promevo™

Rethinking Enterprise Security With Google's BeyondCorp Enterprise

July 2023

promevo™

Agenda

Introductions

Promevo History & Overview

Current State of Enterprise Security

BeyondCorp Enterprise Demo & Key Features

Q&A

Today's Presenters

Brandon Carter
Marketing Director, Promevo

Alex Popp
Partner Development Manager, Google Cloud Security, Google

David Aulick
Practice Director, Infrastructure Modernization, Promevo

promevo™

With the expertise, agility, and commitment you can only get from a partner that is solely **100% Google-focused**, Promevo is with you every step of the way, enabling clients to have the best Google life experience possible

Engaged Across Entire Google Lifecycle

Google Products

- Cloud
- Workspace
- Chrome
- Maps

Engagement Models

- Sell
- Service
- Build

Certifications

- Google Certified teams for holistic support with 100+ Certifications

Specializations

- App Dev Svcs
- Cloud Migration Svcs
- Workspace Transformation for SMB

Promevo Runs on Google

chromeOS

Looker

apigee

Google Cloud

Google Workspace

Forming Partnerships that Matter

BRAINSTORM

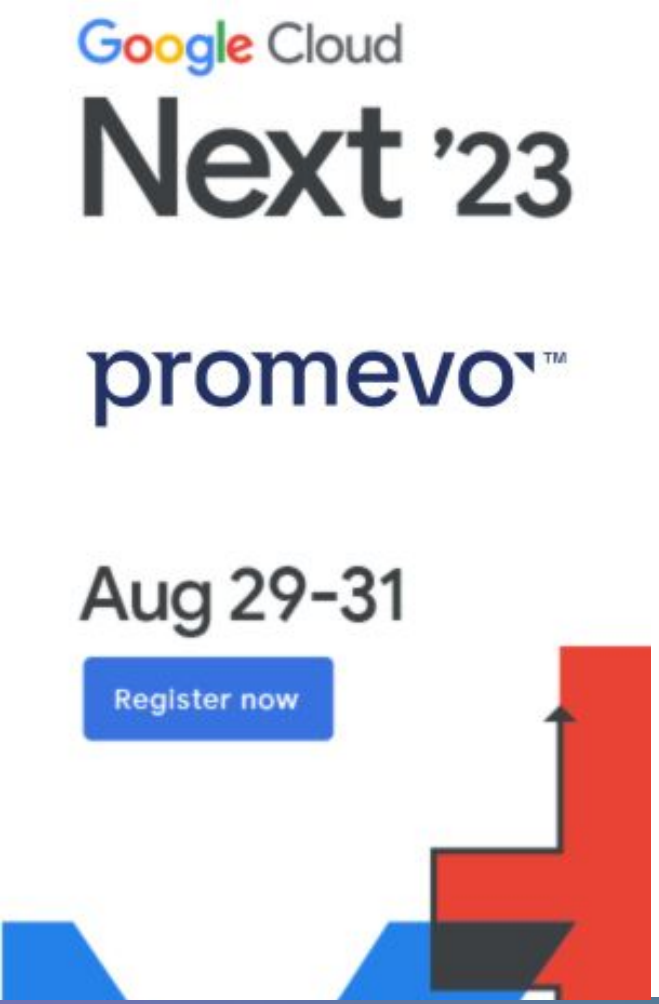
CAMEYO

promevo™

gPanel® Enterprise Launching Next Week

Introduction Webinar: August 15, 2023 1PM Eastern

promevo.com/gpanel/enterprise



Let's Meet up at Google Cloud Next!

Booth 1201

bit.ly/promevo-next23

promevo™

Current State of Enterprise Security

promevo™

The Modern Workforce: Browser Security is Critical

71% of workers are working from home or remote

84% of employees routinely use personal devices for work

71% of the time cloud workers spend on devices is in browsers or virtual meetings

promevo™

The Risks of Compromised Browsers

- Phishing remains the leading infection vector, identified in 41% of incidents (IBM)
- 2022 saw the highest average cost of a data breach in 18 years, with the cost rising from $3.86m to $4.35m (IBM)
- 54% say cyberattacks are too advanced for their IT team to handle on its own (Sophos)

Common Web Security Concerns

- Risks of browser extensions
- Not enough visibility into browser environment
- Lack of controls over browsers in an organization
- Data exfiltration
- Phishing and malware
- Unmanaged devices, contractors, remote workforce

Secure Enterprise Browsing

Security built into the browser

Customize policies to manage and secure your browser environment

Real-time protection against external and internal threats

Visibility into your browsers and potential web-based threats

Users can work productive and securely without interruptions

promevo™

Mitigate data exfiltration risks with data loss prevention.

