



Welcome and Opening Remarks

Michael Watson

Feb. 6, 2019



ISOAG Feb. 6 ,2019 Agenda

I. Welcome and Opening Remarks

Mike Watson, VITA

II. Data Governance

Carlos Rivero, Office of Administration

**III. Program Protection Planning,
Relationship(s) to Identity and Access
Management, and Impacts to Risk
Management/Information Security**

Roy Logan, NASA

IV. Data Protection in the Cloud

Willis Zhang, Cloud engineer, Google

V. Upcoming Events

Mike Watson

VI. Partnership Update

SAIC



office of the governor of the commonwealth of virginia

Data Governance

Chief Data Officer Carlos Rivero

Why data governance?

- To ensure data are sound, **secure**, and accessible to qualified users
- To improve **productivity** and efficiency
- To increase the **value** of the commonwealth's data assets by guiding and enabling its evolution from information to intelligence
- To promote data discovery, exploration, integration, and sharing through the implementation of enterprise **standards**

Data value chain

- A data value chain describes the **evolution** of data from information to intelligence within an organization.
- It encapsulates the various **forms** data can take as organizational units transform it to fit their needs.
- As such, its inherent **value** increases the more it is used.
- A **feedback** loop is created when changes to data collection programs are implemented due to the identification of knowledge gaps.
- Thus, supporting a virtuous cycle of **continuous improvement** and increasing the value of the organization's data assets.

collect

DATA

interpret

INFORMATION

assimilate

KNOWLEDGE

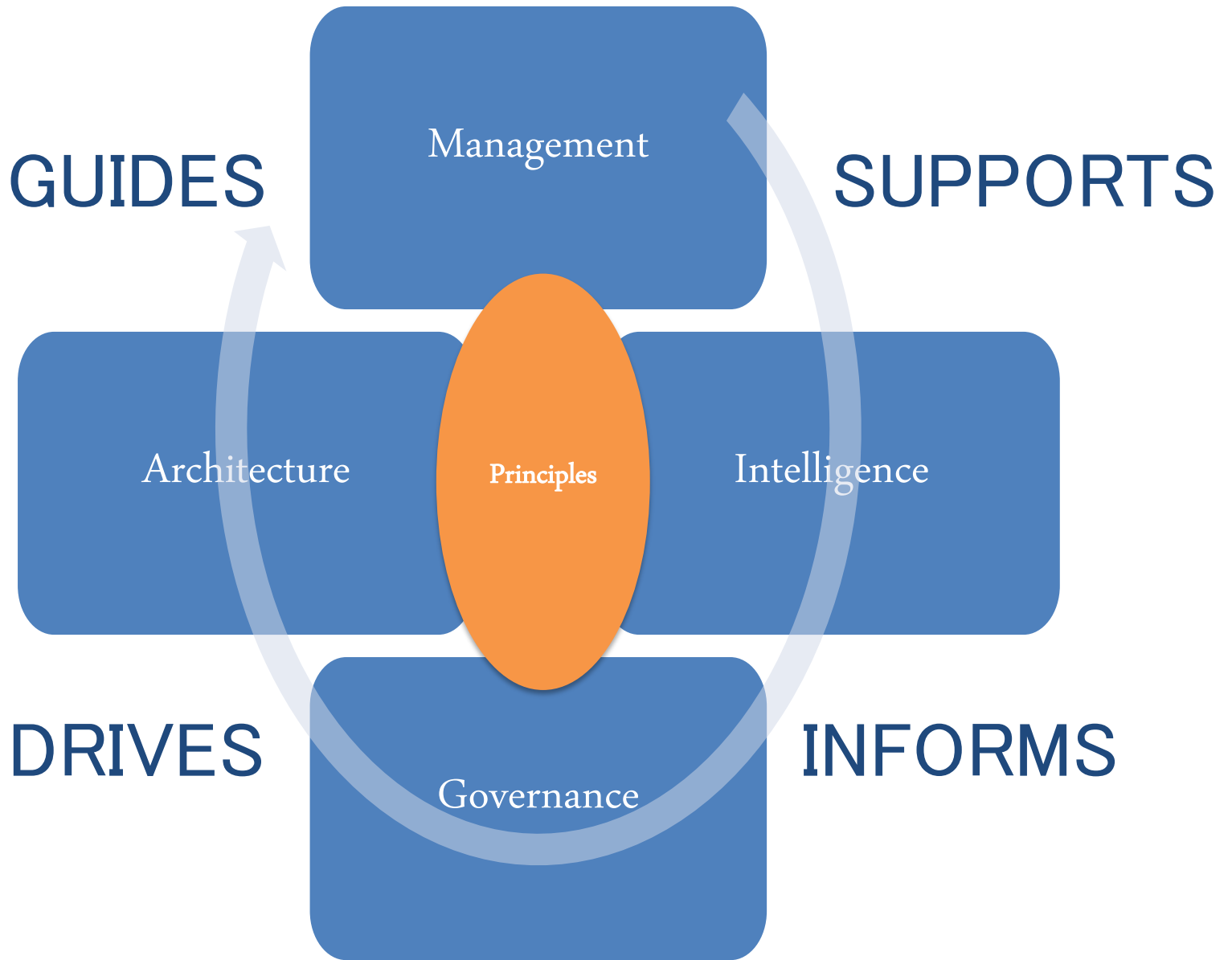
integrate

INTELLIGENCE

Actionable Decisions

Chief data officer

- **Guides** the development of enterprise standards, policies, and best practices to ensure the organization's data holdings *increase* in **value** over time
- **Liaise** between Mission and Technology Programs
- **Leads** enterprise data governance across the Commonwealth
- **promotes** secure data sharing



Principles

- Used to support **mission** goals
- Interpreted, analyzed, and assimilated to support **actionable** decisions
- Standardized to promote **interoperability** and integration
- Managed to maintain quality, **integrity**, and reliability
- Accessible with appropriate **security** controls
- Disseminated to promote **reuse**

Data culture

- Establish **awareness**
- Facilitate **engagement**
- Provide **inspiration**
- Promote **empowerment**

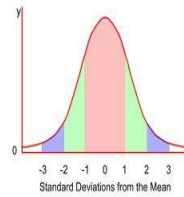
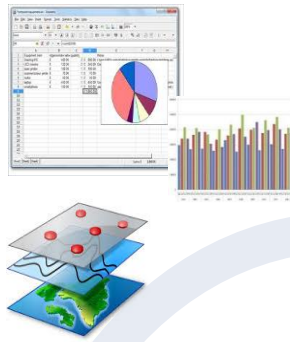
Student engagement

- Rural **Apprenticeship** Program
 - Data Documentation and Visualization
 - Data Quality Assessments
- Commonwealth Data **Internship** Program
 - Exploratory Data Analysis
 - Data Modeling
- Commonwealth Analytics **Fellowship**
 - Data Analytics
 - Predictive Modeling
 - Machine Learning

Data science brain trust

- Students work on increasingly complex data projects as they mature academically
- University faculty collaborate with agency subject matter experts on research proposals to support students and develop algorithms
- Innovative businesses “operationalize” algorithms developed by research universities through integration with the stakeholder’s intelligence framework supporting **Actionable Decisions**

Data
Interoperability
supporting integration
and tactical use

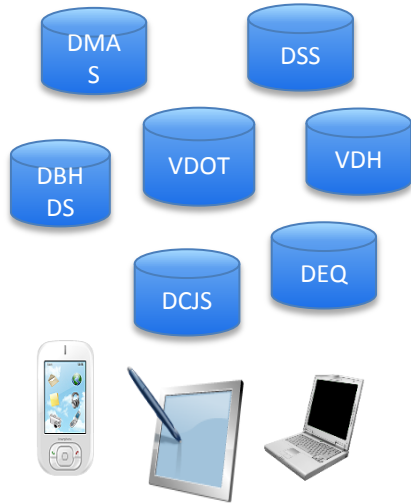


$$p = \frac{e^{a+bX}}{1 + e^{a+bX}}$$



Research universities and
private businesses
conduct analytics
research and develop
algorithms

