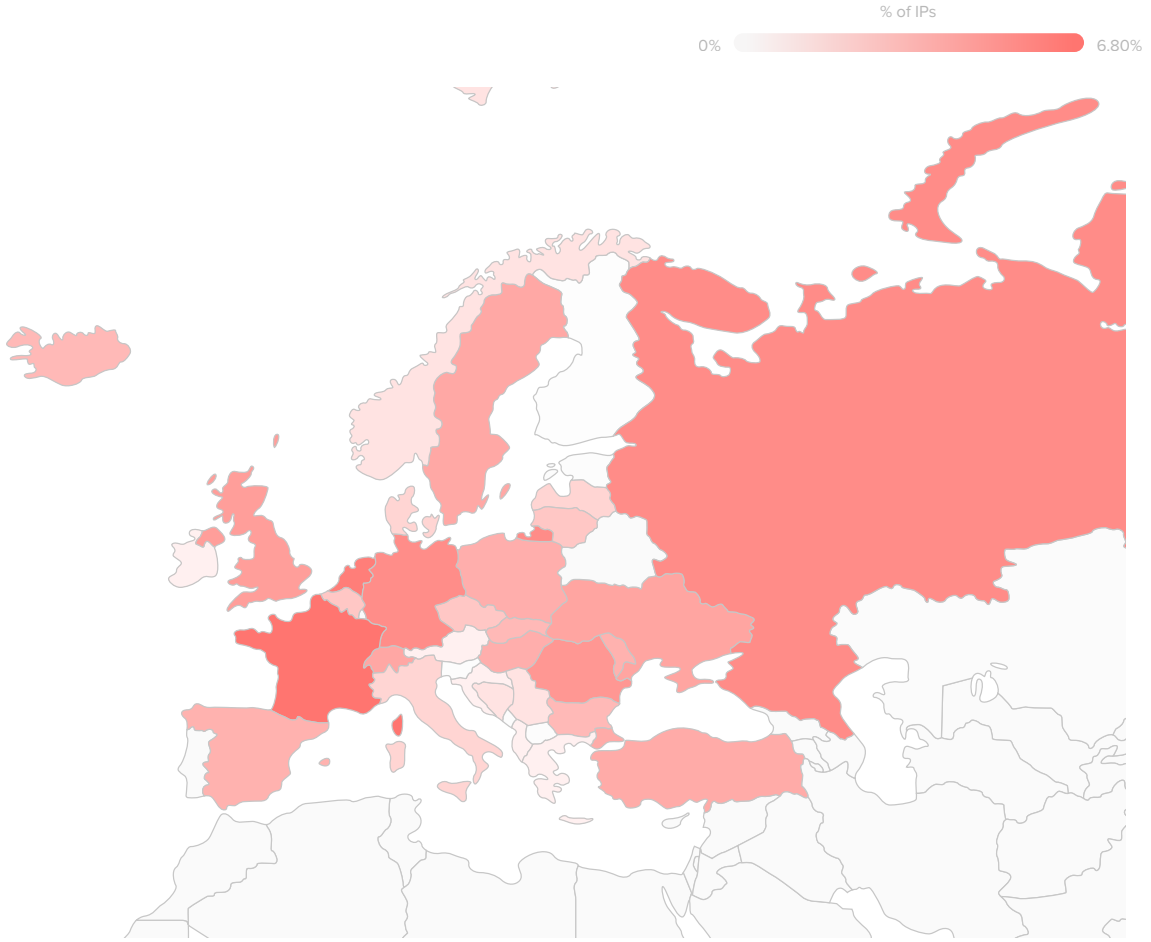
Attacks Without Open Source Threat Intel

53% of global threats we see do not appear on open source threat feeds. While we still see 35% of these threats originating in Asia (specifically 21% in China), the largest percentage of these originate from countries in Europe at 36%.



Attacks that do not Appear on Open Source Threat Intel - Europe

Of these European threats that do not have open source intel, we found that the threats originated from IPs geolocated across 33 different European countries. 19% are from France, 12% from the Netherlands, 11% from Russia, and 10% from Germany. The remaining 48% come from the rest of the European nations.



So what does the threat landscape tell us? Cloud services are getting attacked—a lot. And these cloud attacks are not evenly distributed throughout the world. To better protect themselves, organizations should conduct their own security detection and monitoring, and leverage threat feeds from multiple sources (both open source and paid). Furthermore, if organizations aren't anticipating any business will come from dark web or certain higher risk geographies, they should attempt to block them.