Protect your corporate data while users work securely on the web, from anywhere and with any device.

Protect users with real-time phishing and malware protections.

Control access to your critical applications using zero-trust security.

promevo™

Live Look at BeyondCorp Enterprise

promevo™

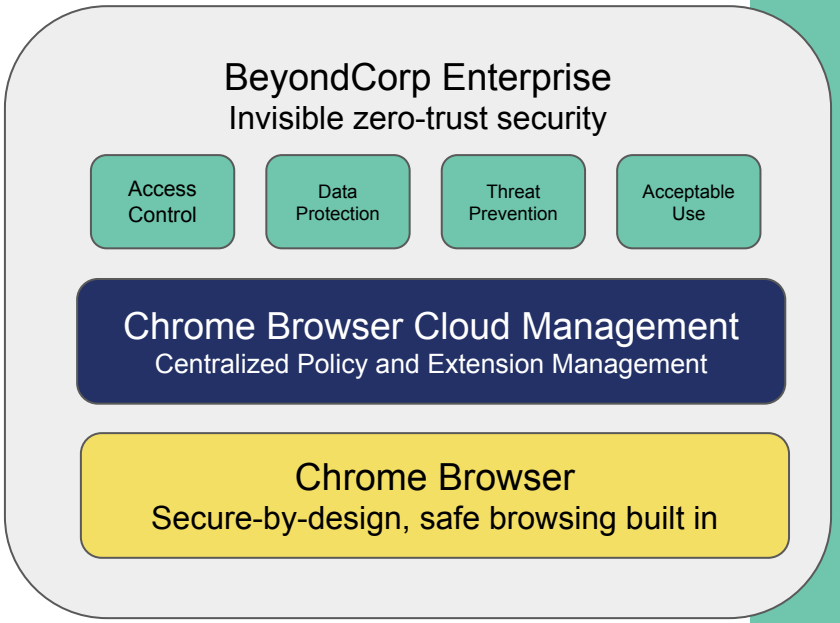
BeyondCorp Enterprise

BeyondCor
p Enterprise

promevo™

Secure Enterprise Browsing Starts Here

BeyondCorp Enterprise and Chrome Enterprise

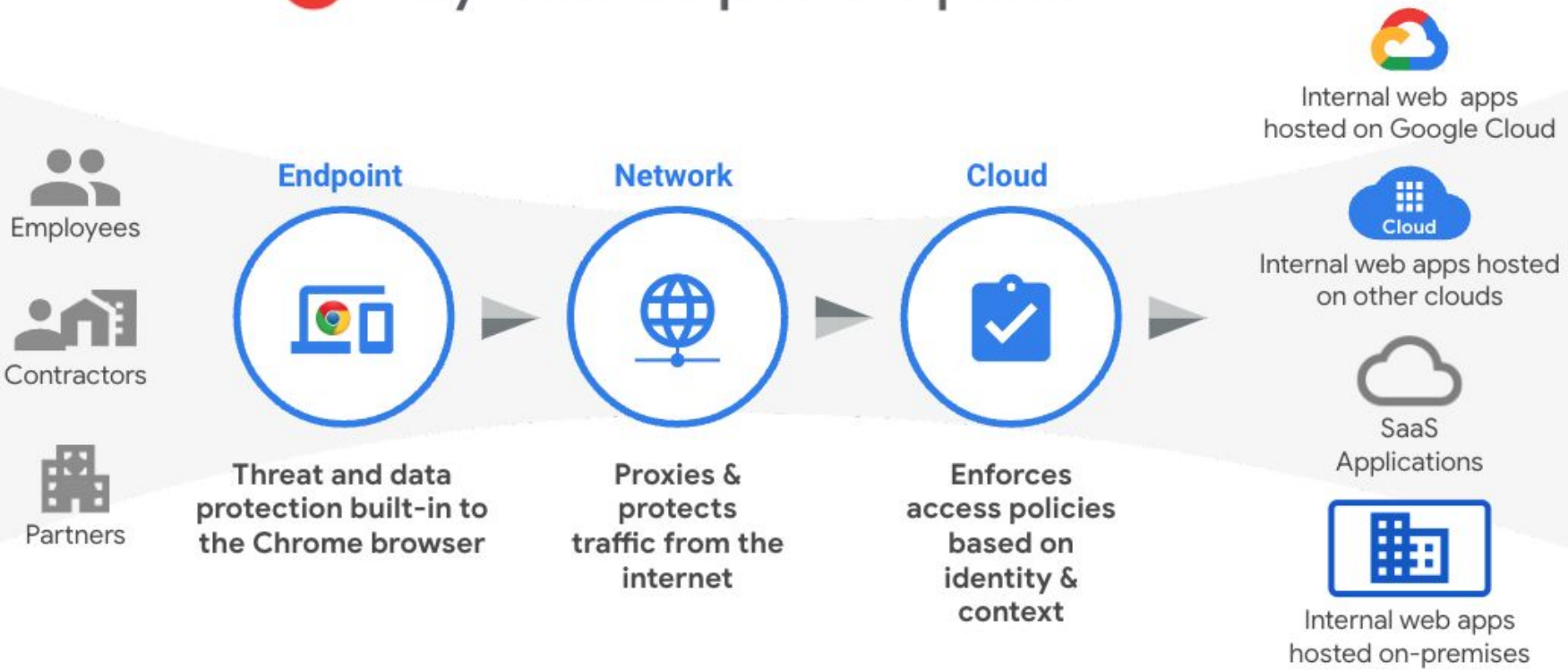


Invisible zero trust security

for all web applications using an agentless approach, whether on managed or unmanaged devices.

\+ Google Workspace

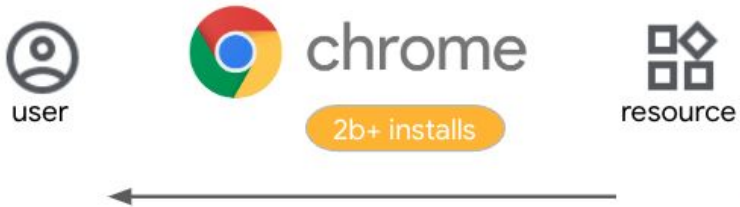
BeyondCorp Enterprise



Built-in threat and data protection

Threat Protection

Real-time enforcement before access to resource / data
- warn user
- block access



Powered by Google Safe Browsing
- Includes data on more than a million unsafe URLs
- Stays up to date by examining billions of URLs each day

Data Protection

Real-time enforcement before data is returned to user
- block download
- block copy / paste

Powered by Google Cloud DLP
- 120 built-in info types
- Supports structured and unstructured data, including images
- Contextual accuracy checks to help prevent false positives

Google Cloud

Third Party Protection

Policy Examples

- Mandate that the device that the request originated from is approved by a domain administrator.
- Allow access to apps only from company-issued devices
- Allow access to Drive only if a user storage device is encrypted
- Restrict access to apps from outside the corporate network