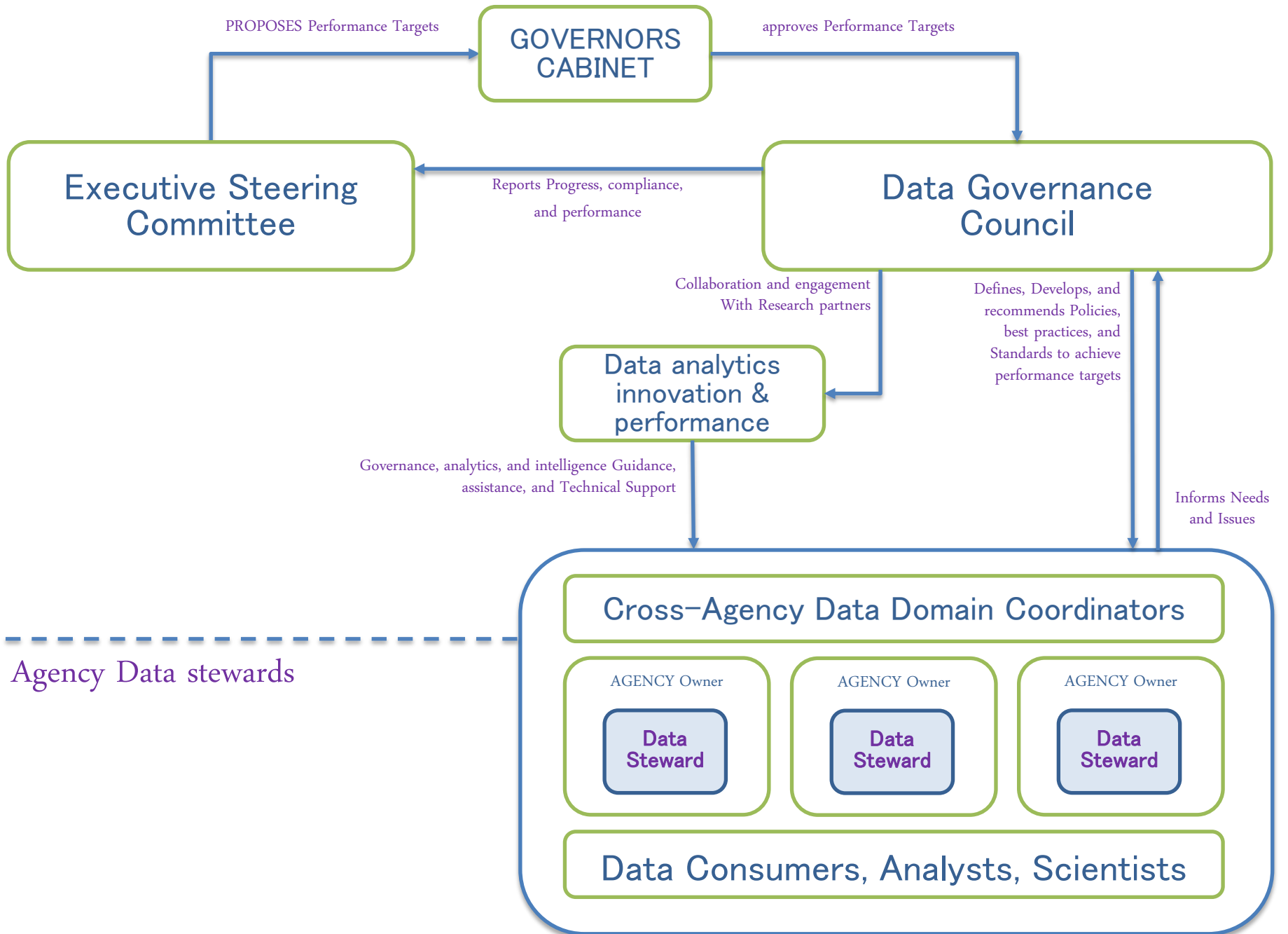
*Knowledge gaps
identified and
mitigated supporting
Continuous
Improvement*



Agency Operations

Algorithms are
'operationalized' and
embedded
into commonwealth
intelligence products VIA
Tech transfer supporting
strategic, tactical,
operational levels





Roles and responsibilities

Executive Level

- Executive Steering Committee

Strategic Level

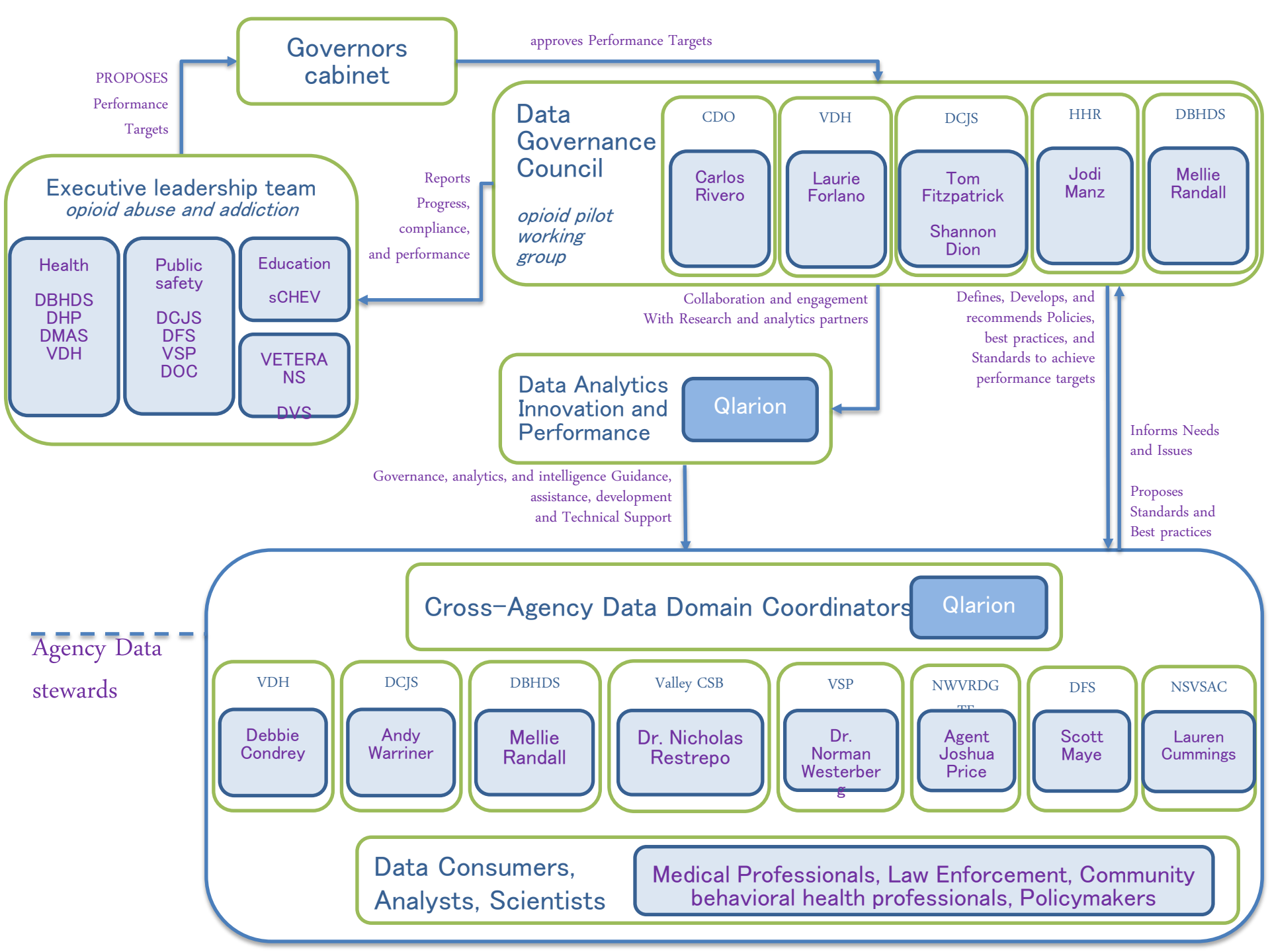
- Data Governance Council

Tactical Level

- Agency Data Officers
- Data Management Technical Team
- Data Domain Managers/Experts
- Business/Program Management
- Geospatial Information Officers
- Information System Security Officers
- Information System Security Managers

Operational Level

- Data Stewards
- Data Scientists, Architects, Engineers, Analysts, and Consumers