How effective are password policies at protecting against online credential-based attacks?

Threats are coming from everywhere, and are heavily targeted at user credentials. According to the **Verizon Data Breach Investigation Report 2017**, 81% of all hacking-related breaches leveraged either stolen and/or weak passwords. Even though many businesses deploy additional security tools, passwords remain one of the principal means of defense—and areas of weakness, if not employed well. So, we wanted to look at the effectiveness of the current state of password policies. In other words, how are organizations using passwords to protect assets, and how are users contributing to organizational security?

Because all passwords stored in Okta are encrypted, we (rightly) can't analyze them. We can, however, see the various password policies that organizations have put in place. To better understand how our customers approach strong passwords, we reviewed the common set of password policies our customers are enforcing.

Today, the typical organization in the Okta Identity Cloud enforces the following password policies:

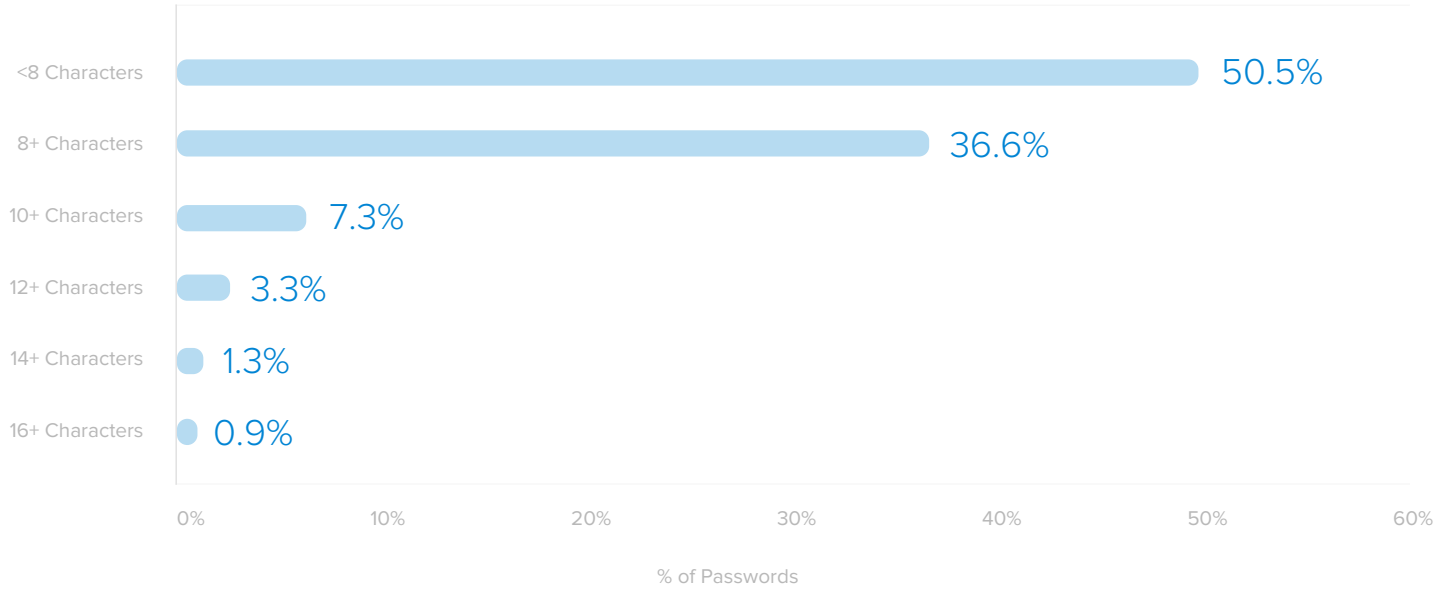
1. A minimum length of eight characters
2. At least one lowercase letter, one uppercase letter, and a number
3. A maximum of ten password attempts before locking a user out of his/her account
4. Recovery tokens expiration period is set at one hour
5. Prohibit any password that includes the username

We know how companies are approaching strong passwords. But do these policies make a difference? How do policies impact user choice?

