Deloitte.

Trust, verify, grow.

A global pharma company wanted to service new markets with high cyber risk. But how?

Life Sciences & Health Care	Zero Trust
Industry	Solution

Cyber Stories

The situation

Imagine the ultimate set of velvet ropes: nobody's on the list. Never mind what happens in comic books; there's no such thing as an indestructible material. In the real world, even the most durable items are vulnerable to microscopic cracks that will, under the right conditions, expand and cause failure. Sometimes catastrophically. And more surface area means more vulnerability.

The same principle, as any chief information security officer (CISO) might tell you, applies to cybersecurity: a micro vulnerability—like a moment's inattention from an employee—can expand into a profoundly damaging data breach.

Every enterprise contends with this dynamic; one global pharmaceutical company decided to address it head-on. The company's surface area was already considerable—tens of thousands of employees; thousands of research and logistics partners and third-party service providers; plus, the patients, physicians, and other health care providers around the world that relied on them. Even so, there were emerging markets left unserved, and leaders wanted to expand accordingly.

This posed a considerable challenge: How could the company maintain the collaboration its current stakeholders enjoyed on its network, extend that access to *even more* stakeholders, and continue safeguarding its sensitive data? How could it prevent information loss when its employees and contractors traveled to these high-risk markets? And how could it do so while adhering to local cultural norms and business models, and complying with recent cyber laws and requirements?

The solution would require a complete rethink of the company's network architecture, with a coordinated program of security controls that could support growth in risky environments without compromising data. Therefore, company leaders reached out to Deloitte's Cyber & Strategic Risk practice.

Cyber Stories

The solve

As a concept, the Deloitte team proposed shifting the company's IT architecture to a [zero-trust](#) approach where every request to connect to the company's network would be treated as though it came from an unknown actor. It would be like having the ultimate set of velvet ropes: nobody is on the list, and everyone gets verified.

And when someone is ushered in, assigned seats only. Before, someone accessing internal applications could also access the company network; with zero trust, user access is compartmentalized through detailed, policy-based controls. Users can only connect to the resources they need in the moment. (Additionally, this approach also streamlines user experience. No more navigating multiple firewalls and VPNs.)

Insights to inspire

The concept looked great on paper, but would it work at the scale, complexity, and risk the company was contemplating? To test it out, the Deloitte team used a business-driven methodology for creating information security systems—the Sherwood Applied Business Security Architecture (SABSA) model—to design a reference architecture. This reference architecture laid out the company's current, interim, and future (zero trust) states, including plans for implementing an access control technology.

Informing the architecture from an IT perspective: a prioritized inventory of the company's global services, including dependencies for their migration from on-premise servers to the cloud, as well as the applications, sites, and countries considered particularly high risk. From a people perspective (and to achieve a cohesive architecture), the team helped align company stakeholders specializing in network services, identity management, information protection, privacy, enterprise apps, and cloud engineering.

(Side note: This is usually the part of the story where teams are blindsided by a global crisis—you know the one—and scramble to adapt. Not this story though. The pandemic only affirmed and accelerated the team's work. The shift to remote work and subsequent geopolitical turmoil cemented the company's decision to shift to zero trust.)
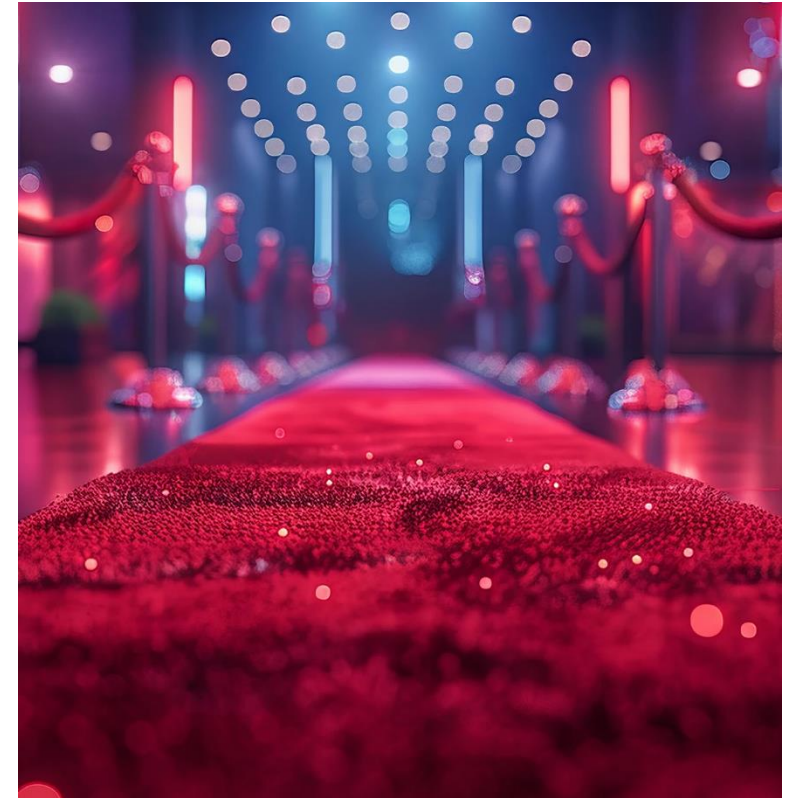
Cyber Stories

The impact

With zero trust, every request for access is suspect. In a way (and as noted), the company's zero-trust transformation was already demonstrating its value midstream and continues to do so today. Leaders have been provided a road map to achieve their target state and an executive dashboard to track achievements, risks, and risk reduction efforts. The velvet ropes are also in place: The access control solution successfully replaced the traditional VPN solution, with global users and servers migrated from proxy appliance-based internet access to cloud proxy internet access.

Whatever the future holds in the geopolitical sphere, the company's pivot to a zero-trust model should help further protect it from vulnerabilities (micro or macro), support secure growth, and enable the overall mission of service to continue. **Velvet ropes: in place. New markets: engaged.**

Cyber Stories

Trust, verify, grow.

Let's talk Zero Trust

How will your organization create a modern security architecture that allows your business to grow with confidence? Discover how Deloitte's worldwide team of industry-focused cyber specialists can help you identify new opportunities for value with a Zero Trust approach. Contact us to get the conversation started.

deloitte.com/cyber

Contacts

Chris Stanoch
Managing Director
Deloitte & Touche LLP
cstanoch@deloitte.com
+1 848 702 4513

John Lu
Principal
Deloitte & Touche LLP
jolu@deloitte.com
+1 609 658 3351

Miroslav Kral
Senior Manager
Deloitte & Touche LLP
mikral@deloitte.com
+1 347 673 4895

Lee-Lan Yip
Specialist Leader
Deloitte & Touche LLP
leyip@deloitte.com
+1 415 318 6140

Mark Adams
Specialist Leader
Deloitte & Touche LLP
markadams@deloitte.com
+1 571 424 3992

Haley Berner
Manager
Deloitte & Touche LLP
hberner@deloitte.com
+1 415 203 5136

Deloitte.

Cyber Stories