Zero Trust Access: 5 Critical Steps

The COVID-19 global pandemic has forever changed how we work. Today, 71% of the people who can work remotely are working from home. With so many people and devices now beyond the corporate walls — abolishing an established perimeter — zero trust access is critical to the security of your organization.

We recommend that you follow these steps to begin your implementation of zero trust:

1. Deploy endpoint verification
   During the pandemic, the proportion of cyberattacks using unseen malware or methods rose to 35%. Ensure visibility and access control by verifying all endpoint devices, managed or unmanaged.

2. Enable threat and data protection
   25% of employees noticed an increase in fraudulent emails, spam, and phishing attempts in their corporate email since the beginning of the pandemic. Protect your data and applications to offset the risk.

3. Develop a zero trust policy framework
   As with all security models, a policy framework sets the rules for users, the apps they can access, and how they can connect—ensuring clarity, security, and compliance across your organization.

4. Apply zero trust policies to corporate resources
   With enterprises on average using up to 1,000 cloud apps, it’s important to apply access policies and the framework you set across your entire app ecosystem.

5. Control access to applications, VMs, and APIs
   With every passing second, 75 records go missing worldwide due to cyber attacks. Apply your policies based on user identity, device health, and other contextual factors to control access to corporate resources.

Visit our website or contact us for more information.

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.

1 Pew Research Center, How the Coronavirus Outbreak Has and Hasn’t-Changed the Way Americans Work, December 2020
2 Cynet, COVID-19 Cyberattack Analysis report
3 Deloitte, Cyber crime – the risks of working from home
4 CIO.com: Enterprise on average use up to 1,000 cloud applications
5 Techjury, How Many Cyber Attacks Happen Per Day in 2020?

In collaboration with Deloitte’s industry leading cyber practice to assist throughout zero trust journeys, organizations around the world are empowering workers to be productive and secure from anywhere with BeyondCorp Enterprise by Google Cloud.