Immediate goals/actions

- Stakeholder Identification and Engagement
- Data Governance Research
 - Internal (Commonwealth Agencies, Commissions, Boards, and Localities)
 - External (State CDOs)
- Data and Technology Inventory, Data Dictionary and Catalog
- Pilot Projects (Opioid Substance Abuse, Roadway Safety)
- Data Sharing Platform

long term goals

- Standard Data Sharing Agreement Process
- Secure Multi-tiered Information Sharing Environment
- Multiple Data Analytics Platforms
- Standardize Identity Management across Operational Systems



VITA Briefing NASA ICAM Issues/Impacts



**Special Agent Roy Logan
Center Chief of Security
Langley Research Center
Hampton, Virginia**

Feb. 7, 2019



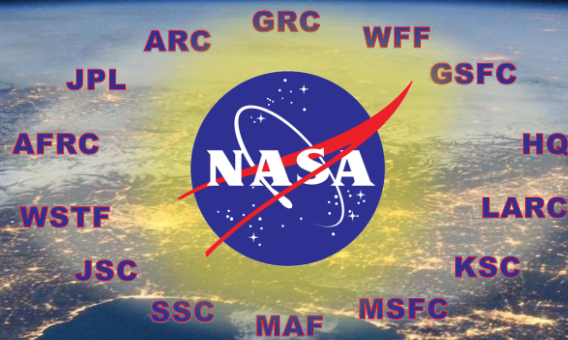
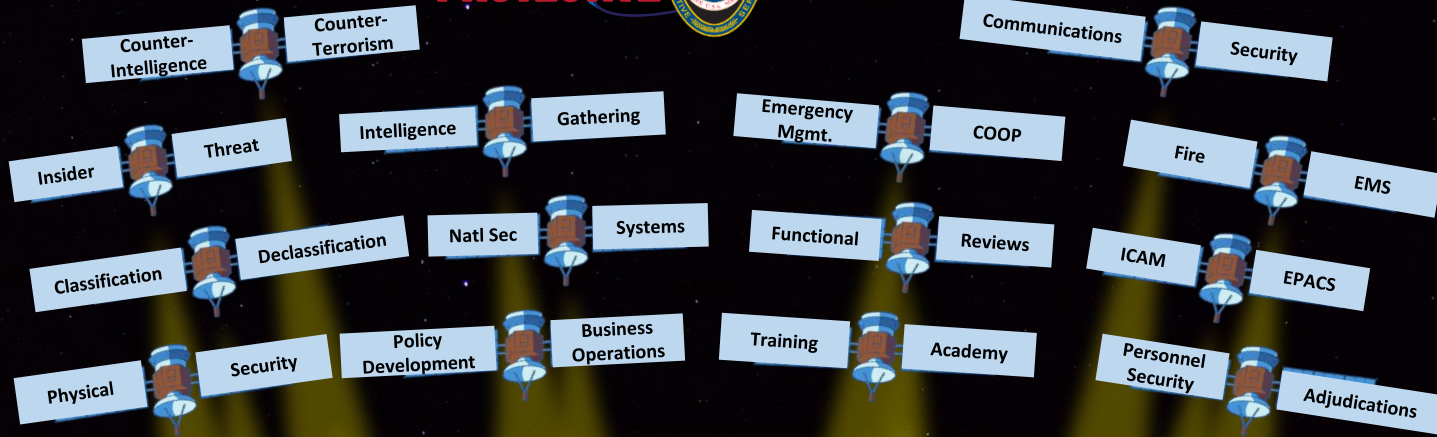


Overview of Topics

- **Perspective**
- **Identity**
- **Credentials**
- **Security Level(s)**
- **Risk Matrix**

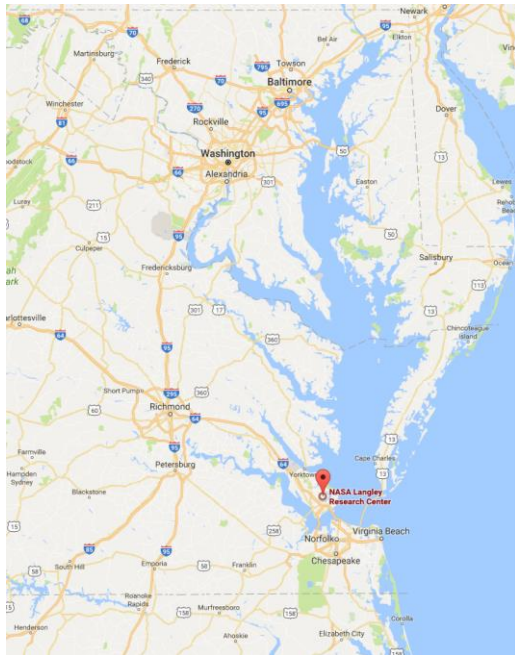


NASA Protective Services Enterprise





Langley Research Center Overview



The First NASA Center

Specializing in Aeronautics Research

Wind Tunnel Test Facilities
Laboratories for Acoustic,
Atmospheric Science, Structures and
Materials, Laser, Lidar and Remote Sensing
research

