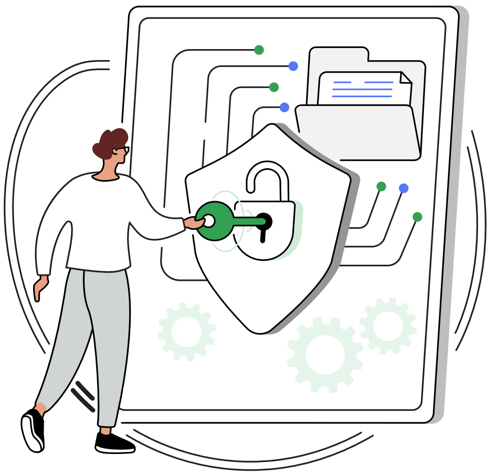
Google Cloud

Deloitte.

Securing your extended workforce with BeyondCorp Enterprise



Human error is responsible for 23% of data breaches. Given IT cannot control user behaviors, this statistic is worrisome.

The COVID-19 pandemic has magnified the risks with most people working outside of the office and beyond the corporate perimeter. Access to apps and data is no longer constrained within the data center and it's likely some active work devices are not corporate-owned.

Three use cases within your extended workforce, e.g., contractors, frontline workers, vendors, partners, and others, require the greatest care. Especially when shared or unmanaged devices are in the mix.

Frontline worker

- Retail, other public-facing roles
- Shares devices with co-workers
- Signs in and out as shifts change
- Needs access to select apps (e.g., point of sale systems)

Contractors / temporary worker

- Workers contracted from a vendor or hired temporarily
- Uses a device not managed by IT
- Needs access to select apps required for their work

Remote / BYOD worker

- Employees who travel, work remotely or within a BYOD environment
- Uses a personal device
- Needs access to a broad range of apps

These use cases present potential security risks, including to sensitive data such as customer payment info, records, PII, and intellectual property. It's also important to limit access by these workers to only those apps and infrastructure needed to do their jobs.

Zero trust with zero touch

BeyondCorp Enterprise provides an agentless approach to zero trust, leveraging the Chrome browser. It is easy to use, more secure, with a simple and straightforward deployment for well-defined user groups.

01

Deploy as a no-impact overlay to your existing security architecture

02

Target specific sets of users and applications and expand as desired

03

Reduce legacy access and network controls as deployment increases

The solution allows you to build protected profiles in Chrome to provide access and protection to your extended workforce. These employees can do their jobs safely and securely, with appropriate zero trust access to authorized resources—regardless if the device is managed by IT, an outside organization, or the individual. Workers can access critical apps and services securely, with integrated threat and data protection built right into the browser.

BeyondCorp Enterprise

BeyondCorp Enterprise is informed by Deloitte's industry-leading Cyber practice, working in collaboration with Google Cloud to provide end-to-end architecture, design, and deployment services to assist in your 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

[1] IBM, 2020 Cost of a Data Breach Report

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.