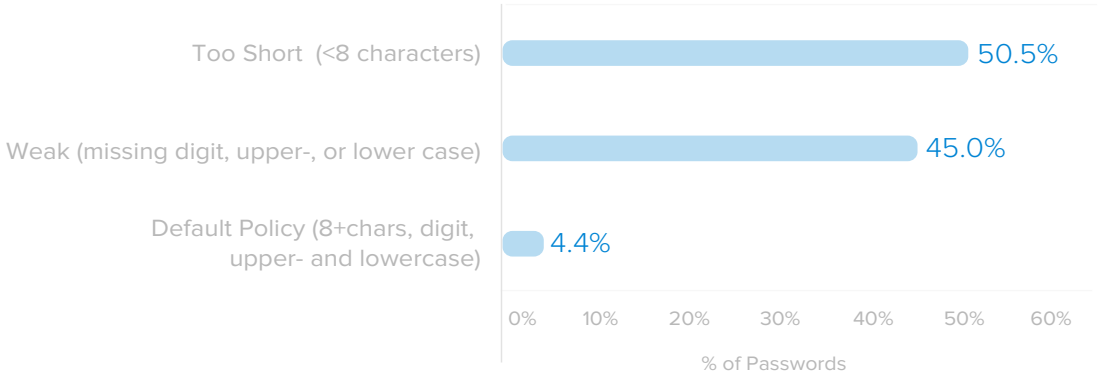
Because we (rightly) cannot see user passwords in Okta, we checked a representative sample from a breached password list[4] against the average policies in use by Okta's customers. We found that only 49.5% of those passwords used at least 8 characters. We also found that only 4% of the passwords would meet the average policy of more than 8 characters and at least one uppercase letter, one lowercase letter and one number.

4. The exposed password list used in our analysis originated from multiple sources including consumer websites, and does not necessarily represent enterprise-managed password policies alone.

Password Strength Based on Character Length



Password Strength Based on 8 Characters and at least one uppercase letter, one lowercase letter, and one number



We can clearly see the impact that policies have on users' password choices. When given the option, users often choose shorter passwords. But the real money question is: does password complexity equate to increased security? With **NIST's** updated recommendations saying complexity is better achieved by length than additional symbols, should companies change their password policies? Or more simply, is the current average policy complexity good enough to mitigate online credential-based attacks?

There are three common tactics used to obtain credentials: credential phishing, password spraying and brute force attacks. Credential phishing we've all heard of, and probably received emails with a "**security alert**." In a phishing attack, the attacker pretends to be a trusted user, website or organization with the goal of tricking another user into sharing their credentials. In a password spray attack, attackers use common passwords (i.e. password123) and "spray" them across many domain accounts or domains using a cloud service, essentially playing a game of guess and see, with the hope of one working. Brute force attacks are a more extensive version of a password spray that we see far less often; they use a scripted computer algorithm to attempt to guess passwords.

Does the policy help mitigate these types of attacks?

With the average Okta policy based on the alphanumeric, case-sensitive set of 62 characters (A-Z, a-z, 0-9), we calculated the total number of password combinations possible across those characters. To cut right to the mathematical result, the number of combinations would be 62^8, or 2.2E+14. Assuming a purely online threat vector, and allowing for a rate of 1,000 requests/second, it would take approximately 70 centuries (yes, that's 7,000 years) to try every possible character combination as a password based on the average policy. When we run the same computation across the entire 255-character ASCII (American Standard Code for Information Interchange)[5] range, with the same assumptions, we calculate 7,000 centuries, or 700 million years to try every character combination of an 8-character password.

But, the reality is, attackers also know that an exhaustive brute force attack isn't their most effective course. That's why they employ more **sophisticated strategies** like first adding special characters at the beginning or end of a password. And because hundreds of millions of passwords that have been exposed in past breaches are available online, attackers are able to attempt to login using these previously used and common passwords (**i.e. password or password1**) across many accounts. Furthermore, attackers are able to successfully compromise accounts by capitalizing on bad habits like adding special characters at the end, including usernames in passwords, or adding uppercase characters at the beginning, and making just enough attempts to remain any lockout thresholds.

It's imperative that organizations take steps to weed out bad passwords, including those that have already been exposed through a previous breach. Resources like HaveIBeenPwned.com allow companies (and their users) to see what passwords have been exposed. Vendors should offer the capability to prevent using common passwords.

Despite the increasing sophistication in **password guessing algorithms**, organizations can still minimize the risk of both brute force and password spraying attacks by (1) increasing the minimum password length and optional complexity and (2) enforcing policies that rule out common/breached passwords, and (3) enforcing MFA on all logins.

5. ASCII (American Standard Code for Information Interchange) is a system of character encoding used in most forms of electronic communication.

How does that compare to NIST's length requirements?

