The need for zero trust: Three lessons learned from the COVID-19 pandemic

When much of the world left the office to work from home at the onset of the COVID-19 pandemic, few organizations were prepared to support this new way of working. Suddenly, many employees were working beyond the corporate perimeter, leaving security teams scrambling to keep their people and the businesses protected.

Within the first few months of this shift, 42%[1] of the US labor force was working from home full time. As a result, VPN usage rose dramatically in the early days of the pandemic as organizations sought out ways to give their workforce access to corporate resources.

However, where it was once thought of as a trusted layer in the enterprise security playbook, VPN technology has been shown to present challenges, including issues with scalability, performance, and a lack of granular control for user access. These challenges can be especially impactful for organizations that rely on an extended workforce consisting of contractors, frontline workers, vendors, or partners, where leveraging managed devices is not always possible.

The pandemic shed light on the fact that a new layer of protection would be needed to accommodate the wholescale shift that was underway. On the flip side, organizations that had already implemented a zero trust approach were able to scale secure access more easily at the onset of the pandemic.

Zero trust with BeyondCorp: A new approach

BeyondCorp Enterprise is a zero trust security solution by Google Cloud and was developed based on Google's own experience providing zero trust access to its workforce. Unlike solutions that focus on securing a network perimeter, a zero trust model shifts away from the notion of privileged networks. Instead, it is much more targeted, providing users with access only to those applications and resources they need to do their jobs, based on policies and their ability to validate their identity, device, and other contextual information deemed necessary by the organization.

BeyondCorp Enterprise leverages the Chrome browser, which allows organizations to quickly deploy and scale zero trust access.

[1] Stanford research provides a snapshot of a new working-from-home economy, Stanford News

Three key lessons learned

Implementing secure remote access can be a journey. As you begin your shift to a zero trust strategy, keep in mind how the following lessons can help you take a more modern approach:

A layered approach to security remains the best approach
Build security policies around identity and devices, not the network. A zero trust approach allows you to customize your policies and add additional layers to your security strategy as trends change and new innovations arrive.

Endpoint security is an imperative
Lack of visibility into user behavior can be a challenge for organizations with remote workers, so protecting the endpoint is critical. Measures like encryption must be in place regardless of user or location.

Protecting the extended workforce should be core to your security strategy
Frontline workers, contractors, and remote workers are typically located beyond the perimeter and are often working from shared or unmanaged devices. These user groups can be more vulnerable to threats, so securing their access to corporate resources is critical. This can be accomplished easily, by taking an agentless approach and leveraging the browser.

Enterprise security today and in the future

As we move forward from the pandemic, the shift to a zero trust security model is already underway for many. With the ability to grant secure access in a controlled manner, IT and security teams can provide both a secure and seamless experience for workers, from anywhere they choose to work.

Deloitte's industry-leading cyber practice works in collaboration with Google Cloud to provide end-to-end architecture, design, and deployment services to assist customers in their zero trust journey.

As the security landscape continues to evolve, organizations around the world are transitioning to zero trust for continuous end-to-end protection. Visit our website or contact us to learn more.

- **Philip Bice**
  Global Manager, Service Providers Partnerships and Channel at Google Cloud
- **Ryan Lee**
  Alliance Manager at Deloitte Services LP

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.