Cloud Adoption and Security in a Virtual Work Environment

April 16, 2020

Cybersecurity Coalition

CENTER FOR CYBERSECURITY POLICY AND LAW

Speakers

Ross Nodurft, Senior Director of Cybersecurity Services, eCommerce, Privacy, and Cybersecurity, Venable LLP

Michael Duffy, Deputy Associate Director, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

Matthew Scholl, Chief of the Computer Security Division in the Information Technology Laboratory at the National Institute of Standards and Technology

Ned Miller, Chief Technology Officer, US Public Sector, McAfee

Jeannette Manfra, Global Director, Security and Compliance at Google

James Snow, Head of Security and Compliance Sales Engineering Google Cloud

Agenda

Introduction – Setting the stage for the discussion today (2 mins)

Cybersecurity and Infrastructure Security Agency (CISA) – Current environment (7 mins)

National Institute of Standards and Technology (NIST) – You're in the cloud, now what? (7 mins)

McAfee – Threat Landscape, Shared Responsibility, TIC/CASB, and Zero Trust (7 mins)

Google Cloud – New Normal, Shared Responsibility Model, BeyondCorp, How it's working at Google (7 mins)

Moderator Questions – The moderator will ask a series of questions (15 mins)

Audience Questions – The hosts will open up the floor to attendee questions (15 mins)

Department of Homeland Security, CISA – Michael Duffy

- The Current Environment
- Federal Agencies – What CISA is Seeing
- Current and Future CISA Guidance/Policy
- The Challenge Ahead

Did You “Go To The Cloud?”

Many of us supporting a telework enterprise on short notice.

Where did you go and, now what?

- A Fedramp approved provider?
- Do you know how responsibilities are shared?
- What does this change for you?
- What Common Controls and Inheritance still applies?
- What trust algorithms needs changing?
- Connections, Connections, Connections.

What can you do?

- Microservices and containers
- Policy enforcement and SDL Practices
- ZTA Concepts and implementations
  - E2E Encryption vs Logging
  - Strong Identity Management
  - End Point Assurance
  - Isolation and Segmentation
- Learn, update and refine
- IT, Devices and Ownership

SP 800-210 General Access Control Guidance for Cloud Systems

SP 800-207 Zero Trust Architecture (2nd Draft)

SP 800-204A Building Secure Microservices-based Applications Using Service-Mesh Architecture

SP 800-204 Security Strategies for Microservices-based Application Systems

SP 800-190 Application Container Security Guide

SP 800-189 Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation

SP 800-177 Rev. 1 Trustworthy Email

SP 800-146 Cloud Computing Synopsis and Recommendations

SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing

SP 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection

SP 1800-19 Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments

A Few References That Might Help

Cloud Adoption & Security in a Virtual Work Environment

Evolving Cloud Threat Landscape, New Cloud 360 Responsibility Model, Use Cases for Cloud Security, Zero Trust Now is the Time!

Ned Miller – Chief Technical Strategist, McAfee US Public Sector

16 April 2020

McAfee

Evolving Cloud Security Threat Landscape…

Managing sensitive data shared & stored in the cloud and understanding your risk….