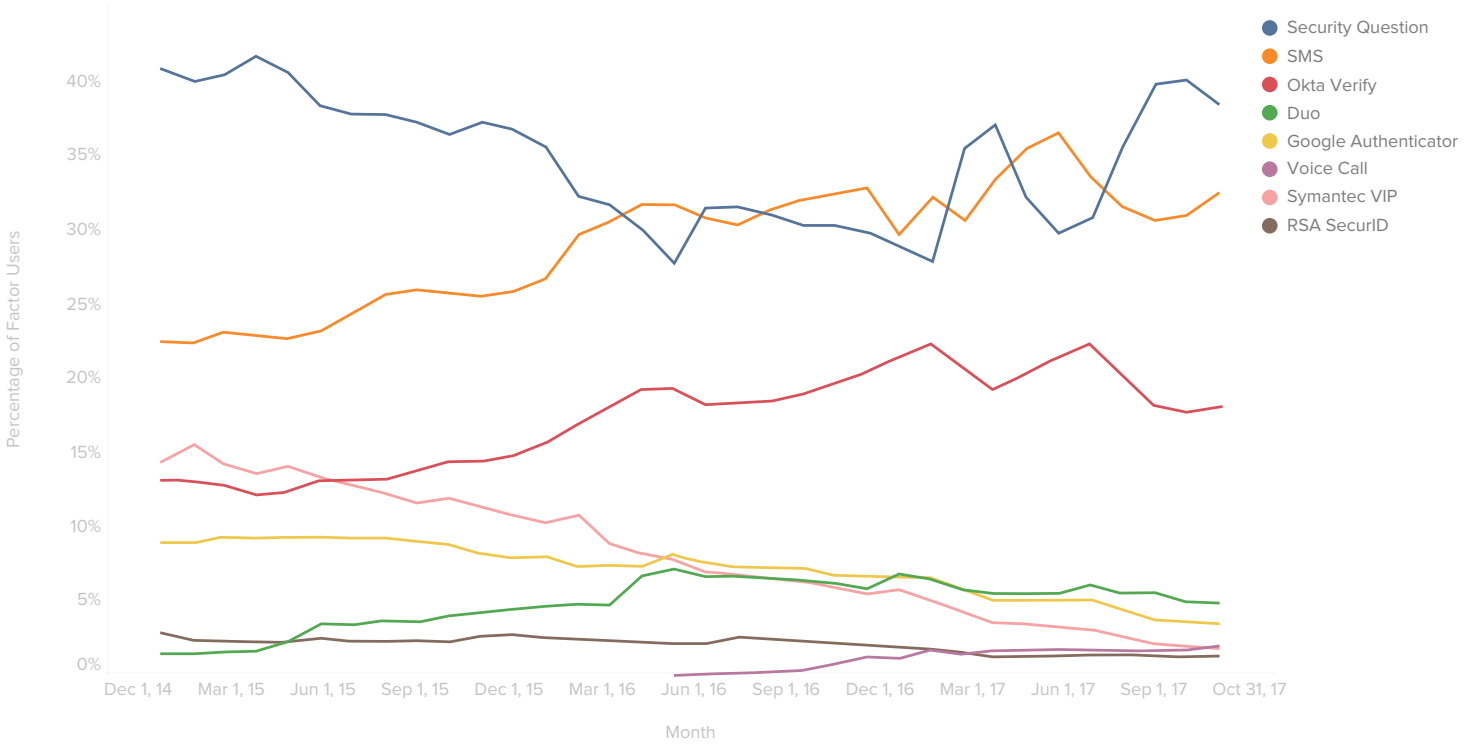
NIST guidelines requires a minimum length of 8 characters (consistent with the average Okta customer password policy), and also encourages increasing security by increasing password length, rather than alternate character types. And what we've found in our analysis shows that while strong, smart password policies are a start, they're not a silver bullet—and they're not going to help at all if you've given over your credentials through a successful phishing attack. As NIST also recommends when it comes to credential protection, one of the most secure ways to effectively mitigate all credential-based attacks is by combining strong password policies with MFA.

What are the most popular verification factors?

Passwords alone are not the best way to secure your data. More than ever, having a second factor is critical. MFA adoption among Okta's customers continues to grow. And, while the security question and SMS (two of the least secure factors; check out Google's research on the former **here**) were converging in our last Businesses @ Work **report**, the security question has emerged as the clear favorite in our network this year. (For now...)

