Google Cloud

Moving to the Cloud: Zero Trust Security Model

2022 TechEx

Kristy Patullo

Customer Engineer, Google Cloud SLED

Zero Trust approach to security in two words

Trust Nothing

Core zero-trust principles

1

Connecting from a particular network must not determine which services you can access

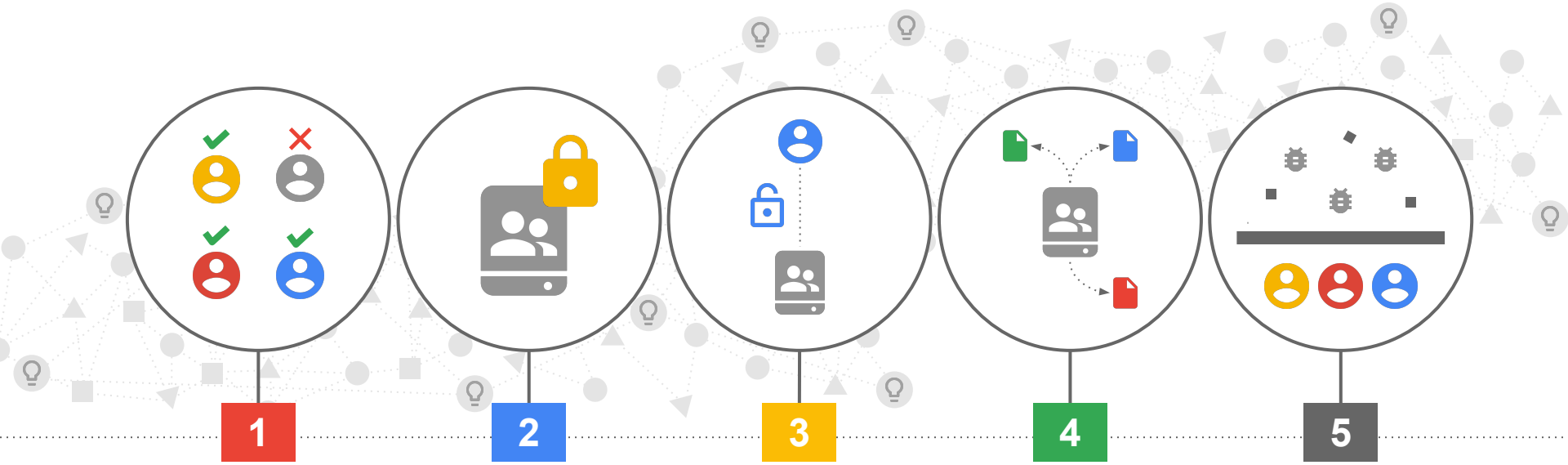
2

Access to services is granted based on context: what we know about you and your device

3

All access to services must be authenticated, authorized and encrypted

Zero Trust is achieved by fully-integrating defense-in-depth layers on turnkey platforms



1. Identity and Provisioning
2. Multifactor Authentication
3. Context Aware Authorization/ Access
4. Encryption (at rest, in transit)
5. End-to-end visibility and security monitoring

Google Cloud

Zero Trust solution components

Google Cloud

Zero Trust platforms incorporate signals from across your ecosystem and provides support for your different environments

User Policies

- Role / group
- MFA / Security key
- Credential strength
- Geographic origin
- Time and date

Device Policies

- OS version
- Encryption status
- Managed devices
- Password enabled
- Network
- Device type
- Alliance partner signals