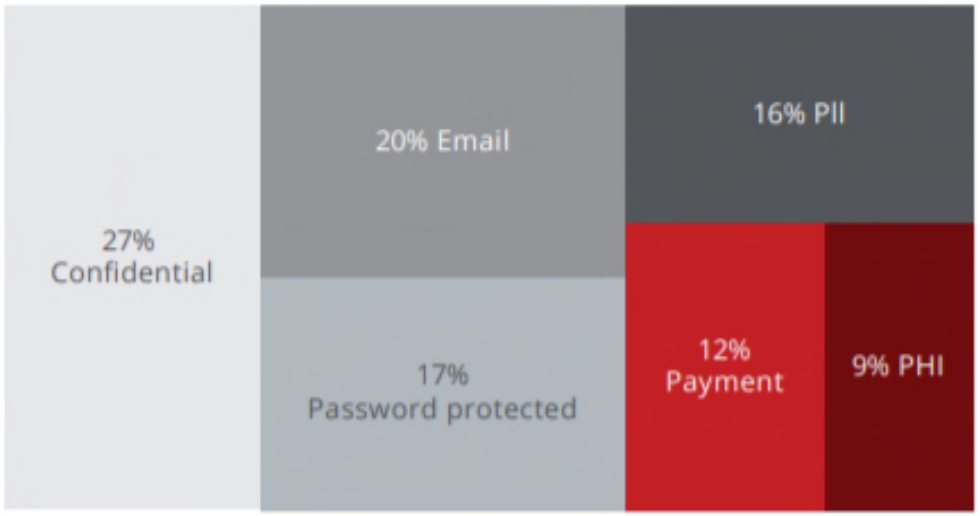


Figure 1. Types of sensitive data in the cloud.

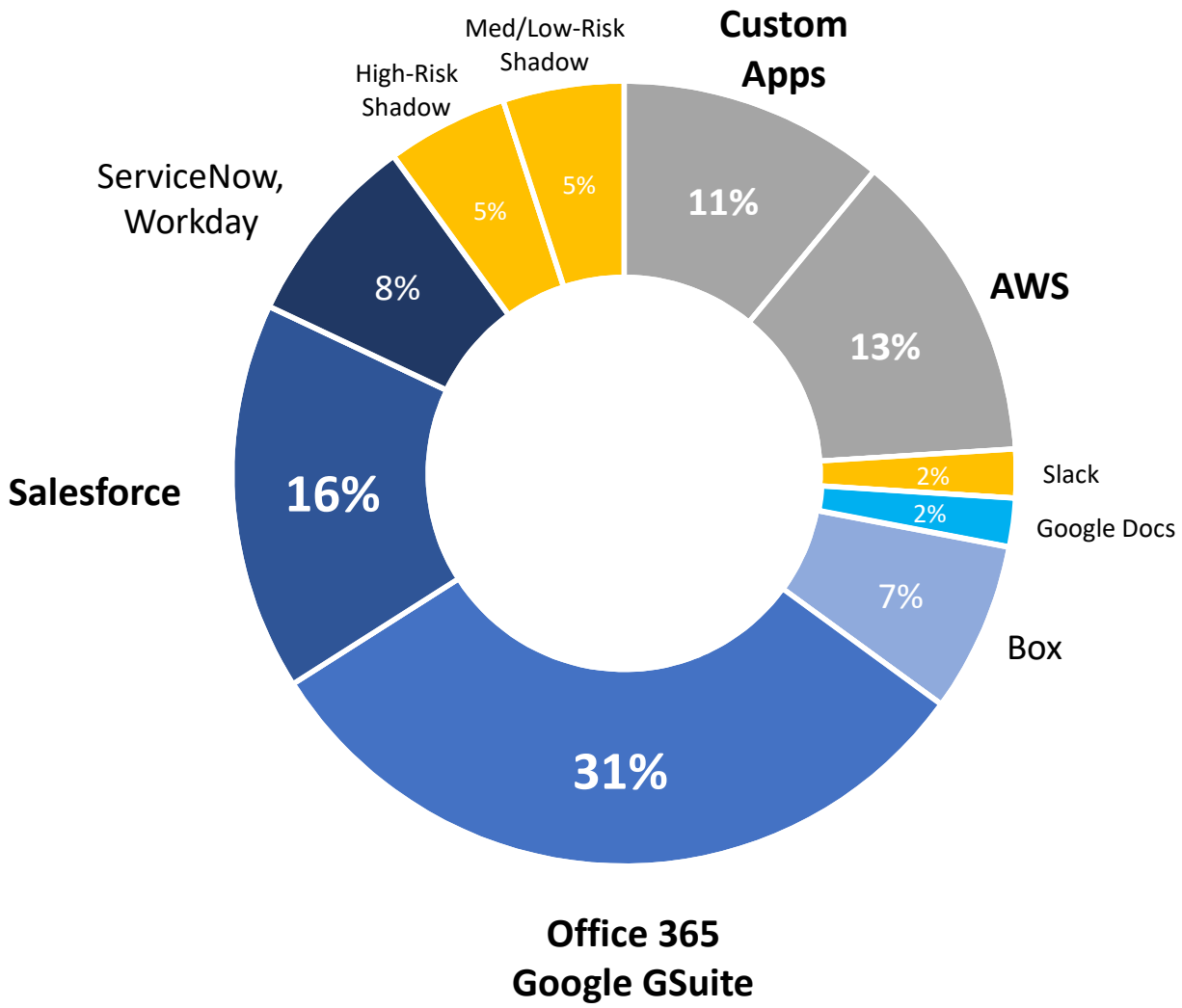
Common Cloud Security Threats Amplified Due to Cloud Surge Usage:

- Lack of Cloud Security Architecture and Strategy
- Limited Cloud Usage Visibility [Shadow IT]
- Mis configuration and inadequate change control
- Insufficient Identity, Credential, Access and Key Management
- Account Hijacking
- Insider Threat
- Insecure Interfaces and API's
- Weak Control Plane
- Abuse or Nefarious Use of Cloud Services

Where is your Sensitive Data in the Cloud?

Survey Says:

- ✓ 65% in top 5 SaaS apps
- ✓ 25% in IaaS/PaaS
- ✓ 10% in shadow/permitted



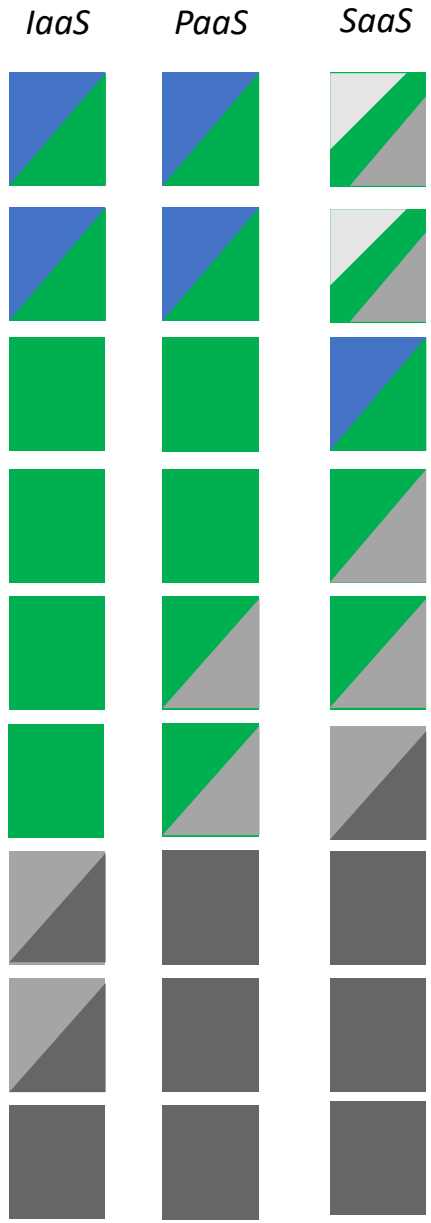
Cloud Security 360^0 Shared Responsibility Model…

