okta

Cover Your Bases: Best Practices for Protecting Remote Work

Okta Inc.
Level 37, Ocean Financial Centre
10 Collyer Quay,
Raffles Place, Singapore, 049315

info@okta.com

The accelerated path to remote work

Before 2020, businesses across industries and regions were already navigating a gradual, but important shift towards remote work. However, the remarkable circumstances caused by a global pandemic have accelerated this process, forcing organizations to quickly revisit how their employees access the tools and resources they need to do their work.

Around the world, companies and institutions have had to upscale their virtual private networks (VPNs), adopt cloud-based workplace applications at record speed, and make several rapidfire decisions to better enable their teams. But this sudden transition to remote work has raised an important question: how can we effectively secure our remote workforces?

To answer this question, it's important that we know the cyber security trends we're dealing with. First, many organizations lack the infrastructure to effectively secure connections from remote home networks—which are likely not secure and exposed to potential threats—and personal devices. In addition, cyber criminals have capitalized on the pandemic, targeting insecure networks, deploying ransomware, and conducting themed phishing campaigns. In fact, between February and March 2020, targeted spear phishing attacks rose 667%. Where traditional security focused on building a hardened corporate network and trusting anyone behind the firewall, the new requirements for a large remote workforce have put a spotlight on the need for modern identity and access management (IAM) solutions that protect our workforces and resources.

At Okta, we weren't immune to the effects of the pandemic. While dynamic work has been a long-term goal for some time, our security team still had to find a way to enable a fully remote workforce in a matter of days—a massive tactical task. We had to be able to effectively secure access for our thousands of users while avoiding any obstacles to productivity.

In this whitepaper, we'll share the steps we took to protect our remote workforce and provide actionable security advice for those looking to secure their company as they continue to explore this new era of remote work. Let's get started.

Protecting our identities: What we did and how we did it

As organizations across industries have moved away from traditional networks, security has become much more complex. Businesses that were once contained by a physical network perimeter are now having to account for their individual users, and the devices they use to access corporate resources. With more endpoints than ever before, companies need to employ a Zero Trust framework and support IAM solutions that authenticate users, deploy context-aware policies, monitor and manage devices, and so much more.

As the Okta security team, we know employees are the first line of defense when it comes to protecting our company and customer data. So when we were faced with growing our remote workforce from 30% of employees to 100%, we put this knowledge to practical use. Operating with the tenets of Zero Trust and employing the core features of the Okta Identity Cloud, we were able to accommodate this new, fully remote workforce in a matter of days—without compromising our security. We supported our users by securely connecting them to their work and each other, and kept our IT and security teams in control throughout the process.

Now, we want to share the lessons we've learned. From prohibiting access from unknown devices and making authentication easier, to creating safe environments for digital events, here are six things we've done that you can adopt at your organization.

Remote work checklist

- [ ] Contextualize access management
- [ ] Simplify authentication
- [ ] Enable remote incident management
- [ ] Refine remote onboarding
- [ ] Revisit employee training
- [ ] Invest in home offices

1. Contextualize access management

Defining who—and what—has access to your resources is a core component of a modern IAM solution. As part of our strategy, we've used Okta's Device Trust feature to determine that users can only access high-risk corporate resources from their work laptops.

Device Trust makes it easier for your IT team to stay in control as it ensures that unmanaged devices don't have access to your resources, putting you in a better position to protect your sensitive data. It also allows you to minimize the friction caused by multi-factor authentication (MFA) prompts, as employees using trusted or managed devices can experience seamless logins—an ideal balance of security and usability.

Another opportunity here is to use your modern single-sign on (SSO) and MFA tools to determine access policies that are specific to a remote work environment. For instance, you can integrate your SSO with an endpoint management system to prevent access to high-risk data from unmanaged devices, or create policies that deny access or prompt for MFA when a user accesses your apps from an untrusted network. Conversely, you can use access policies to allow employee access to low-risk services with minimal friction.

2. Simplify authentication

Over the years, we've learned that it's important to keep security simple for employees. If your access policies are too complex or cumbersome, your users may try to bypass them, using tools that your security team hasn't vetted. That's why we've worked hard to make authentication experiences as seamless as possible, while still abiding by the Zero Trust premise of never trusting and always verifying our users.

To do this, we've adopted the following features, all of which you can embed into your security roadmap:

- **Adaptive MFA:** Combined with SSO, this added layer of security mitigates the risks posed by poor password hygiene—80% of security breaches involve compromised passwords. By analyzing each login request for location, network, user behavior, and more, it allows for seamless experiences in low-risk situations.
- **Biometrics:** "Something you are" factors like fingerprints and facial recognition are amongst the most secure forms of identity verification.
- **Passwordless authentication:** Modern passwordless solutions are threat-resistant and give you enhanced admin visibility and control.

While protecting your resources, these processes give your remote workforce uninterrupted access to the applications and data they need.

3. Enable remote incident management

In a fully remote environment, our security team had to take additional steps to protect against human error, fraud, and hackers, among other threats.

For example, when people work together in an office, it's easy for IT to monitor for potential threats and walk to an employee's desk to help. But a remote workforce means that's no longer an option, as your IT team is also working from home. In this instance, we suggest revisiting your protocols for security incidents. In our case, we relied on endpoint detection and response tools to investigate security problems—in real time—from a distance.