750 acres

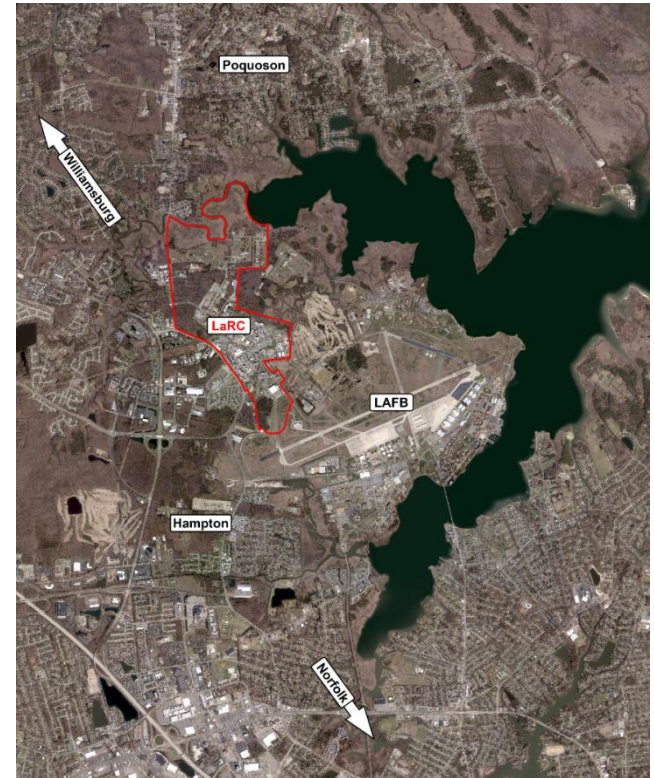
198 buildings

6338 rooms

Approx. 3.4M gross sq ft

Replacement value of \$3.6B

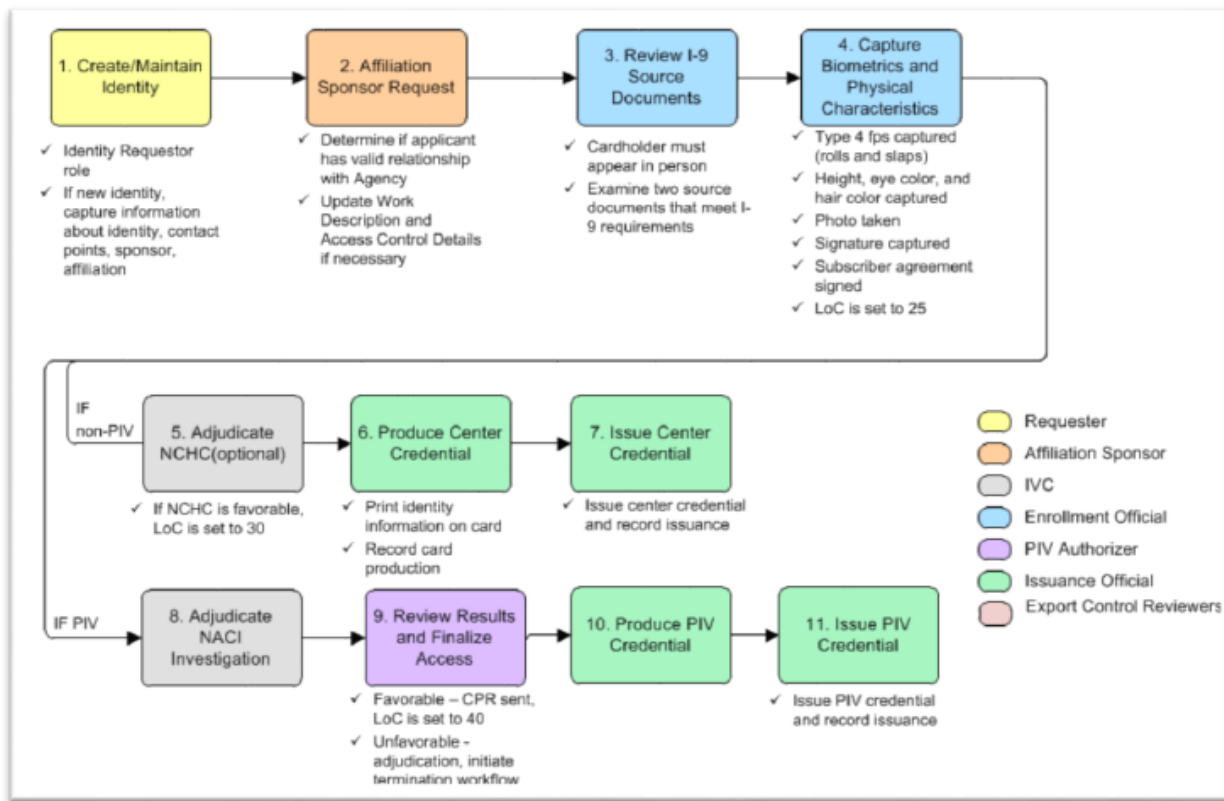
5069 Civil Servant and Contractor
Employees divided into 19 managerial
organizations





Identity, Position Risk, and Credentialing

IDENTITY ONBOARDING WORKFLOW





Personal Identity Verification (PIV)

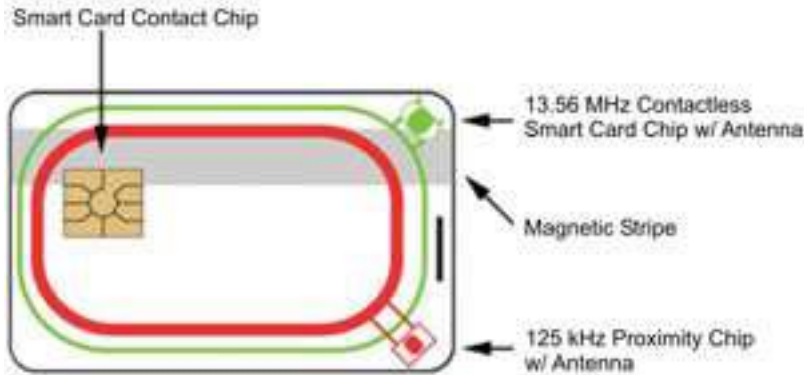
Level of Confidence	Tiering	Risk Level	Favorable Investigation
10			Identity Created
20			NCIC (Remote Identity Proof)
25			Enrollment (F2F Identity Proof)
30			NCHC (FBI Results to Fingerprints)
30			SAC (Fingerprints)
40	1	Low	NACI, CNACI
50	2	Moderate/Position of Trust	MBI, NACLCL
55	3	Non-Critical Sensitive	ANACI
60	4	High Risk/Position of Trust	BI, PRI
65	5	High Risk/With TOP SECRET	SSBI, PPR
70	5	Critical/Special Sensitive	SSBI, PPR





Personal Identity Verification (PIV)

Based on level of confidence - used for all logical systems and physical access controls.





Credential Requirements

- **Homeland Security Presidential Directive (HSPD) 12 (Aug 2004)**
- **Federal Information Processing Standard (FIPS) 201 (Mar 2006):**
 - Outlines the cryptographic algorithm standards for PIV
- **FIPS 201-2 (Aug 2013):**
 - Updated standards. Mandated 4 Cert cards to include:
 - Card Authorization Key (replaces CHUID)
 - Digital Signature Key (digitally sign documents)
 - Key Management Key (generated, exchanged, stored, and used)
 - Facial Image (stored on card)
 - Provides for On Card Comparison (OCC) and Derived Credentials



Facility Security Level(s)

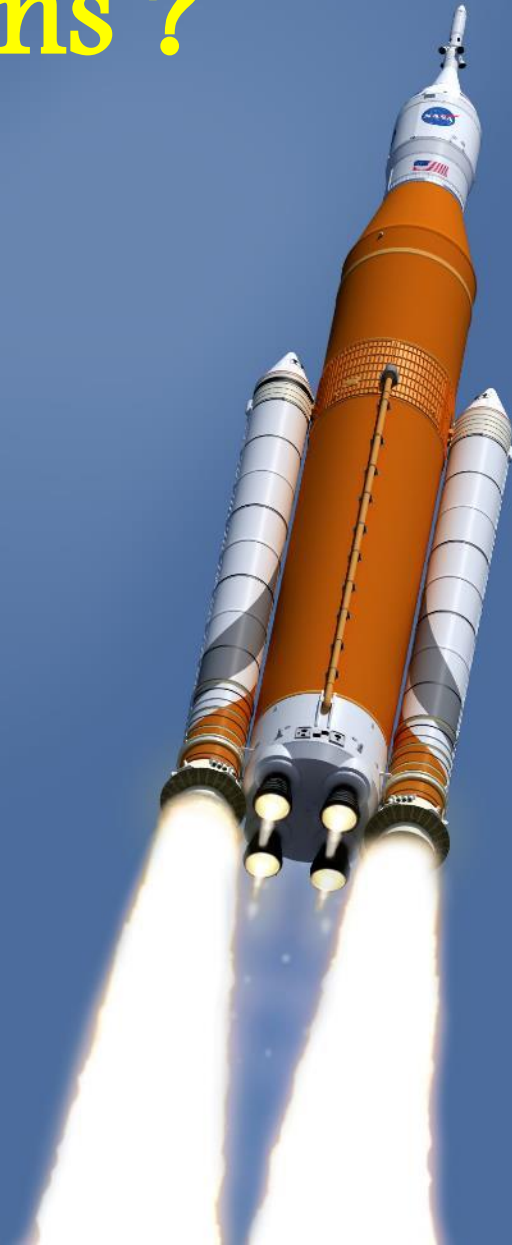
- **FSL I - IV:**
 - NPR 1620.2 provides evaluation guidelines
 - NPR 1620.3 provides protection requirements by facility type/level
 - Access controlled by EPACS/NAMS (BLA3 Center common)
 - So what? Now very difficult to manipulate locally
 - Enhanced protections for NCI (B648, B1236, B1265)
 - Waivers require AA / OPS approval
 - Issue for visitors / summer students