User Responsibility

Enterprise Responsibility

Service Provider feature, enterprise configuration

Service Provider Responsibility



✓ **Collaboration** Control

✓ **User/Device/Data** Control

✓ **Data** Classification & Accountability

End-Point Protection

Identity & Access Management

Application Level Security

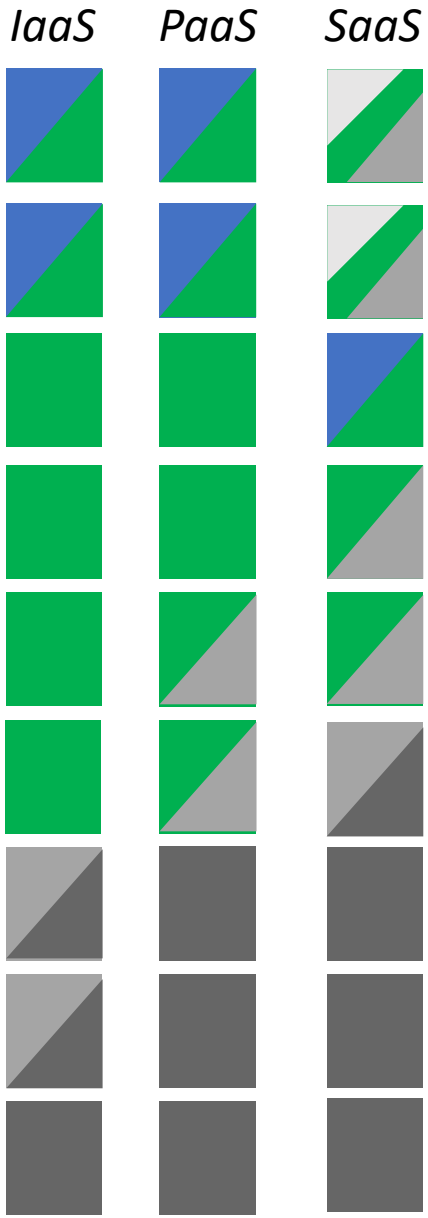
Network Control

Host Infrastructure

Physical Security & Connectivity

McAfee

Technologies Required - Cloud 360^0 Shared Responsibility Model



Link control, domain check, email controls, encryption

✓ **Collaboration** control

User Behavior analytics, user & device policies

✓ **User/Device/Data** control

DLP, on demand scan

✓ **Data** Classification & Accountability

Compromised account detection, malware scanning

End-Point Protection

SSO integration

Identity & Access Management

Configuration audit

Application Level Controls

Audit of cloud configurations

Network Control

CIS benchmarking

Host Infrastructure

Physical Security

Trusted Internet Connection 3.0 Architecture – CISA Telework Guidance

The primary use cases for CASB as part of your cloud security architecture….

Key Use Cases

■ Enforce data loss prevention (DLP) policies on data in the cloud, in sync with your enterprise DLP strategy.

■ Prevent unauthorized sharing of sensitive data to the wrong people.

■ Block sync/download of agency data to personal devices.

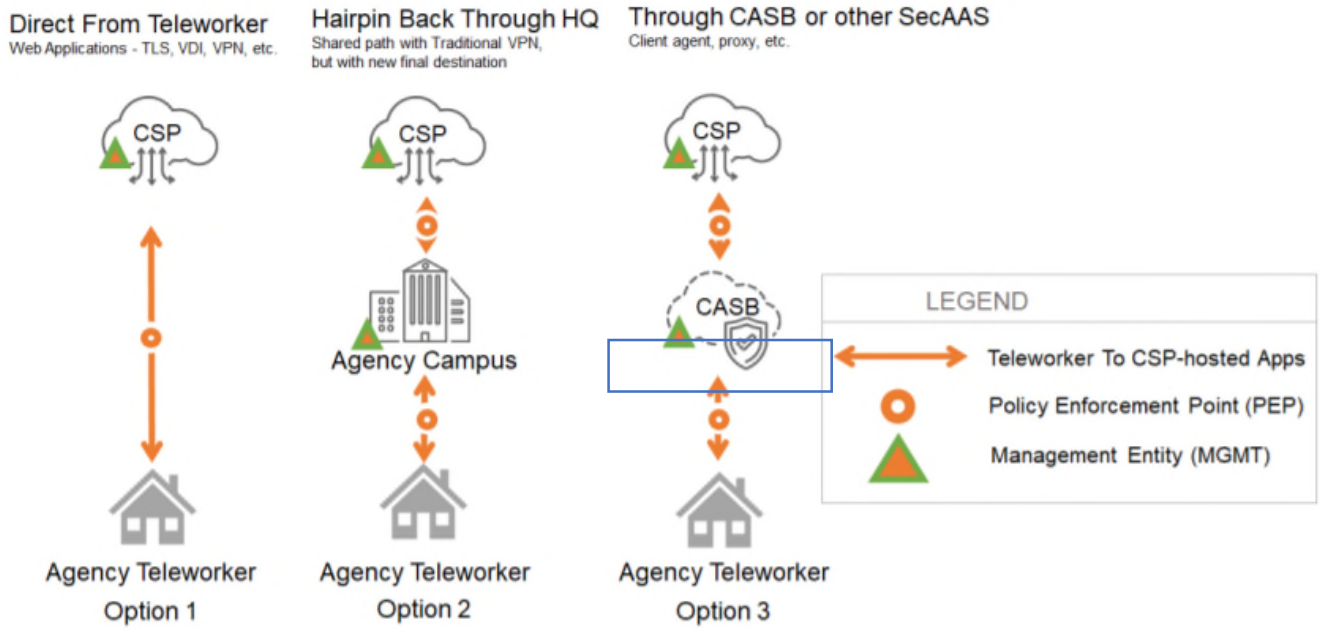
■ Detect compromised accounts, insider threats, and malware.