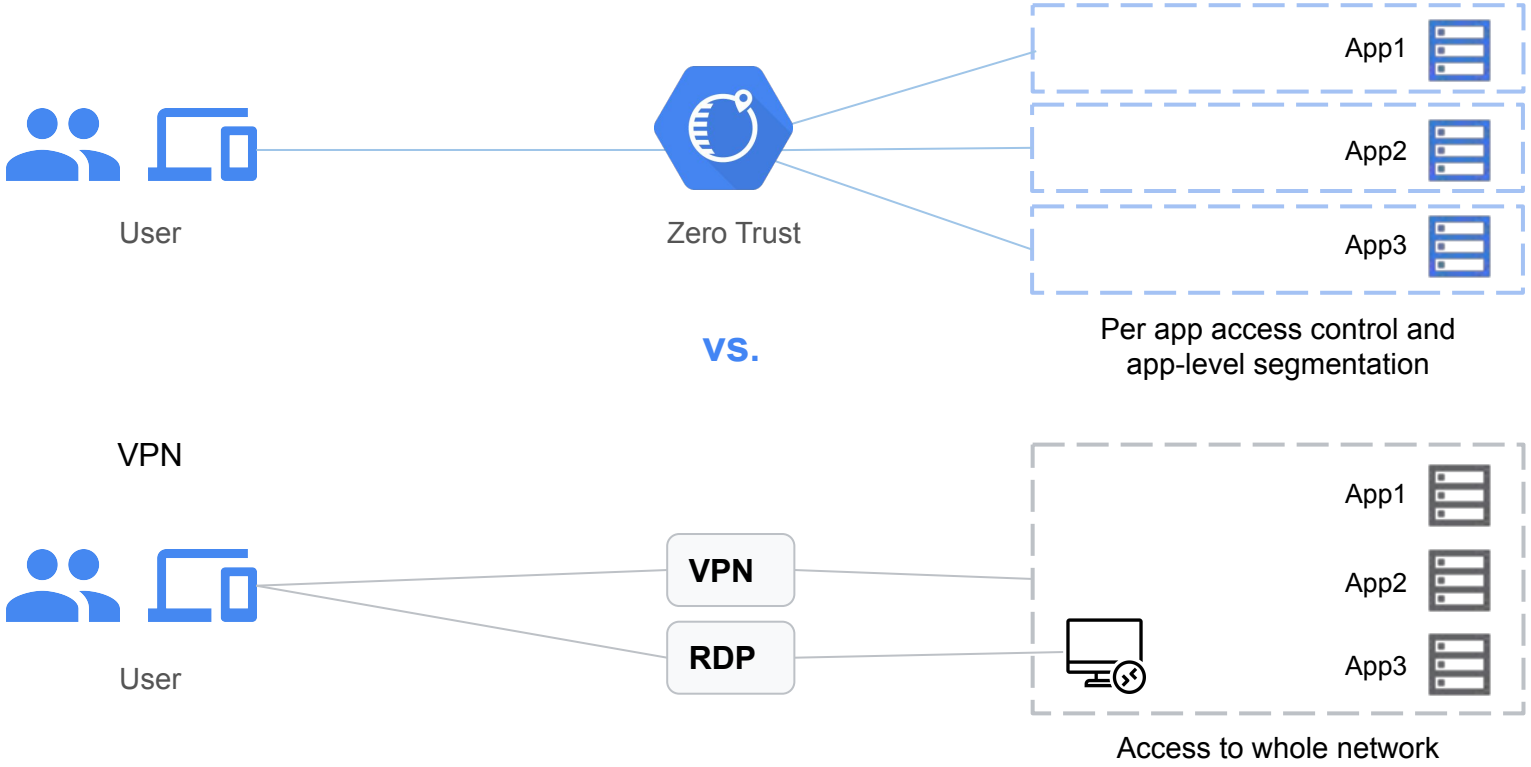
Application Support

- Cloud Applications
- On-Prem Applications
- SaaS (SAML) Applications
- Apps on 3P Clouds