Level of Risk/Level of Confidence Matrix

Logical Description Examples	Physical Risk Description	Physical Description Examples	Position Risk	Position Sensitivity	Level of Risk	Level of Confidence Required	Netting Required to Establish Confidence	Level of Assurance Required	Minimum Credentials Allowed for Logical Access	Type of Logical Authentication Required	Minimum Credentials Allowed for Physical Access	Type of Physical Authentication Required	Physical Access Readers Required
User is prevented from requesting IT access.	No access allowed to NASA facilities.	User is prevented from requesting physical access.	None	None	-5	-5	N/A	N/A	N/A	N/A	N/A	N/A	N/A
User requires no logical access.	No current access to NASA facilities.	User requires no physical access.			0	0	None	0	No Credential	None	N/A	N/A	N/A
This asset presents a very low risk to the Agency. Examples include SATERN and WebEx.	Public access only	This asset presents a very low risk to the agency. Examples include access roads and "open" events.	None	None	10	10	None - Claimed Identity	1 (10)	None, Anonymous/Guest, or UserID/Password	One Factor	Visitor Badge	Visual	N/A
This asset presents a very low risk to the Agency. Examples include basic tools such as E-mail, desktop applications, and access to their own privacy data.	Open facilities	This asset presents a low risk to the Agency. Examples include "open" facilities such as cafeterias and gyms.			20	20	Name Check w/o Identity Proofing	2 (20)	UserID/Password, Visitor Badge	One Factor	Visitor Badge	Visual	N/A
This asset presents a very low risk to the Agency. Examples include tools requiring in-person proofing such as PKI encryption and signing certificates, and LoA 2 and 3 credentials.	Unrestricted facilities	This asset presents a low risk to the Agency. Examples include facilities that require card reader access to enter, such as a day care or parking garage.			30	30	Identity Proofing with Fingerprint Check	3 (30)	RSA Token	Two Factor	Local Badge	Prox	R40
This asset presents a low risk to the Agency. Examples include user level access to smartcard authenticated employee/worker IT resources such as NASA business systems, desktop computers, access to a limited amount of privacy data, and/or elevated privileges on their own workstation. Users will normally obtain and utilize a PIV credential to access these assets. Allows access to an asset (without a flag) by an individual who has a submitted but not completed investigation.	Controlled facilities	This asset presents a low risk to the Agency. Examples include unrestricted access to NASA center perimeters and administrative facilities. Users will normally obtain and utilize a PIV credential to access these assets. Allows access to an asset (without a flag) by an individual who has a submitted but not completed investigation.	Any of the below	Any of the below	35	35	Investigation Submitted		Smartcard		Smartcard, Local Badge on Exception	PKI-CAK	R40
This asset presents a low risk to the Agency. Examples include user level access to smartcard authenticated employee/worker IT resources such as NASA business systems, desktop computers, access to a limited amount of privacy data, and/or elevated privileges on their own workstation. Users will normally obtain and utilize a PIV credential to access these assets.	Controlled facilities	This asset presents a low risk to the Agency. Examples include unrestricted access to NASA center perimeters and administrative facilities. Users will normally obtain and utilize a PIV credential to access these assets.	Low	Non-Sensitive	40	40	OPM Tier 1		Smartcard		Smartcard	PKI-CAK	R40
This asset presents a moderate risk to the Agency. Examples include privileged level access to Agency and/or center unclassified IT resources such as ICAM infrastructure, or unlimited access to systems containing sensitive data such as privacy, SBU, and ITAR/EAR data. Users are required to utilize a PIV credential to access these assets.	Limited / NCI facilities	This asset presents a moderate risk to the Agency. Examples include NASA critical infrastructure (NCI), data centers and server rooms, SBU/ITAR/EAR storage areas, and electrical infrastructure. This access can include additional approval and training.	Moderate	Non-Sensitive	50	50	OPM Tier 2	4 (40)	PIV Smartcard	Hard Crypto two-factor	PIV Smartcard	PIV Auth	RKCL40
This asset presents a moderate risk to the Agency and to National Security. Examples include user or privileged level access to NASA CLASSIFIED IT resources such as SIPRNET terminals and infrastructure. Access requires a completed background investigation and clearance. Requires a signed DD-254 for contract employees.	Limited facilities w/ national security (SECRET)	This asset presents a moderate risk to the Agency and National Security. He/she will need to have a completed background investigation and clearance before access will be granted. Examples include SECRET reading rooms and classified storage areas.		Non-Critical Sensitive	55	55	OPM Tier 3		Classified network credential		PIV Smartcard	PIV Auth	RKCL40
This asset presents a high risk to the Agency. The user will need access to systems that the compromise of could cause severe harm to the Agency and/or mission. Examples include privileged level access to high risk NASA IT resources such as command and control systems, human flight and safety systems, EPACS regional and application administrative, and credential production systems. Users are required to utilize a PIV credential to access these assets.	Exclusion facilities	This asset presents a high risk to the Agency. Examples include areas with hazardous materials, weapons, and/or explosives, areas with NASA critical IT infrastructure, areas storing investigation information and materials for producing credentials.	High	Non-Sensitive	60	60	OPM Tier 4		PIV Smartcard		PIV Smartcard	PIV Auth w/Bio	RKCLB40
This asset presents a very high risk to the Agency and to National Security. Examples include user or privileged level access to TOP SECRET NASA IT resources such as JWICS terminals and infrastructure. Access requires a completed background investigation and clearance. Requires a signed DD-254 for contract employees.	Exclusion facilities w/ national security (TOP SECRET)	This asset presents a very high risk to the Agency and National Security. He/she will need to have a completed background investigation and clearance before access will be granted. Examples include		Critical/ Special Sensitive	70	70	OPM Tier 5		Classified network credential		PIV Smartcard	PIV Auth w/Bio	RKCLB40

Questions ?





Virginia Information Technologies Agency

Willis Zhang, Google





Virginia Information Technologies Agency

Upcoming Events





WILLIS ZHANG

Customer Engineer, Google Cloud

CONTACT

williszhang@google.com



[linkedin.com/in/zhangwillis](https://www.linkedin.com/in/zhangwillis)



ABOUT ME

Willis provides technical solutions to state and local governments looking to innovate using what's available in public cloud. He advises government officials on how to achieve reliable, cost-effective, and secure architectures for specific use cases that benefit local communities such as improving access to public services and securing local elections.

Prior to Google, Willis did consulting work with Accenture and Protiviti and helped large commercial businesses with their cloud adoption strategy – whether on public or hybrid cloud. He contributed to many successful IT transformations including virtualizing and migrating environments to the cloud.

**CONFIDENTIAL AND PROPRIETARY
MAY NOT USE WITHOUT PERMISSION**

Hello, Virginia!



Data Protection in the Cloud

williszhang@

Feb 6, 2019

Speaker's promises

1. Industry best practices
2. Be as straightforward as possible



Our journey today

The public internet

Cloud
applications

Cloud
infrastructure

The public internet

Cloud applications 

Cloud
infrastructure

End-user risk is a fact of life

Phishing attacks

91%

of attacks start with a phishing email.¹

Targeted threats are extremely tough to detect.

Malicious attachments

66%

of malware was installed via malicious emails & attachments.²

4.3x

More malware received by corporate inbox than end-user inbox.

Attackers rapidly change tactics to defeat email security measures.

Data breach

90%

of all reported breaches caused by employee negligence, extortion, & external threats.³

Lack of admin controls on user emails makes remediation particularly hard.

Ransomware

15x

increase in ransomware losses from 2015-2017.⁴

Inconsistent back-ups increase the risk of business continuity.

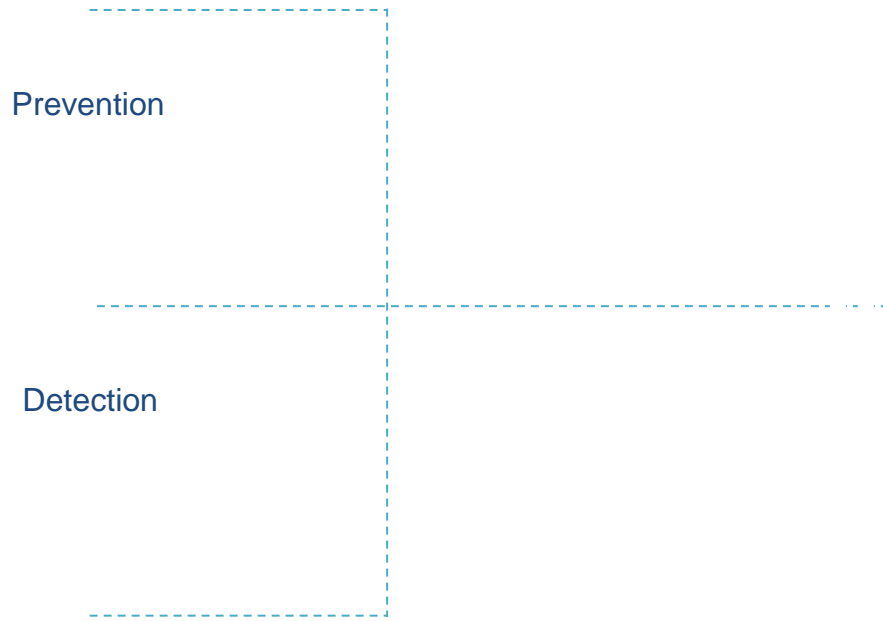
¹ [Enterprise Phishing Susceptibility and Resiliency Report, Cofense](#)

² [Verizon DBIR 2017](#)

³ [Willis Towers Watson 2017 Cyber Risk Survey](#)

