

The Next Value Accelerator for IT

Securing Distributed Work with Modern Identity



okta

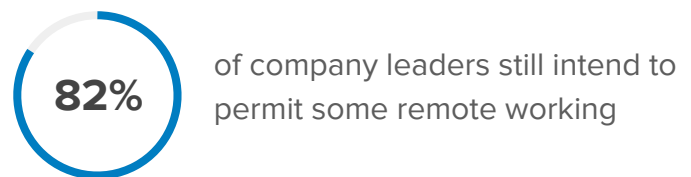
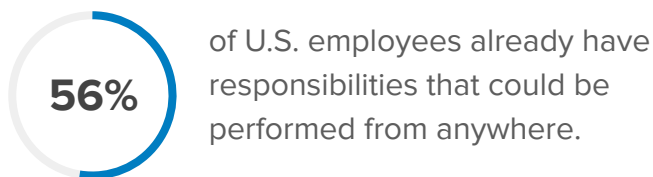
Table of Contents

The current state of workforce technology	3
Distributed work: IT's next frontier	4
Barriers to maintaining resilience amid uncertainty	5
Shifting business continuity and security priorities	6
How to protect and enable workers, wherever they may be	7
Stages of distributed work IAM maturity	
Stage 0: Gradually migrate traditional work environments to the cloud	7
Stage 1: Rapidly enable secure remote work	8
How to build a best-of-breed environment for productive remote work	8
Stage 2: Enhance productivity for your distributed workforce with IT automation	9
FedEx secures its remote and essential workforce during pandemic	9
Stage 3: Embrace zero trust access rooted in identity	10
Ensure rapid time-to-value and agility with Okta	11

The current state of workforce technology

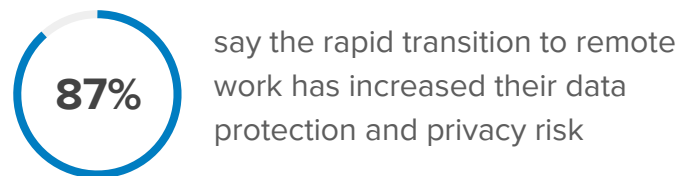
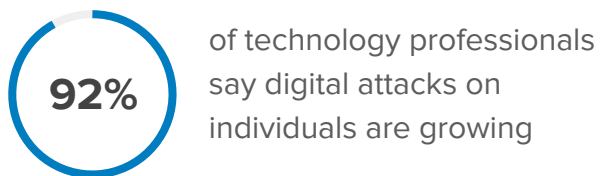
The COVID-19 pandemic has created several new difficulties for global workforces and brought many existing challenges into sharp relief. For the first time, tens of millions of people are suddenly working in relative isolation amid [varying circumstances](#). They might be at their primary or secondary home, caring for parents or children, or even on a road trip. To survive the aftershocks of coronavirus, companies have no choice but to embrace new techniques for productivity, connectivity, and security—and to do so quickly.

Global Workplace Analytics notes that [56% of U.S. employees](#) (that's 75 million workers) already have responsibilities that could be performed, at least in part, from anywhere. According to Gartner, [82% of company leaders](#) still intend to permit some remote working as employees return to the workplace post-pandemic. Perhaps unsurprisingly, [IDC's May 2020 Tech Index](#) noted that, despite budget cuts, IT demand is rising for the technologies required to support distributed workers, with top priorities being cloud, security, and workforce/employee tools.



This reality, of course, has major implications when it comes to protecting your users, applications, devices, and data. It's accelerating the erosion of traditional network perimeters, and contributing to a rise in cyberattacks, especially [phishing](#). According to the [ISACA](#), 92% of technology professionals say digital attacks on individuals are growing, and 87% say the rapid transition to remote work has increased their data protection and privacy risk.

But COVID-19's impact isn't all doom-and-gloom. In fact, companies that can successfully overcome all of these hurdles in the short-term will be poised to gain significant long-term business value.