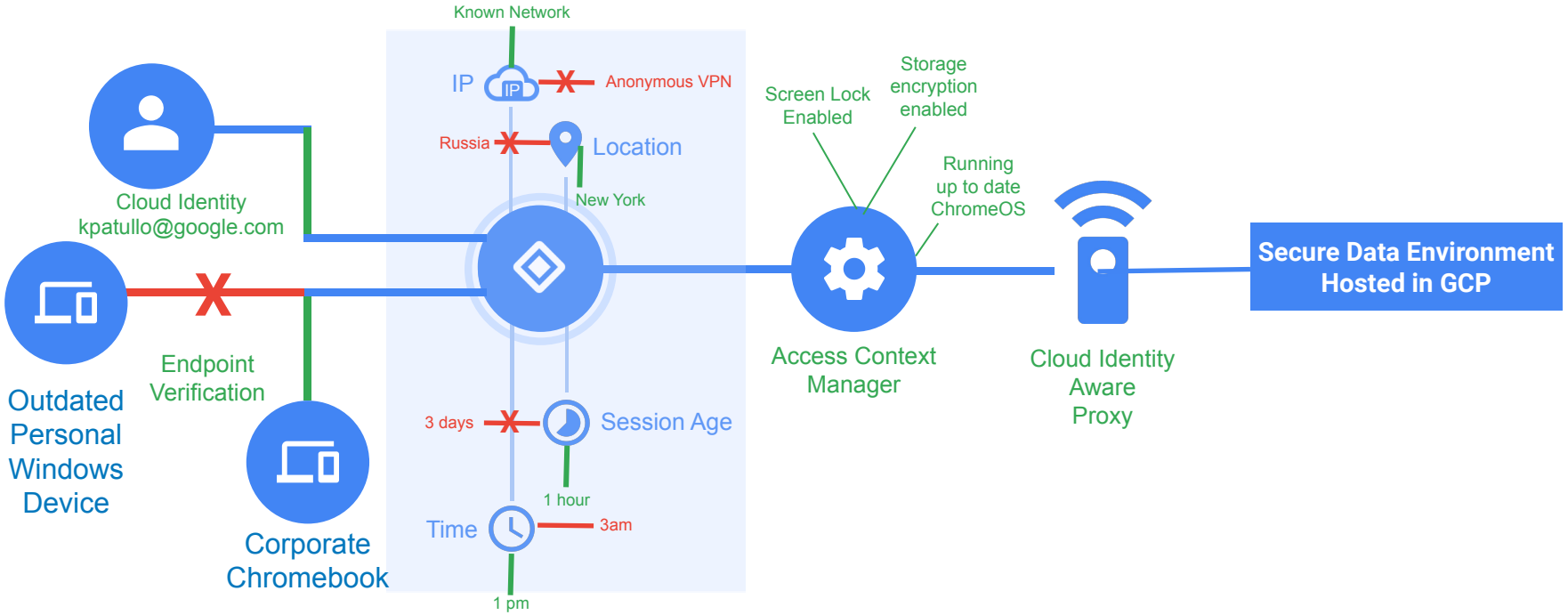
Operating Systems

- Chrome OS
- Windows
- macOS
- Linux

Limit access and lateral movement



Example Architecture: Beyondcorp Enterprise



Google Cloud

Zero-Trust: In Summary

Access becomes Context-Aware:

- Access based on user identity and context
- Shifts controls from network layer to application layer
- Allows users to work more securely from any location
- Allows access without a remote-access VPN

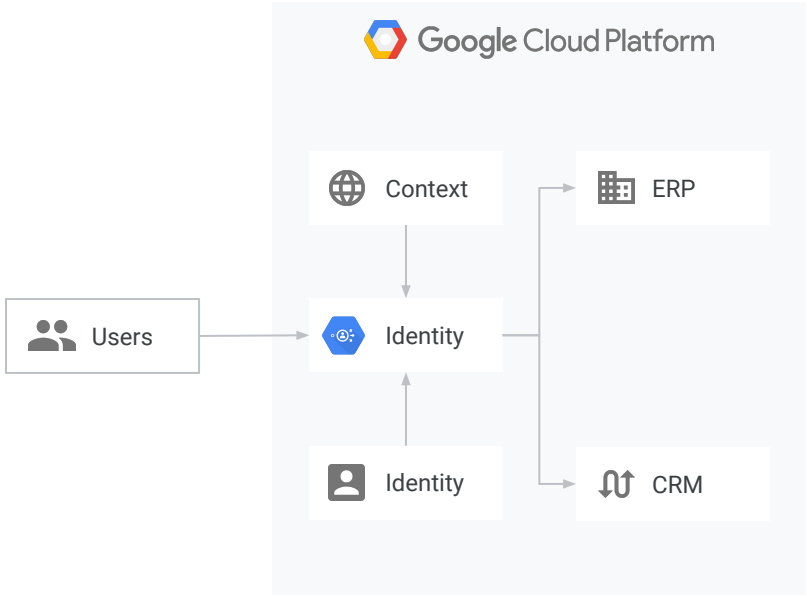
Google Cloud

Cloud IAP- for web apps / VMs

A reverse proxy sits in front of every data request.