- Disallow access from specific countries
- Mandate that the device that the request originated from uses a desktop Windows operating system and is owned by your organization.
- Use device attributes to verify that the device used to access Google Workspace is reported by **Lookout** as compliant with policies, and the health score is Very Good.

Policy Examples

- Only allow access to shift workers during their shift hours
- Allow Temporary Access
- Allow access only from a managed Chrome browser with latest updates
- Allow access to devices with screen lock enabled
- Allow access to users based on the strength of the user's login credentials
- Only allow access when device data from **CrowdStrike** is fresh
- Disable Downloading of any Drive Files
- And more

Employees

Some teams (e.g. DevOps) only need access to specific web apps

Prevent exfiltration of code and confidential information

Frontline workers

Employees just need access to point-of-sale system

Protect guest payment info and block employee web surfing

Call centers

Staff only need access to internal, browser-based call center apps

Safeguard customer records and PII

Contractors and consultants

Vendors utilize BYOD and only need access to certain apps

Secure corporate records and sensitive information

Simple Implementation

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

Target
specific sets of users and applications and expand as desired

Reduce
legacy access and network controls as deployment increases

promevo™

Questions

Thank You!

Visit Promevo.com for more info and check your email

Next Webinar:

- Introducing gPanel® Enterprise
- August 15, 2023 1pm Eastern