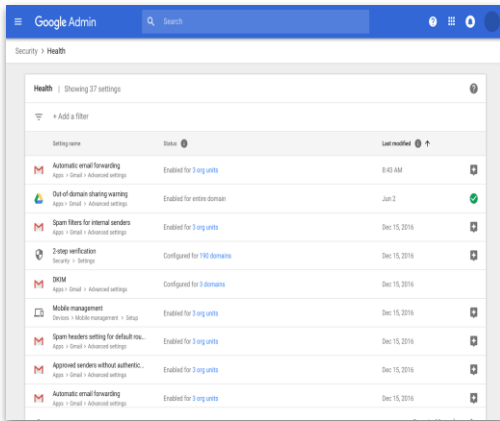
⁴ [2017 Cybercrime Report, Cybersecurity Ventures](#)

Endpoint protection lifecycle



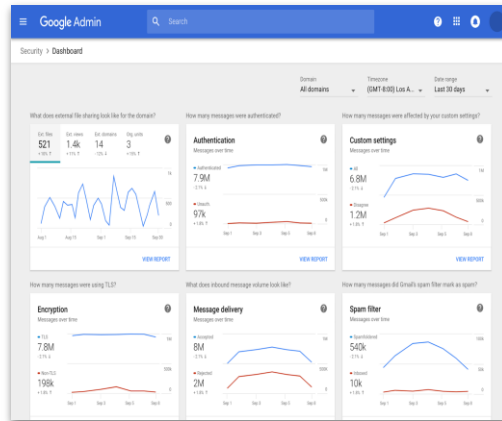
Remediation

G Suite Security Center



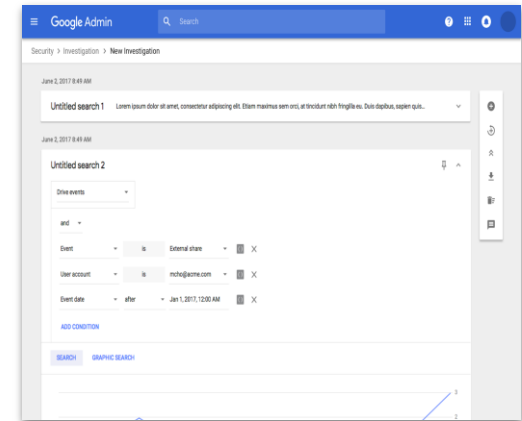
Security health

Help admins manage and improve the security posture of their domain (e.g. proactive phishing protection).



Security dashboards

Provide admins and IT decision makers with actionable security insights (e.g. phishing risks).



Investigation tool

Help analysts and admins diagnose, triage and resolve security issues across G Suite.

1

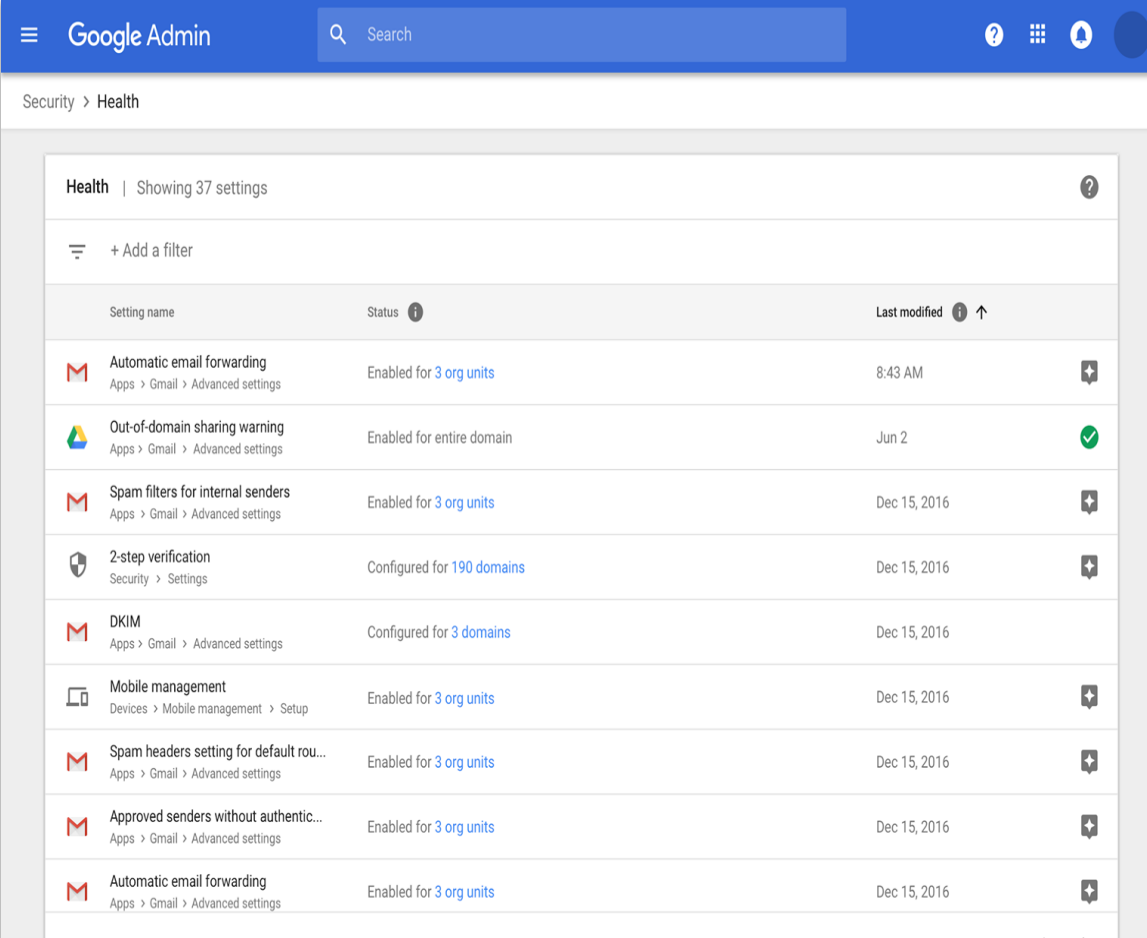
Prevention

Preventing incidents before they happen










Security Health

Advice on **security best practices** for content, communication, mobility and user security.

Recommended security settings that outline consequences of inaction to **help you be more proactive.**



The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo, a search bar, and utility icons. Below the header, the breadcrumb path is 'Security > Health'. The main content area is titled 'Health | Showing 37 settings' and contains a table of security settings. The table has columns for 'Setting name', 'Status', and 'Last modified'. Each row includes a status icon (e.g., a shield for '2-step verification', a checkmark for 'Out-of-domain sharing warning') and a plus icon for more options.

Setting name	Status	Last modified
 Automatic email forwarding Apps > Gmail > Advanced settings	Enabled for 3 org units	8:43 AM
 Out-of-domain sharing warning Apps > Gmail > Advanced settings	Enabled for entire domain	Jun 2
 Spam filters for internal senders Apps > Gmail > Advanced settings	Enabled for 3 org units	Dec 15, 2016
 2-step verification Security > Settings	Configured for 190 domains	Dec 15, 2016
 DKIM Apps > Gmail > Advanced settings	Configured for 3 domains	Dec 15, 2016
 Mobile management Devices > Mobile management > Setup	Enabled for 3 org units	Dec 15, 2016
 Spam headers setting for default rou... Apps > Gmail > Advanced settings	Enabled for 3 org units	Dec 15, 2016
 Approved senders without authentic... Apps > Gmail > Advanced settings	Enabled for 3 org units	Dec 15, 2016
 Automatic email forwarding Apps > Gmail > Advanced settings	Enabled for 3 org units	Dec 15, 2016

Security health

Gmail

Checks around automatic email forwarding, DMARC settings, POP/IMAP access, whitelists

Drive

Apply policies around file sharing, Drive add-ons, offline availability, stringent sign-in requirements