Distributed work: IT's next frontier

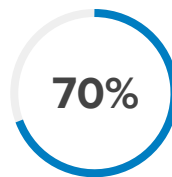
The silver lining in all of this is that forward-thinking CIOs and IT teams are recognizing they face a once-in-lifetime opportunity to elevate their role in the organization by delivering crucial results fast. As we navigate continuing waves of the current pandemic—as well as ripple effects that will surely persist long after we contain the virus—the technology function will either be perceived as a business blocker or an enabler. This is why it's important to think beyond just how to support your newly distributed workforce today.

According to McKinsey, more than [90 percent of global executives](#) expect COVID-19 to bring fundamental changes to their companies, and experts forecast that over [25 million U.S. employees](#) will regularly work from home within the next two years. This has the potential to help enterprises tremendously, since [70% of managers report the same or better work performance](#) since widespread quarantine began, and a typical employer can save an average of \$11,000 per half-time remote worker each year—thanks to increased productivity; reduced turnover, absenteeism, and real estate costs; and being able to continue working in the event employees can not get to work.

In addition to these workforce performance improvements and cost savings, providing secure remote access drives several other mission-critical benefits. For instance, it acts as an accelerant to digital transformation timelines, clearing the deck for you to laser-focus on projects that might have been on the backburner for years. Now that these initiatives are an imperative rather than a nice-to-have, you can get the top-level support you need to transform the business in new and innovative ways. By honing IT priorities, this new (not-so) normal will help teams dramatically boost agility and take big leaps towards powerful zero trust security strategies that deliver lasting impact.



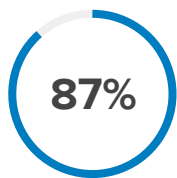
90% of global executives expect COVID-19 to bring fundamental changes to their companies



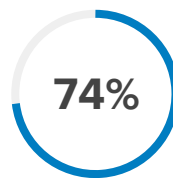
70% of managers report the same or better work performance since widespread quarantine began

Barriers to maintaining resilience amid uncertainty

Naturally, opportunities like these don't come without some challenges. Across the board, IT teams are under intensifying pressure to enable new ways of working while protecting a shifting security perimeter. The move to teleworking requires additional tools that you must deploy rapidly. That's why [87% of global IT decision makers agree that COVID-19 will cause their organizations to speed up migration to the cloud](#), and 74% believe the vast majority of their workloads will be in the cloud within the next five years.



87% of global IT decision makers agree that COVID-19 will cause their organizations to speed up migration to the cloud



74% believe the vast majority of their workloads will be in the cloud within the next five years

In the short term, teams expanded VPNs to ensure employees had access to all of the business tools—both in the cloud and on-premises—they need to stay productive. However, network bottlenecks have caused problems. In the United States alone, VPN usage [soared 124%](#) in the first few weeks of the March 2020 shutdown. [Research amongst our own customers](#) breaks this down, showing that Palo Alto Networks GlobalProtect grew 94% in March over February, compared to 20% for that same period in 2019, and Cisco AnyConnect was close behind with 86% growth.

Unfortunately, [23% of global firms](#) say they're experiencing major disruption to network security, with 61% claiming VPNs have suffered connectivity issues. This also exposes new risks for IT to worry about, according to the [Cyber Infrastructure Security Agency](#), which advises,

"Many organizations have rapidly deployed new networks, including VPNs and related IT infrastructure, to shift their entire workforce to teleworking. Malicious cyber actors are taking advantage of this mass move to telework by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software."

Shifting business continuity and security priorities

Many of the IT changes that enterprises have made to accommodate business demands during the pandemic will most likely become permanent, and this is especially true for security improvements.



Only [51% of technology professionals and leaders are highly confident](#) that their cybersecurity teams are ready to detect and respond to the rising cybersecurity attacks during COVID-19.



Nearly [95% of security professionals](#) believe that COVID-19 increased the cyber threat to enterprise systems and data, with 24% saying this threat is critical and imminent.



Given this, it's not surprising that CISOs expect crisis-inspired security measures to remain [top budget priorities in the third and fourth quarters of 2020](#).