■ Encrypt cloud data with keys that only you can access.

■ Gain visibility into unsanctioned applications and control their functionality.

■ Audit for misconfiguration against industry benchmarks and automatically change settings.

FIGURE 2 - ALTERNATIVE SECURITY PATTERNS FOR TELEWORKER ACCESSING CSP RESOURCES



For more information about the TIC program, please see: https://www.cisa.gov/trusted-internet-connections.
For OMB guidance on COVID-19, please see: https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-17.pdf.

Telework Surge Accelerates Zero Trust & Cloud Security Data Protection Requirements…

Survey Says:

- “Shadow IT” and the recent “cloud surge” expands risk infinitely: Fifty-two percent of organizations who use cloud services have had data stolen in a breach.
- Unmanaged personal devices are black holes: One in four organizations have had their sensitive data downloaded from the cloud to an unmanaged personal device, where they can’t see or control what happens to the data.
- A new era of data protection is on the horizon: Only 31% of organizations have consistent data protection across their devices, networks, and cloud services.
- Intercloud travel opens new paths to risk: Nearly one in 10 files shared in the cloud with sensitive data use a link open to the public, an increase of 111% year over year.
- Dispersion outpaces IT: More than 40,000 data loss incidents are likely missed every month by organizations who don’t monitor their cloud services.

Recommendations:

- Evaluate your data protection strategy for devices and the cloud: Consider the difference between a disparate set of technologies at each control point and the advantages of merging them for a single set of policies, workflows, and results.
- Investigate the breadth and risk of “Shadow IT”: Determine your scope of cloud use, with a focus on high-risk services. Then, move to enabling your approved services and restricting access to those which might put data at risk.
- Plan for the future of unified security for your data: Context about devices improves security of data in the cloud, and context about the risk of cloud services improves access policy through the web. Many more efficiencies apply, while some are yet to be discovered. These control points are merging to deliver the future of data security.

Cloud Security in a Virtual Work Environment

Jeanette Manfra, Global Director, Government Security & Compliance

James Snow, Head of Security & Compliance Customer Engineering - Americas

Google Cloud

Google Cloud
Security fundamentals

Protection

Core infrastructure designed, built, and operated to help secure and prevent threats