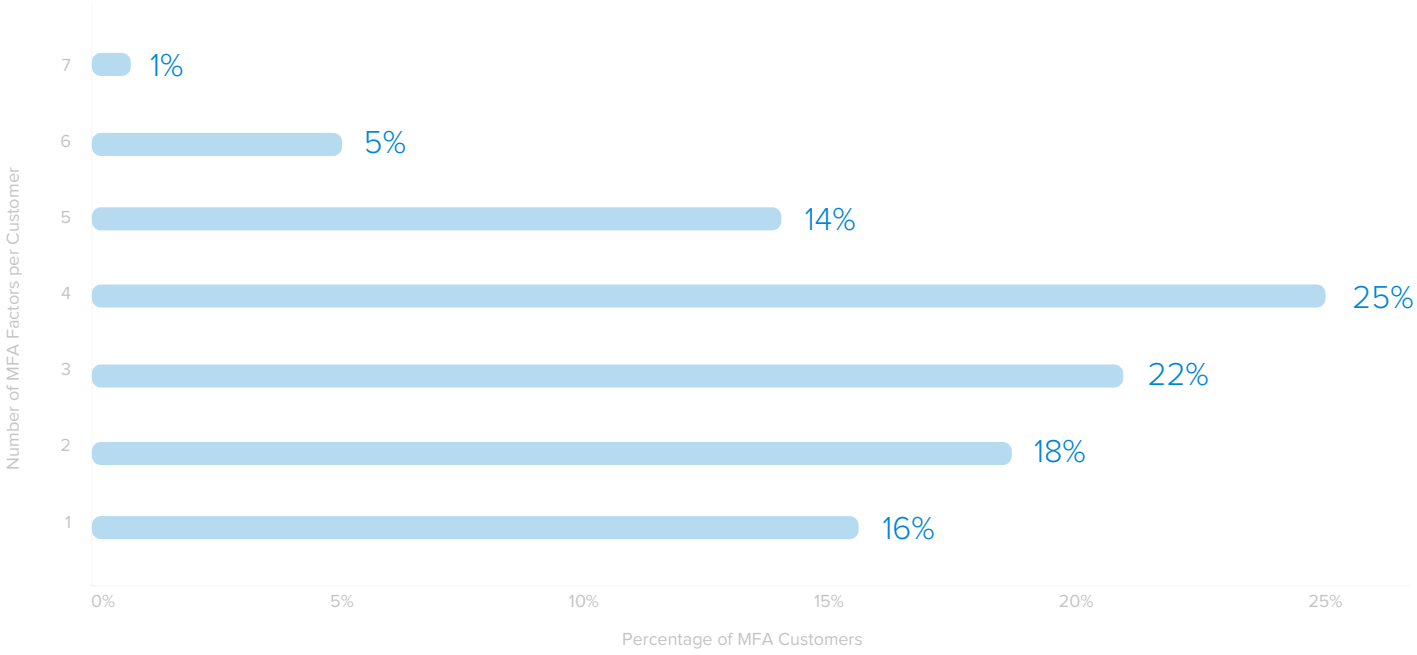
Our data also shows that, increasingly, enterprises are balancing their needs for MFA with end-user experience. One way they are doing this is by providing end-users with factor choice. The average number of factors deployed by customers with MFA continues to rise, with nearly 70% of customers offering their users 3 or more factors today (compared to 62% last year).

MFA Trend



MFA certainly is a critical piece of the security puzzle, but it's not the only piece.

Number of MFA Factors per Customer



Note: As of October 31, 2017

The policies set around MFA are essential. Organizations should require all privileged system users to use MFA, and every user account should be protected by MFA. In addition, access to critical apps should be prompted for a second factor, and organizations should leverage MFA automation based on user context to further mitigate risk. They should consider using certificate-based device trust to determine whether a device is managed or unmanaged by their IT team, and leverage this state to determine whether step-up is required or if access is allowed at all. And, they should require MFA when a user is attempting to mask their IP address through an anonymizer such as Tor or a proxy service.

Ultimately, organizations need to take action to stop the 81% of hacking-related breaches that involve compromised credentials. To improve their overall security posture, companies should:

- Use internal, open source and if possible, commercial threat intel to properly monitor services and update authentication policies as needed to mitigate the latest threats.
- Allow end-users to choose only the most secure MFA factors, and remove security question and SMS as factor options deployed to users. (In July 2016, NIST **discouraged the use of SMS as a second factor because of the high risk of intercepting passcodes**.)
- Enforce best practices in setting policies. For example, given that we see Tor exit nodes being used for attacks, deny access or enforce MFA for anything coming from Tor.
- Use compromised and common password protection. This will help preclude end-users from using passwords that have been exposed in a breach and those most frequently used to conduct password spray attacks.


okta