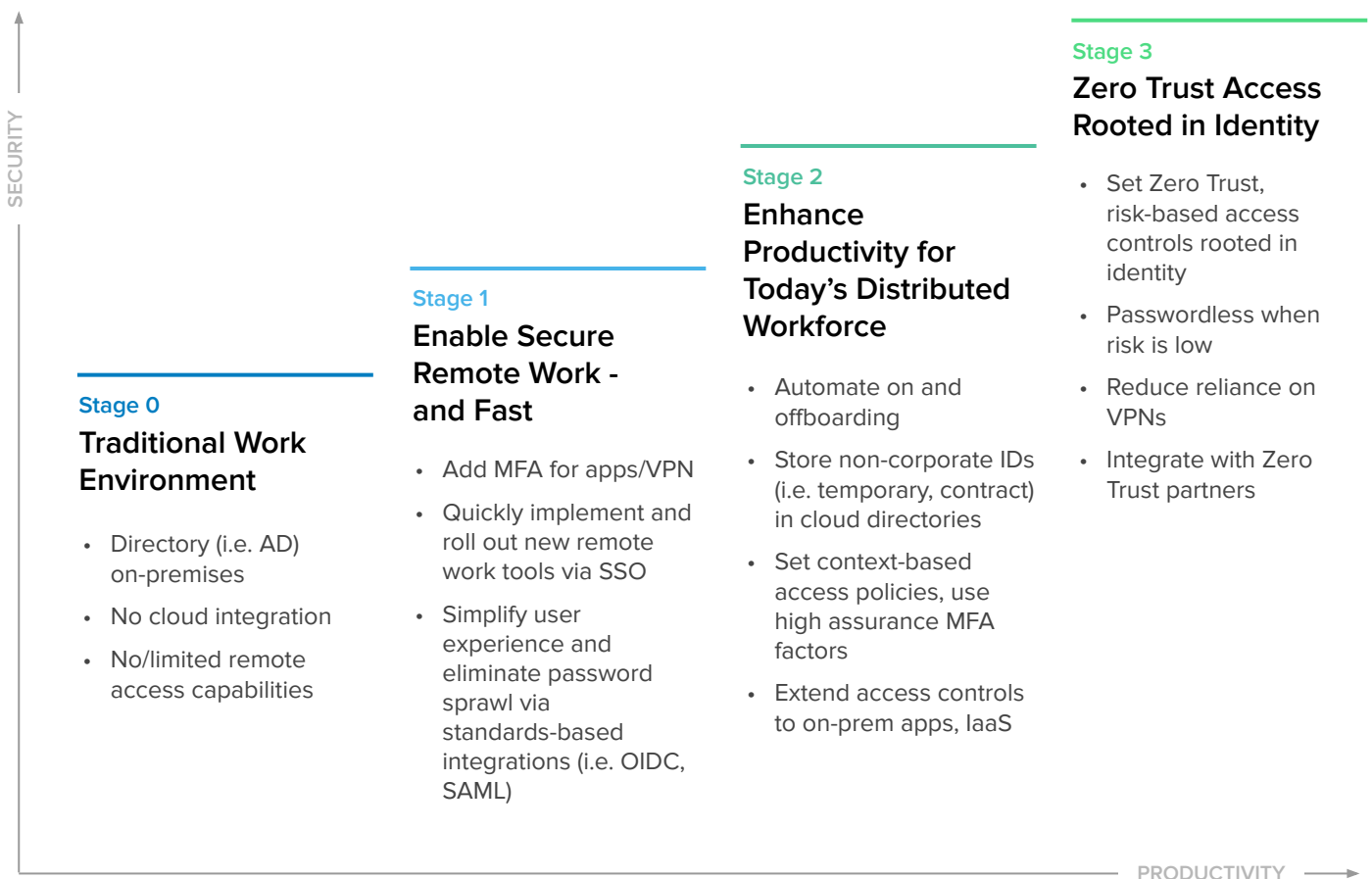
Increased information security spending has grown more common (from 15% in March to 28% of businesses in June) and organizations are spending more on information security tools (42%).