Control

Security controls to help meet policy, regulatory, and business objectives

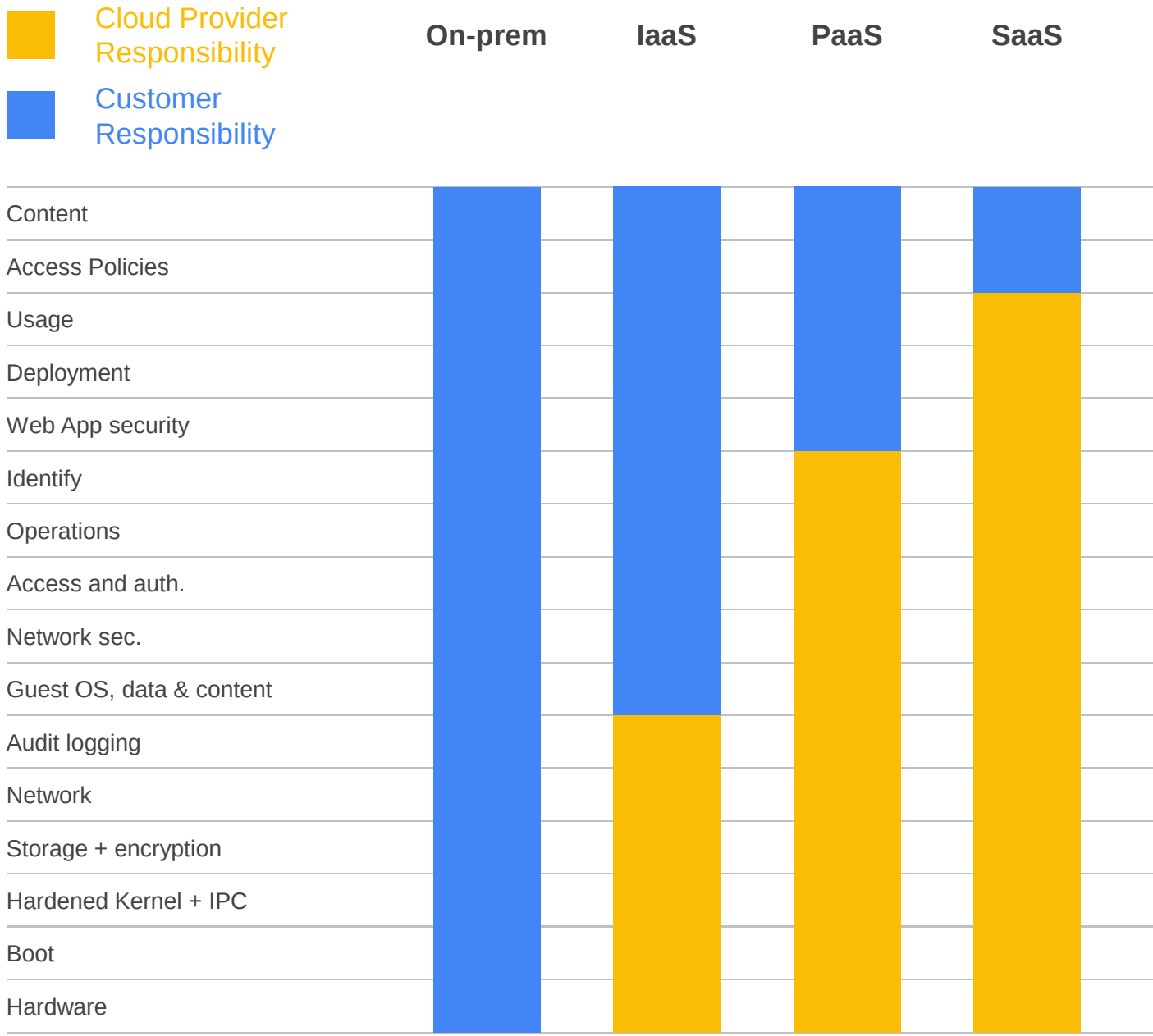
Compliance

Working to meet our responsibilities and make compliance easier for customers

Understanding
shared responsibility

The **boundaries change** based on the services selected by the customer

Customers can use multiple classes of services **simultaneously**



Google Cloud

The world has changed

Remote work is the new normal

US workers who **work from home** multiple days per week

before COVID-19

after COVID-19

You need to provide secure access to internal apps for your employees and extended workforce as quickly as possible

