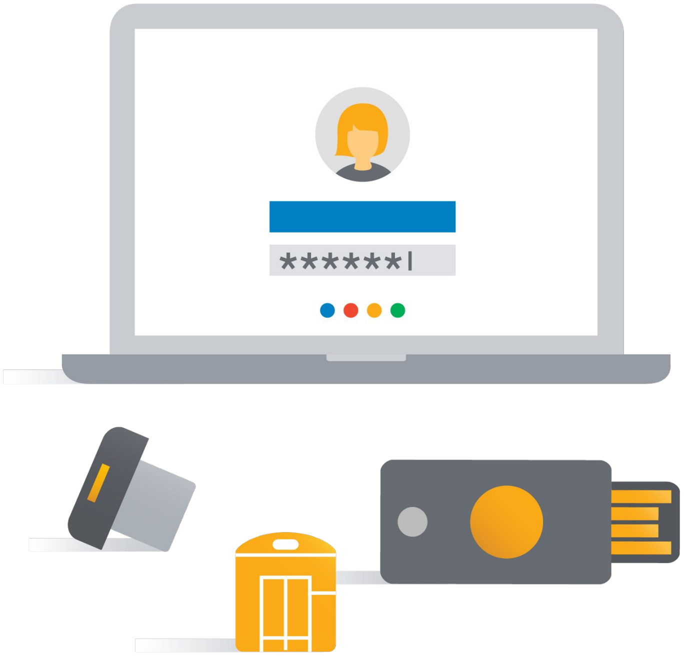
Google Cloud

Zero Trust Foundations

A framework for dynamic security.

Overview Deck



Cybersecurity Action Team

Zero Trust Foundations

Collaborate with the Google Cloud Professional Services Organization (PSO) and the Chief Information Security Officer (CISO) team to develop a Zero Trust Strategy that aligns with NIST SP 800-207, White House Executive Order 14028 on Improving the Nation's Cybersecurity, Google and industry security best practices.

Engagement Goals

1. Educate organizations on zero trust fundamentals, solution options, and cloud-centric security best practices.

2. Assess zero trust maturity and organizational security posture against core zero trust architecture pillars.

3. Help organizations get started with zero trust adoption by crafting a cloud-centric zero trust architecture and migration plan for a target workload.

4. Provide a customized zero trust strategy that systematically outlines a customer organization’s cultural shift requirements for adopting zero trust through people, processes and technology.

Zero Trust Foundations

Timeline: Seven-week engagement led by Google Cloud security consultants from PSO and CISO, in partnership with Customer Engineers (CEs), Technical Account Managers (TAMs), and Strategic Cloud Advisors (SCAs).

Target Audience: C-Suite technology and business leads, technical directors, chief architects, lead engineers and system owners.

Engagement Elements:

- Week 1: Zero Trust Assessment
- Weeks 2-6: Zero Trust Workshop

Deliverables:

- Zero Trust Assessment Report
- Zero Trust Strategy

Zero Trust Foundations: Assessment

Invite key security, business, and IT stakeholders to **collaborate with the Google Cloud CISO team** to break down zero trust fundamentals and security best practices.

Understand your organization's zero trust priorities, maturity, security gaps, and Google's recommendations for starting the zero trust journey.

Learn how Google implements zero trust across a corporate landscape, and how your organization can leverage elements of Google's defense in depth approach.

Identify a targeted workload as the first-mover candidate for zero trust adoption, and as the focus workload for the zero trust workshop.

Zero Trust Foundations: Workshop

- **Engage in deep-dive, interactive sessions** to educate your organization on zero trust components, architecture design, and operation principles.
- **Discuss** first-party zero trust capabilities provided by Google, third-party solutions offered by other vendors, and common zero trust deployment scenarios.
- **Develop a proposed zero trust architecture and adoption plan** for your organization's target first-mover workload.
- Provide an **estimated zero trust delivery timeline and level of effor**t for follow-on implementation, which can be led by the organization independently or in partnership with Google PSO.

Deliverables

1. **Zero Trust Assessment Report**
Consolidated insights from the CISO-led zero trust assessment capturing your organization’s current-state zero trust maturity.

2. **Zero Trust Strategy**
Comprehensive zero trust plan for a targeted first-mover workload. Consolidated insights from the PSO-led zero trust workshop including architecture diagrams, recommendations and organizational findings.

Cybersecurity
Action Team

Thank you.

How Google protects the confidentiality, integrity, and availability of customer compliance data during engagements

☑ All project documentation and collaboration is managed via Google Workspace, which is authorized at **FedRAMP High.**

☑ The Google PSO team will create a **secure folder** to host all project and customer collateral. This folder will have **least privilege access management** - only a defined list of personnel within the customer org and on the Google project team will have access.

☑ If Google works with a partner for delivery, **all partners will be under NDA** and their access to the secure folder hosting customer data will be removed once the project ends.

☑ The default method for sharing project documentation is by **uploading to the secure folder** and sharing **access-controlled links** to the uploaded content. If documentation has to be shared as an attachment, the files can be **password protected if required by the customer.**