Of course, many that were late to the bring-your-own-device (BYOD) game are realizing that personal and professional device lines have blurred, so they must now embrace more flexible policies. Providing consistent, positive user experiences is crucial to support remote workers with many competing priorities and demands on their time. A recent study found that [69% of companies allow their employees to use personal devices](#) to perform their work, while a quarter also enable BYOD for contractors, partners, customers, or suppliers. These organizations say their main BYOD security concerns are data leakage, unauthorized access to data and systems, and malware infections.

How to protect and enable workers, wherever they may be

IT leaders know that having modern identity in place is a key lynchpin for securing remote work. As your company responds to stay-at-home orders and other pressures of the current pandemic, more and more stakeholders should be waking up to the potential value to be gained by expanding your adoption of identity and access management (IAM). In Okta's work with thousands of global organizations, we've observed four primary stages of maturity that IT teams reach as they strive to more efficiently empower highly distributed workforces.

Stages of distributed work IAM maturity



Stage 0: Gradually migrate traditional work environments to the cloud

Before the pandemic hit, many companies still relied on legacy on-premises user directories, such as Microsoft's Active Directory (AD). Some organizations at this stage have started to adopt cloud services or might even be midway through a cloud migration journey. However, those efforts are not quite fully baked or integrated with the rest of the hybrid IT stack yet. That's because most older approaches to identity lack integration with new cloud services, and only offer limited, if any, remote access capabilities.





















Stage 1: Rapidly enable secure remote work

In the spring of 2020, when governments around the world followed Asia's lead to implement shelter-in-place and other protective measures against COVID-19, global enterprises had to react fast. Every IT team's first priority became enabling secure distributed work in order to keep basic operations running, such as by extending their VPNs. Once they discovered the staying power of the pandemic, many businesses moved quickly to adopt new (usually cloud-based) collaboration solutions that helped their workers become more productive at home.

In parallel, some teams also added or expanded [single sign-on](#) (SSO) and [multi-factor authentication](#) (MFA) capabilities for existing apps. This allows organizations to provide safe access to best-of-breed productivity and communications applications like Box, Slack, or Zoom within a single, user-friendly portal—regardless of a user's device or location. As a result, they are both simplifying the user experience through one unified portal to access all resources, and eliminating password sprawl via standards-based integrations, such as OpenID Connect (OIDC) and Security Assertion Markup Language (SAML).

How to build a best-of-breed environment for productive remote work

Across Okta's customers, we've identified several of the [top technologies](#) that enterprises leverage to maintain a happy and productive distributed workforce.

okta	Productivity tools				
	Video conferencing				
	Document collaboration				
	Chat collaboration				
	Robust security platforms				
	Email security/bot detection				
	Workspace/device security				
	VPN access				
	Network security				

Stage 2: Enhance productivity for your distributed workforce with IT automation

As the dust settles from COVID-19's initial upheaval and organizations prepare for ongoing waves, the majority of IT teams should move into the next phase of the IAM journey if they haven't already. At this level, you're likely adding tools that will not just enable remote employees, but truly enrich what is becoming a "new normal" of dynamic work. To do this efficiently, you'll need to leverage automation across your identity processes.

Some key steps to take during stage two include:

- Look for ways to reduce manual, error-prone on- and off-boarding tasks, so you can get employees up and running fast.
- Enable self-service password resets and other services that reduce the burden on your help desk.
- Use low-code or no-code tools (e.g., [Okta Workflows](#)) to free up your developers and automate processes that are complex or unique to your enterprise.

Smart teams use the flexibility of cloud computing to adjust quickly as their business needs fluctuate. For instance, by storing non-corporate identities (such as those for temporary or contract workers) in cloud directories, you can more easily scale up and down amid today's uncertain landscape, or for seasonal requirements, future contractor or partner needs, and more.