Google Cloud

Source: Global Workplace Analytics

How BeyondCorp works

Access internal apps
through a browser

Employees

Contractors

Partners

BeyondCorp
Remote Access

Proxies & protects
traffic from the internet

Enforces access policies based
on identity & context

Browser-based apps hosted
on Google Cloud

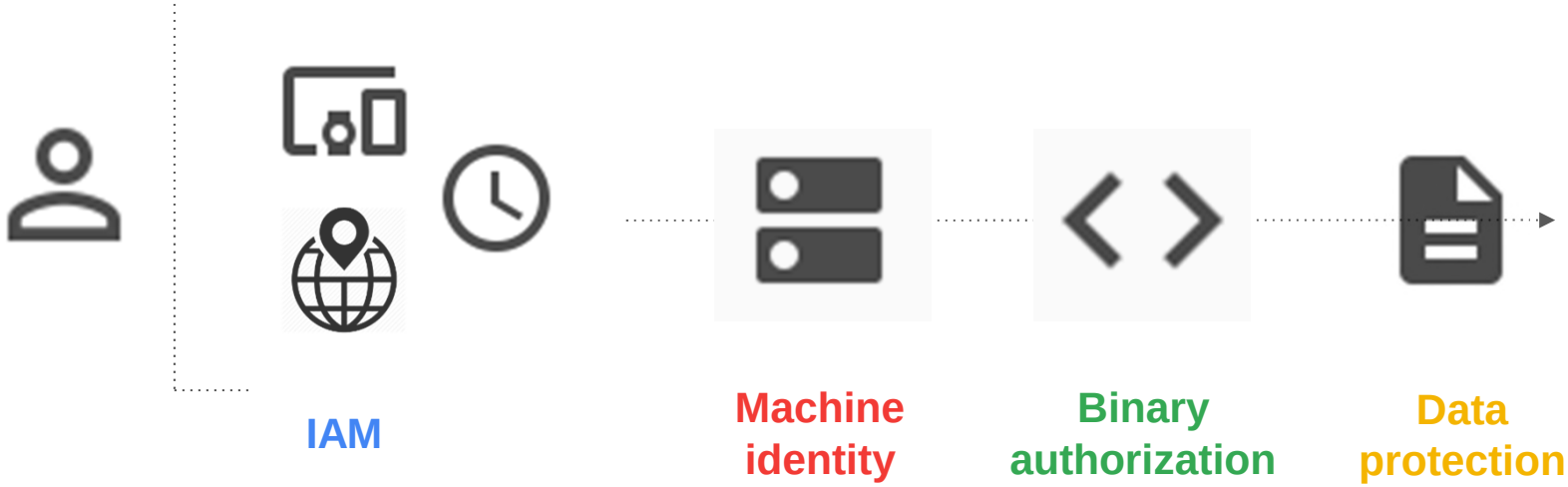
Browser-based apps
hosted on other clouds

Browser-based apps
hosted on-premises

Google Cloud: Cryptographically secured identities

- ✓ User identity
- ✓ Device identity
- ✓ Machine identity
- ✓ Service identity
- ✓ Code identity
- ...

Right identity accessing the right machine authorized by the right code accessing the right data at the right time and context



BeyondCorp

A new approach to enterprise security.