Device Management

Comprehensive action list for Mobile Device Management to mandate secure access

Users

Understand how 2-step verification is being used across users and admins

Hangouts

Checks around out of domain Hangout warnings being in place for all users

Sites and Groups

Check group sharing options and allow public groups on a case by case basis



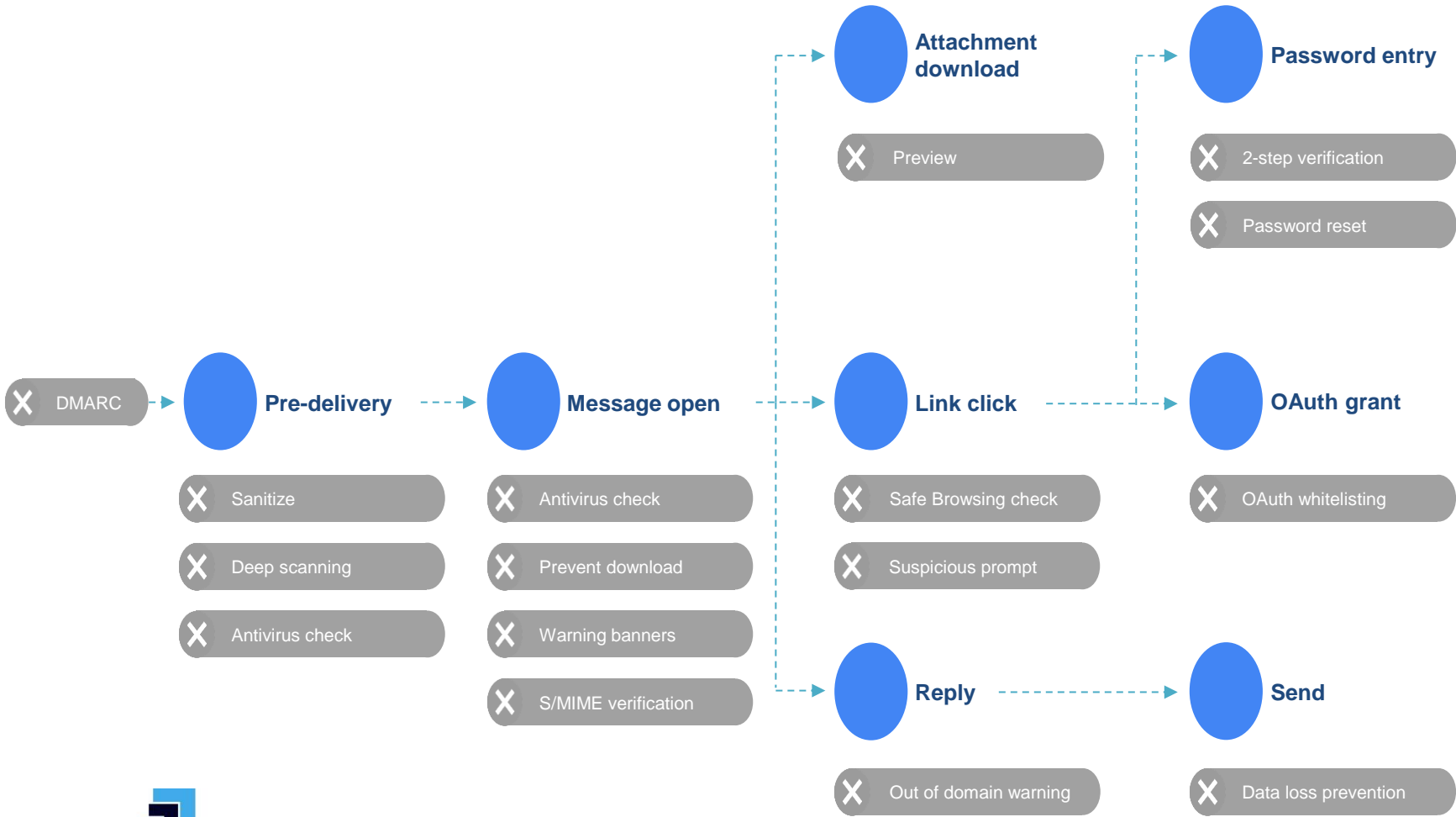
2SV and security keys

Prevent phishing

Security Keys are still the most effective protection we have against phishing.