Stage two is also a good time to rethink secure access for your global workforce, and adopt a more unified approach across cloud and on-prem apps. Your goal should be to ensure the right users have access to only the resources they need, and at the right time. You should:

- Set context-based access policies that utilize risk signals such as device and geolocation, rather than relying primarily on corporate network context.
- Extend access controls to your on-prem systems, infrastructure-as-a-service (IaaS) platforms, or APIs.
- Protect against credential-focused attacks like phishing with adaptive MFA.

FedEx secures its remote and essential workforce during pandemic

As [FedEx](#) moved to enable remote work for office workers and adapt quickly to the growth in customer demand due to COVID-19, its IT team sped up their planned deployment of the Okta Identity Cloud. This allowed them to retire a "spaghetti" IAM infrastructure made up of several different legacy point solutions—including on-prem MFA, federation, and web access management (WAM)—which was adding friction for software developers who were supposed to be focusing on cloud-native IT renewal, as well as for end users.

With Okta, more than 85,000 team members were able to securely access the company's VPN on the first day of work-from-home. Within 36 hours, FedEx also rolled out SSO and MFA so employees could access the over 250 cloud technologies they needed to be successful, such as Microsoft Office 365, ServiceNow, Zoom, and Salesforce. Not only did the organization rapidly move from stage zero to stage one of distributed work IAM maturity, they laid a solid foundation for zero trust in preparation for stages two and three.

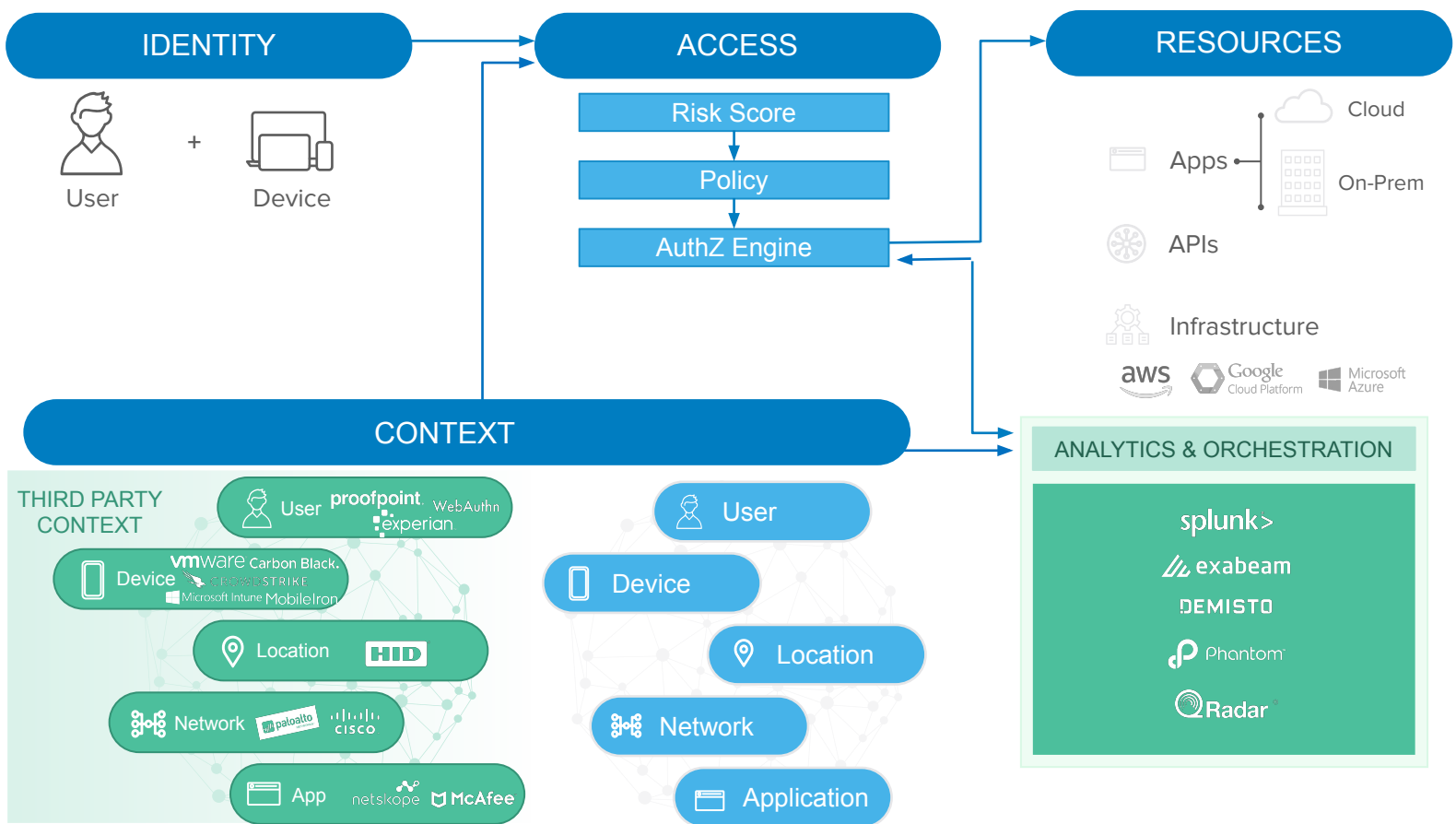
"Zero trust security at FedEx is really about doing user validation and marrying that up with device validation. Instead of using a username and password, we take that a step further and validate the user with push notification and device context. Is the device joined to our main Active Directory domain? Is it managed by our Workspace ONE MDM? And then we use that to make a decision on how to tailor the sign-in experience when they log in to FedEx applications and resources."