4. Refine remote onboarding

As companies embrace a new normal of remote work, they're having to revisit how they conduct core tasks—like onboarding new employees. At Okta, we've created processes that let us set up and deliver hardware to our team, without having to share data with outside vendors. This has ensured that we remain compliant with data security regulations.

Our Lifecycle Management tool has also been indispensable here. With automated user provisioning and deprovisioning, we can continue to ensure that our employees have access to all the workforce applications they need—regardless of where they're joining us from. And our communication tools, like Zoom and Slack, have been indispensable for setting up new employees.

5. Revisit employee training

Whether it's for our employees or our customers, education is a big part of what we do at Okta. During the transition to remote work, we've made a concerted effort to educate our employees on how to make safe, smart decisions while working from home.

Using our online learning management system, we hosted interactive sessions that encouraged questions and discussion. We also sent email updates to keep employees informed on any new or changing policies and shared important resources.

We've also seen a shift in focus in our security training. Instead of spending time on physical threats like tailgating, it's now more important to educate remote workers on how to secure their home environment. For instance, you can train your employees to use a clean desk policy, where they lock up their work materials when they're away from their desks.

When it comes to replacing interactive, in-person workshops, we suggest exploring interactive webinars or online speaker series to drive more engagement and discussions—it's been a rewarding challenge for us!

6. Invest in home offices

Supporting your employees as they build working spaces at home is important to keeping them engaged and productive. To help meet this mandate, we created a program that lets employees buy and expense the equipment they need to securely—and comfortably—work from their homes. This included:

- Software, hardware, and tools to set up their digital workstation
- Ergonomic desks and chairs, as well as extra monitors, to improve posture
- Screen shields to keep their work private

We've also recognized that some employees may not have the physical space they would normally have in an on-premises office—and might be working in a shared environment with partners or roommates who are also working remotely, sometimes with children. In these instances, you can consider making your work hours flexible, so that people can choose when they work around their other commitments.

Turn your vendors into secure partners

As our company adjusted to a fully remote workforce, its technology needs changed. Unsurprisingly, we noticed a steep rise in Zoom and Slack use (now used by 90% of our team, and often on mobile devices), but we also received more requests for app integrations and other solutions that would improve how we interact with our customers, and how they collaborate and interact with data.

This created a new challenge for our security team, as they're responsible for ensuring all digital services meet Okta's requirements. To help with this, we expanded the review stage of our procurement process and started looking at third-party vendors through a partnership lens. In other words, we built a security review into our procurement process so that we could effectively partner with our vendors. It also meant protecting our relationships with tools such as SSO.

Our pivot to secure partnerships was instrumental in helping transition our in-person events to the virtual world. Just three weeks into the pandemic we shifted our Oktane20 conference to become the all-virtual Oktane20 Live event. Our new partnership process not only secured our conference platform, but also protected our speakers, partners, and attendees.

For companies still determining what vendor risk management looks like in a remote work environment, we suggest adding a security step into your procurement process so as to ensure that adopting a new tool or service won't compromise your resources.

A cloud-first future for dynamic work

Okta was founded as a cloud-first company, and that's something we've maintained throughout our history. This aspect of our infrastructure made it much easier for us to respond to the sudden need for a fully remote workforce—but we know not all companies are in the same boat.

Most companies are at various stages of their journey to the cloud, operating in hybrid IT environments that balance cloud-based applications and on-prem systems. This often means that security and IAM protocols vary across these IT landscapes, and remote access to on-prem tools require VPNs, which are cumbersome for employees and have become appealing targets to cyber criminals looking to access corporate networks. With 74% of companies declaring that they plan to adopt permanent remote work plans following the pandemic, this needs to change.

The rapid and necessary shift to remote work has proven that cloud-native solutions are the future—and that it's time for businesses to move away from traditional, on-prem architecture. But moving to the cloud is a marathon, not a sprint. As you transition your systems and infrastructure, start by moving low-impact applications. This will allow you to understand the technical and security implications, while also determining how to best engage your employees as you adopt new technologies.

Above all else, keep security top of mind. As you move to the cloud and establish more connections to your remote workforce, make Zero Trust your guiding framework. Secure and enhance your authentication experiences with SSO and MFA, and extend these features to your on-prem applications with tools like Okta Access Gateway. You can also take security to the core of your operations, securing your cloud-native infrastructure and APIs with Advanced Server Access and API Access Management, respectively. This way, your teams will have the right level of access to your resources, regardless of where they are—and your proprietary data will stay protected.

How we work is always changing, but 2020 pressed the fast-forward button on the transition to remote work. As you navigate this shift, we're here to help by sharing our experiences and setting you up with the tools you need to effectively secure remote work.

To learn how Okta can help you better secure your remote workforce, get in touch. You can also start a free trial to see our tools in practice.

About Okta

Okta is the leading independent provider of identity for developers and the enterprise. The Okta Identity Cloud securely connects enterprises to their customers, partners, and employees. With deep integrations to over 6,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them 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.

Learn more at: www.okta.com


okta