VIEW RESEARCH PAPERS

ENABLE WITH CONTEXT-AWARE ACCESS

BeyondCorp at Google

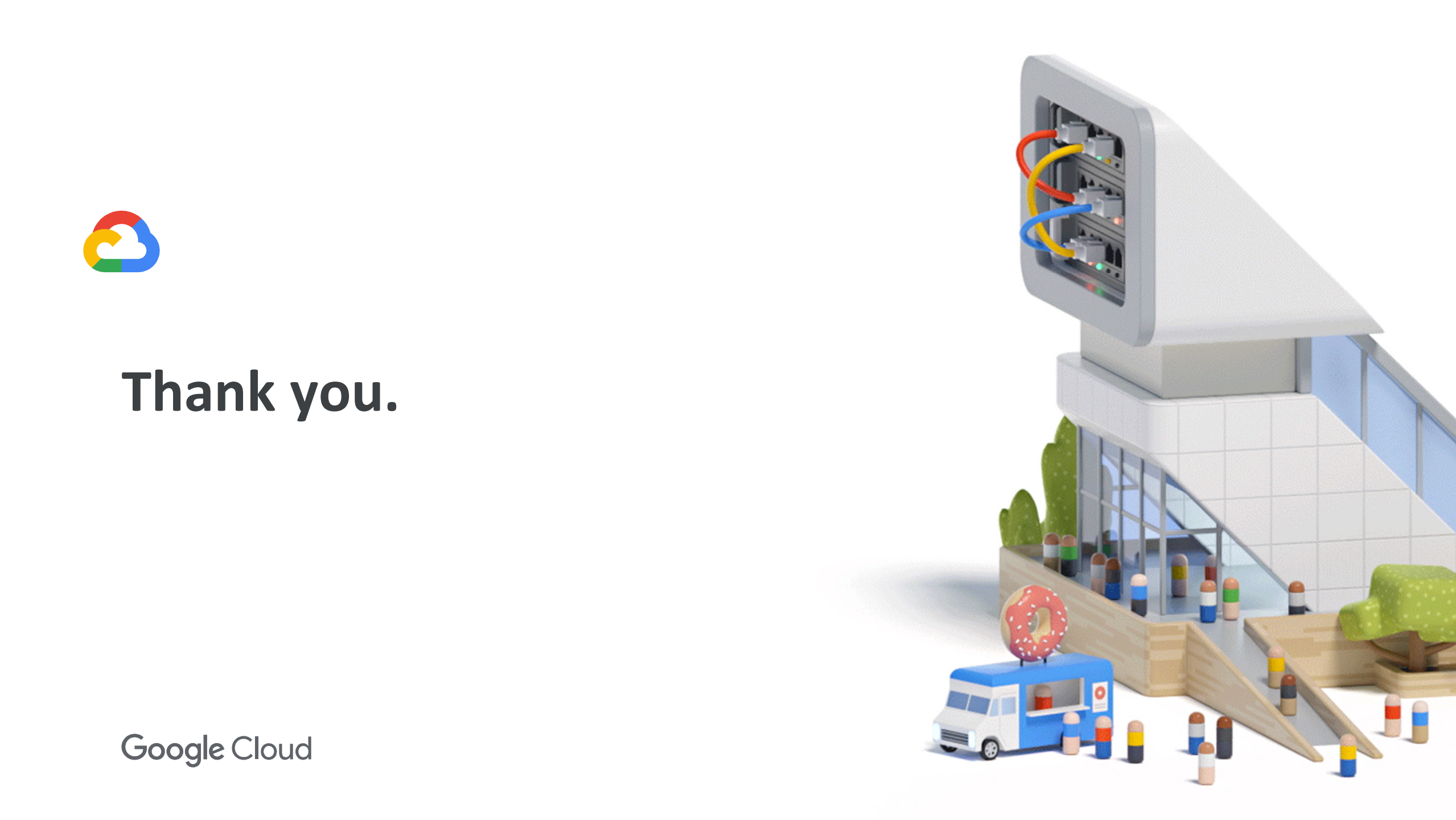
BeyondCorp is Google's implementation of the zero trust security model that builds upon eight years of building zero trust networks at Google, combined with ideas and best practices from the community. By shifting access controls from the network perimeter to individual users and devices, BeyondCorp allows employees, contractors, and other users to work more securely from virtually any location without the need for a traditional VPN.

https://cloud.google.com/beyondcorp#researchPapers

BeyondCorp research papers

These research papers describe the story of BeyondCorp at Google, from concept through implementation:

- An overview: "A New Approach to Enterprise Security"
- How Google did it: "Design to Deployment at Google"
- Google's frontend infrastructure: "The Access Proxy"
- Migrating to BeyondCorp: Maintaining Productivity While Improving Security
- The human element: "The User Experience"
- Secure your endpoints: "Building a Healthy Fleet"



Thank you.

Google Cloud

Questions and Discussion

CENTER FOR CYBERSECURITY
POLICY AND LAW