— Trey Ray, cybersecurity manager, FedEx

Stage 3: Embrace zero trust access rooted in identity

As the FedEx example demonstrates, stages one and two help to establish the essential infrastructure for your long-term zero trust security strategy. When you're ready to head down this path, look for ways to enhance risk evaluation with identity as the cornerstone. Integrate your modern IAM platform alongside other key security technologies to improve security posture and ease-of-use.

A robust zero trust strategy allows you to balance security with usability—and by better understanding risk, you can also make experiences easier for end users, even enabling passwordless login methods when risk is low. Another helpful approach is connecting Okta to a Zero Trust Network Access (ZTNA) tool like Zscaler and gradually reducing your VPN reliance.



Identity as the foundation for a modern, zero trust security strategy. For more information on leveraging Okta for zero trust, visit Okta.com/zero-trust.

Ensure rapid time-to-value and agility with Okta

By using a modern identity platform like Okta as the foundation for your remote work strategy, you'll quickly get up and running to ensure business continuity and resilience as you speed time-to-productivity. In fact, most Okta deployments are up to 7x faster than other identity stacks.

A few of the top productivity benefits our customers love about Okta are:

- Seamless remote access to all resources—cloud and on-prem—from any device right from one streamlined Okta SSO portal.
- Accelerated app deployment, along with reduced help desk calls and tickets.
- Automated provisioning and deprovisioning for the entire distributed workforce with [Okta Lifecycle Management](#) and Workflows. This brings an added security boost by limiting the risks of latent or orphaned account access.

While increasing your IT efficiency and agility, Okta also allows you to shift your perimeter so you can mitigate remote access risk and protect access both today and tomorrow. Our approach to IAM helps enterprises ensure secure user access to all resources—not just cloud and on-prem apps, but VPNs, servers, and APIs as well—and integrate with other leading zero trust solutions. Over time, you might even decide to fully retire your legacy VPN as you adopt [perimeter-less zero trust](#) strategies that focus on context and insights, and make it easier for your developers to shift to cloud hosting and microservices models.

Learn how the [Okta Identity Cloud can help you securely enable remote work](#) with repeatable, reusable components that make it effortless to deploy additional identity features and continuously improve your security posture.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 8,400 organizations, including JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

Learn more at: www.okta.com.