- Applies context-aware access policies defined in rules engine
- Enforces encryption between user and app/data.
- Protects against DDoS, does TLS termination

The proxy needs to have near zero latency to provide “invisible” security.

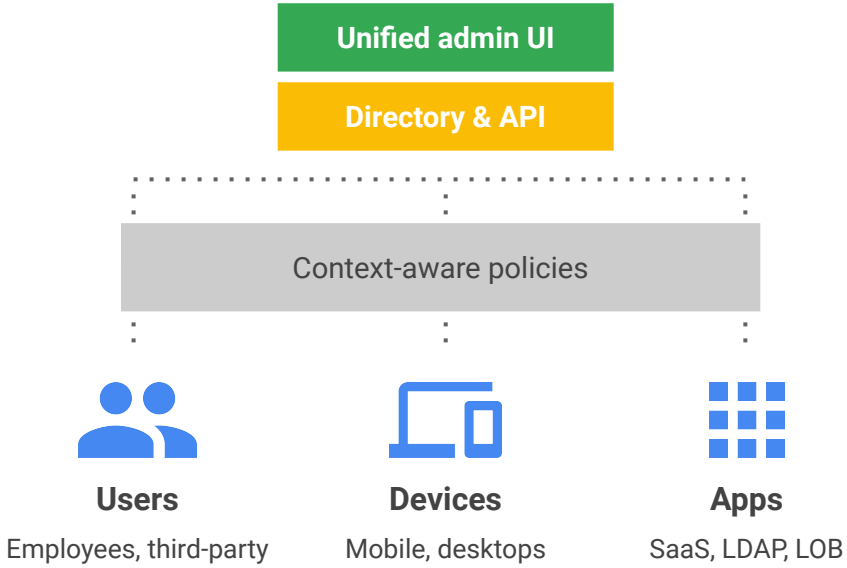


cloud.google.com/iap/

Google Cloud

Cloud Identity - for G Suite apps

- Extend Context-aware for gSuite tools
- Enforce access controls for Gmail, Docs, Sheets
- 3rd party solutions via SAML



cloud.google.com/identity/

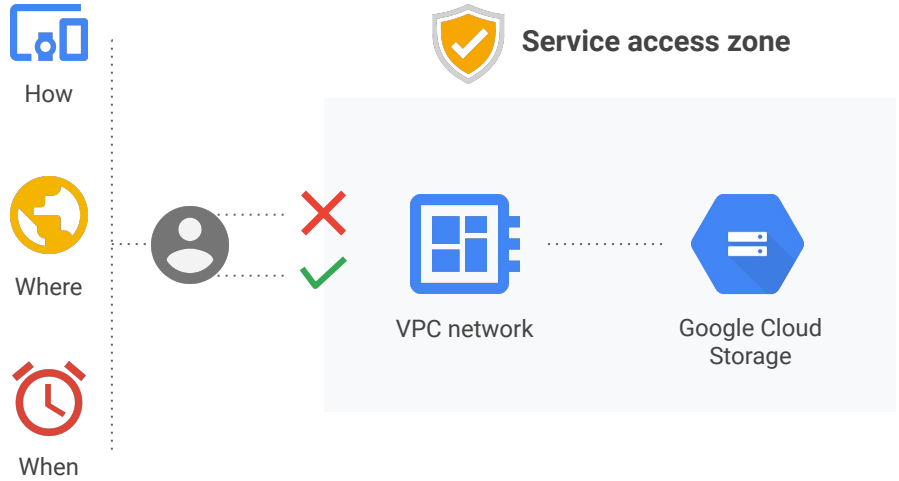
Google Cloud

VPC Service Controls - for GCP APIs

VPC Service Controls allow users to define a security perimeter around Google Cloud Platform resources.

With VPC Service Controls, you can:

- Enforce context-aware access.
- Mitigate data exfiltration risks.
- Extend security boundaries across cloud environments.
- Centrally manage security policies.



cloud.google.com/vpc-service-controls

Google Cloud