Finding business continuity in the cloud:
How Takeda Pharmaceutical Company scaled remote access

Excerpted from Securing Remote Work – Safeguarding Business Continuity with Zscaler™ ©2020, all rights reserved.
For CISO Mike Towers, it was a merger — a very big merger — that propelled Takeda Pharmaceutical Company’s secure cloud transformation.

“We acquired Shire PLC in January 2019 and doubled the size of the company,” says Towers. Takeda’s Shire acquisition grew its workforce significantly. Towers found himself having to integrate an incongruous patchwork of network hardware technologies.

Finding help in the cloud for a “disjointed” network

Fortunately for its CISO, Takeda had begun rolling out Zscaler Internet Access (ZIA) in late 2018, ostensibly to secure employee internet egress via the cloud and provide employees with a better, more consistent user experience wherever they might be, and for whatever device they might use. But ZIA proved particularly valuable when Towers and his team were confronted with integrating what he calls a “quite-disjointed” network architecture.

“We had about 320 or so firewalls that were in local sites, regional sites, core sites, et cetera,” says Towers. “It was a very, very traditional on-premise network appliance-based architecture. That was the predominant way that the perimeter and the network design was instituted, developed, rolled out.”

The merger accelerated Takeda’s migration to the cloud: “We were ready to move toward a Zero Trust, user-to-destination type of model,” continues Towers. “We wanted to do that as quickly as possible and we standardized on ZIA. By doing so, we can displace our ‘next-generation’ firewalls.”

ZIA gave Towers and Takeda greater flexibility in enabling secure employee connectivity — for every type of worker, notably — via local internet breakouts.

“One of the things we are providing is an app-by-app type of approach to giving folks what they need and not having to over-provision access. With the combo of ZIA and ZPA, we’re much more flexible with what we can provide and since we’re running all our traffic through it, we know it can scale.”

Mike Towers, Chief Information Security Officer, Takeda Pharmaceutical Company
Towers points out that Zscaler's policy-based administrative controls help make Takeda more agile: “Seventy-thousand employees in 110 countries, but we had one policy,” he explains. “We can have the same policy regardless of where people travel, with a consistent experience whether you’re on-premise or off the network. When you think about challenging yourself to improve both user experience and better security, Zscaler allows us to do that because folks can be flexible.”

Deploying ZPA slowly…then very, very fast

In an industry built on research, Takeda Pharmaceutical Company relies heavily on internal development, and that requires extensive use of proprietary technologies, applications, and intellectual property. In the past, that dependence had slowed Takeda’s migration to the cloud.

Looking to a cloud future, Towers envisioned “a model of remote access for applications that have historically been on-premise.” He cites regulatory pressures and “machine proximity” for keeping resources in-house: “When you have a manufacturing plant or an R&D lab, there’s expensive equipment in those environments that require computers to run them. Those often have to stay on-premise, and we want folks to have access to those applications without having access to the full network.”

In 2019, Towers and team began rolling out Zscaler Private Access (ZPA) to deliver secure connectivity to internal resources, prioritizing its deployment by both application and user. Towers notes that Tokyo-headquartered Takeda — the oldest pharmaceutical firm in the world — is “values-driven,” and shifting to ZPA was a bit of a cultural change for the company.

Towers prioritized extending remote access and retiring VPN hardware. “Remote access historically has meant remote network access,” says Towers. “We no longer think that way.” ZPA changed the way Towers viewed VPN technology at Takeda: “Remote users are used to clicking on a VPN client to connect, but inherently, VPN is not about application access, but about network access. In our mind, this is more around the applications and the services folks need…and VPN really doesn’t do much because you’re coming into a network just to back out again.”

Towers had to reassess Takeda’s infrastructure, in particular its remaining use of VPN technologies in light of Takeda’s progress toward cloud transformation.

Today when he considers VPNs, Towers asks rhetorically, “What’s the point?” As he puts it, “We can provide that same level of assurance and control natively in the cloud. We want to remove as much friction as possible.” Zscaler helps Takeda remove that friction. Continues Towers, “ZPA allows us to have the application accessed without somebody having to ever think about whether they have to click some other window or some other emulation engine to get to it…We want to support that capability as quickly and with as little friction as possible.”

When working from home becomes the new normal

In early 2020, Towers and his team were progressing with a measured ZPA rollout at Takeda. And then the coronavirus outbreak hit. Like many multinational companies, Takeda saw its first operational impacts in China, where Towers notes branch offices were still using “legacy VPN infrastructure” on “dated network architectures that made application access and performance quite slow.” The solution? A “quick pivot to ZPA,” led by Towers and team.

But as the urgent need for employee remote access grew, Towers had to figure out how he and his colleagues around the world could sustain business continuity given such “unprecedented” challenges. “We’ve never had a situation where we have so many
Remote Access
Remote application access for users whose processes are historically on-premises (e.g., regulatory)

Cloud Workloads vs. On-prem
Focus on authorization and control, regardless of whether systems are on-premises vs. cloud workloads and applications

VPN Replacement
Aggressive removal of legacy VPN technology in challenging parts of the world

Fast User Experience
Making the experience more frictionless, given everything employees are dealing with at home (e.g., children not in school)

When working remotely means less hardware, not more
ZPA has enabled Towers and team to secure Takeda’s transition to fully-remote operations. As the company has adopted ZIA and ZPA, Takeda has achieved what Towers calls “significant cost savings” by retiring its firewall hardware. CISO Towers aims to get the number of corporate firewall appliances down from its high (320+) to just a dozen.

Takeda’s realized benefits with Zscaler aren’t limited to VPN and firewall hardware. After struggling with “a lot of niche point solutions,” Towers is now leveraging Cloud Access Security Broker (CASB) capabilities via Zscaler’s inline-proxy security architecture: “Zscaler can help us do more with CASB controls,” explains Towers, “and help us be smarter with the data, and make security decisions based on data, and because it’s in the cloud, and we’re already sending our traffic through it, we know that it will scale [and be operationally stable].”

As employees have shifted to local internet breakouts, Towers has been able to retire costly networks. “Ninety-eight percent of what [users are] going to is on the internet anyway,” he explains. “We can get rid of a lot of expensive WAN links.”

In the past two years, Towers and his IT team have had to adjust (much more adroitly than they could have imagined) to operational obstacles placed in their path. But though his company’s secure cloud transformation may be progressing at a faster-than-expected pace, Towers remains optimistic.

“What with the combo of ZIA and ZPA, we’re much more flexible with what we can provide and since we’re running all our traffic through it, we know it can scale,” concludes Towers. “This is a good time to be a security professional because you don’t have to worry about trying to balance user experience and security anymore. You can do both!”

People working from home,” he says. “You practice for widespread work-from-home quite regularly, but no one practices with everyone doing it at the same time when all their children and families are home.” Access was one thing, managing crowded bandwidth was quite another: “Every worker [at home] is competing with Netflix and Xbox from the kids at the same time, so performance optimization for internet access is something that we’ve had to focus on.”

Towers and team looked at how Takeda users work with internal applications. They shifted Takeda’s “control and provisioning approach” so users would be concerned with which applications they needed to get their work done, and not so much with where those applications might reside. “We don’t want to think that way anymore,” he explains, and now IT can instead provide “an app-by-app type of approach to giving folks what they need, and not having to over-provision access.”

Figure 6-3. CISO Mike Towers led Takeda’s (accelerated) initiative to enable employees to work from anywhere. He prioritized four objectives: remote access, VPN replacement, better user experience, and a focus on control (regardless of whether the system is on-prem or in the cloud).
About Zscaler

Zscaler was founded in 2007 on a simple but powerful concept: As applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.