Gmail phishing and malware protection



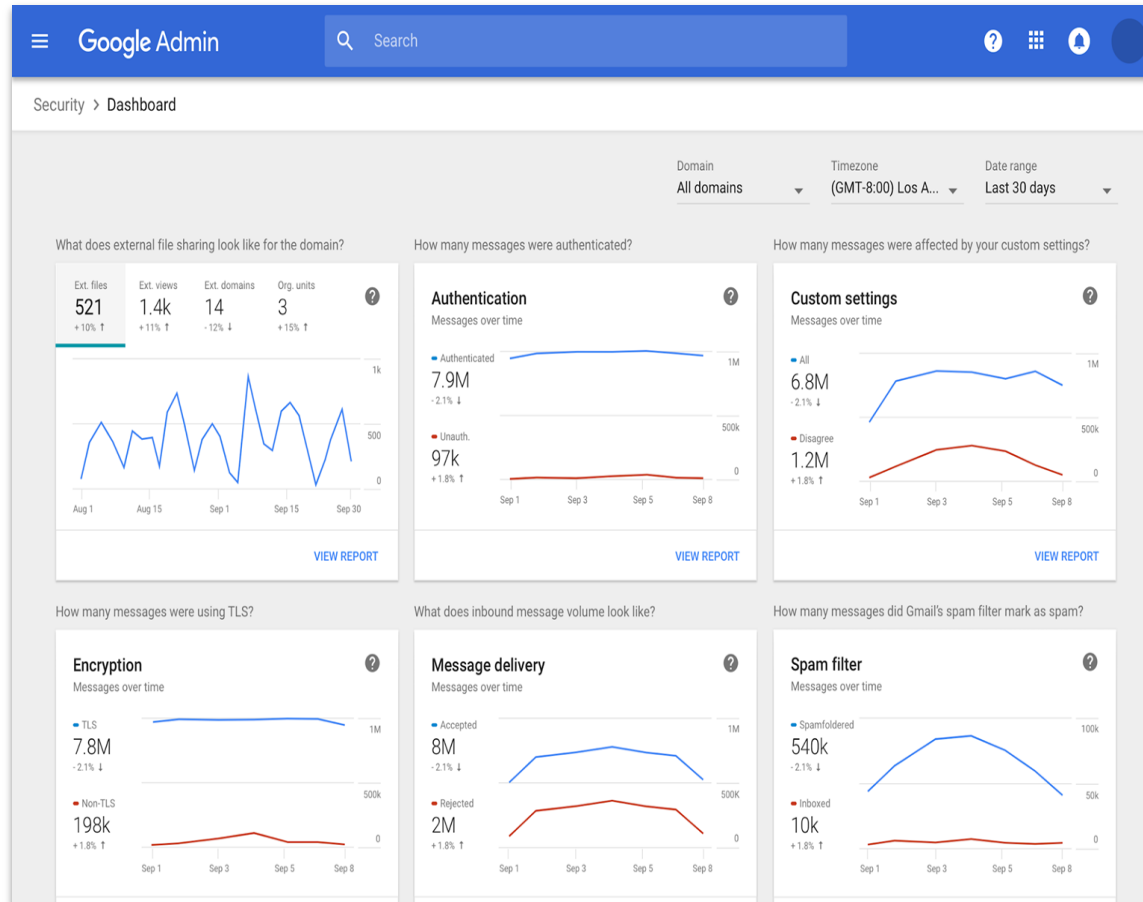
2

Detection

Detect incidents as they happen

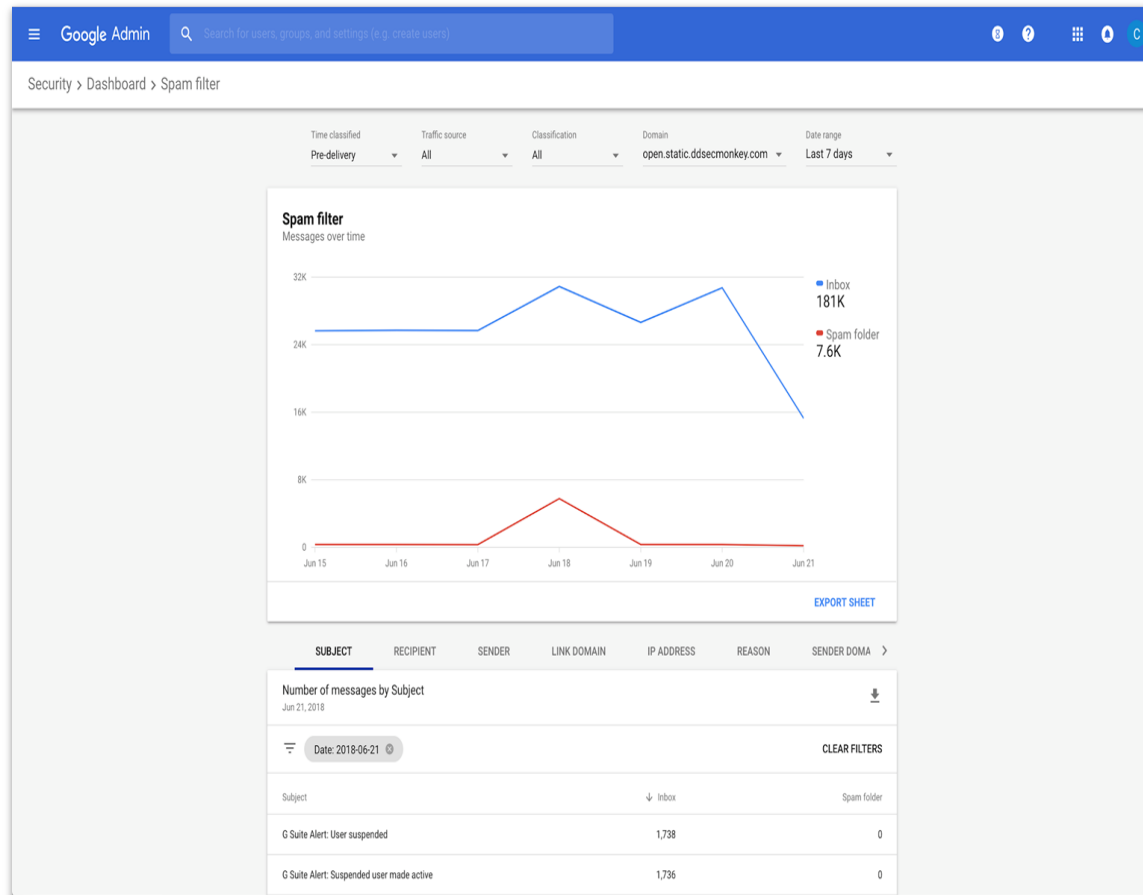
Security dashboards

High-level metrics that give the user a pulse of security-related data within their domain



Security dashboards

Drill into individual charts to explore data and find actionable insights.



Security dashboards & insights

File exposure

Know which files have been shared outside your domain and the DLP rules that have been triggered on the shared files.

Authentication

Find out how many messages don't meet your authentication standards - DMARC, DKIM, SPF.

Encryption

Ensure that that messages sent by your domain are encrypted by TLS. Info on domains that are sending unencrypted messages to you.

Email delivery

See what percentage of incoming messages were accepted and whether whitelisting caused any suspicious messages to get delivered.

Spam and malware classification

Deeper dive into messages spam, phishing, suspicious or malware.

User perception

Re-evaluate whitelists by finding out whether users are tagging delivered messages as spam/not spam or phishing.



3rd party apps whitelisting

Control OAuth applications access to users' data

- . Ensure users can only authorize trusted OAuth apps
- . Control any OAuth app across all platforms (Web, iOS, Android)

3

Remediation

Diagnose, triage and resolve incidents

Investigation Tool

Perform **advanced queries** over many different data sources.

Pivot between different sources to see how data correlates.

Bulk actions to remediate issues quickly when they are identified.

Google Admin Search

Security > Investigation

Search 1
superadmin@acme.com

Data source: Gmail log events

AND

Condition: Date After Date: 2017-08-30T00:00:00-0800
Pacific standard time. [Edit](#)

Condition: Date Before Date: 2017-08-31T00:00:00-0800
Pacific standard time. [Edit](#)

Condition: Traffic source Is Traffic source: Inbound

Condition: Domain Is Domain: seconddomain.com

Condition: Authentication Is Authentication: Unauthenticated

ADD CONDITION

SEARCH

Showing 1-30 of many results

Date	Message ID	Subject	Event	Sender
2017-12-11T15:49:04-0800	74629F...me.com	Dancing santa news	Received	really.long.name@acme.com
2017-12-11T15:49:04-0800	50564D...me.com	Have you seen the dancing santa?	Received	really.long.name@acme.com
2017-12-11T15:49:04-0800	02889R...me.com	Dancing Santa comes to town	Received	really.long.name@acme.com
2017-12-11T15:49:04-0800	92821V...me.com	There's a dancing santa on the couch	Received	really.long.name@acme.com
2017-12-11T15:49:04-0800	84727A...me.com	Dancing santa	Received	really.long.name@acme.com
2017-12-11T15:49:04-0800	77212Q...me.com	Dancing santa working it out	Received	really.long.name@acme.com

Large fault tolerance actions

Large sets of data

- Performing actions on a selected set of entities or an unbounded set of data defined by a query

Reliable execution

- Large scale execution may take long time
- Execution is carefully tracked and can survive intermittent hardware failures
- Results are available for review

Feedback on status of bulk actions

YOUR TASKS OTHERS' TASKS

Completed

- ✓ Erase messages action completed.
Hide details
[View results](#)
Total attempted: 8
Successes: 8
Failures: 0
Started on Jul 2, 2018, 3:53:29 PM
Completed on Jul 2, 2018, 3:53:38 PM
- ✓ Erase messages action completed.
See details
- ✓ Erase messages action completed.
See details
- ✓ Erase messages action completed.
See details

Long-Running Task Pane

Track the status of your current and pending actions

Erasure task completed.

Showing 1-8 of 8 results

Date	Message ID	Subject	Owner	Result
2018-07-02T15:53:37-07:00	<CABZ...all.com>	Test Erase	corp2@open.static.ddsecmo...	✓ The message was successfully erased.
2018-07-02T15:53:35-07:00	<CABZ...all.com>	Test Erase	invisible@open.static.ddsec...	✓ The message was successfully erased.
2018-07-02T15:53:35-07:00	<CABZ...all.com>	Test Erase	corp3@open.static.ddsecmo...	✓ The message was successfully erased.
2018-07-02T15:53:34-07:00	<CABZ...all.com>	Test Erase	demo@open.static.ddsecmo...	✓ The message was successfully erased.
2018-07-02T15:53:34-07:00	<CABZ...all.com>	Test Erase	corp1@open.static.ddsecmo...	✓ The message was successfully erased.
2018-07-02T15:53:32-07:00	<CABZ...all.com>	Test Erase	modifiableuser1@open.static...	✓ The message was successfully erased.
2018-07-02T15:53:32-07:00	<CABZ...all.com>	Test Erase	annie1@open.static.ddsecm...	✓ The message was successfully erased.
2018-07-02T15:53:32-07:00	<CABZ...all.com>	Test Erase	annie2@open.static.ddsecm...	✓ The message was successfully erased.

Rows per page: 30 Page 1 of 1

Task Result Card

A granular view of the outcome of your action

The public internet

Data loss prevention
(DLP)

Cloud
applications



Protecting sensitive data: goals

Use sensitive data properly

- least privilege
- need-to-know

Be accountable

- demonstrate proper use
- Monitor, audit, remediate

Maintain strong governance as business and data grows

Minimal hindrance on business and services to users

Examples of sensitive data

Examples:

- Personally Identifiable Information (PII)
- Financial Data
- Health Data

Formats:

- Documents or Images
- Databases and production systems

Common Sources:

- Data collected from or about your users
- Data collected from or about employees
- Data shared to/from partners

PII:

Name

Email address

Phone number

Social Security number



Handling sensitive data
begins with knowing where
your sensitive data exists



Ensure governance across the data life cycle

Know where sensitive data is:

- Collected & stored
- Processed
- Used for analytics
- Shared with partners
- Retained / deleted

Address areas where sensitive data might be inadvertently collected

Let's walk through a scenario

Your company manages customers orders and provides customer support. You are going to build a new ML-based support bot that will wow your users. You want to make sure that you are properly handling customer sensitive data.

You want to do the following:

- **Scan:** Discover where sensitive data exists in your cloud project.
- **Real-time redaction:** Remediate unexpected collection.
- **De-identification and risk analysis:** Share data for internal and external analysis.

DLP = Data Loss Prevention

Identify sensitive data and prevent it from being overexposed or leaking into areas where it should not be.



Predefined content detectors

Detectors for PII, e.g., Credit Card, License #, etc. in _ countries

Custom rules

Easy to create custom rules with keywords and regular expressions

Optical Character Recognition (OCR)

Common image types and scanned documents are analyzed for DLP

Content thresholds

Reduce false positives with custom frequency and confidence thresholds

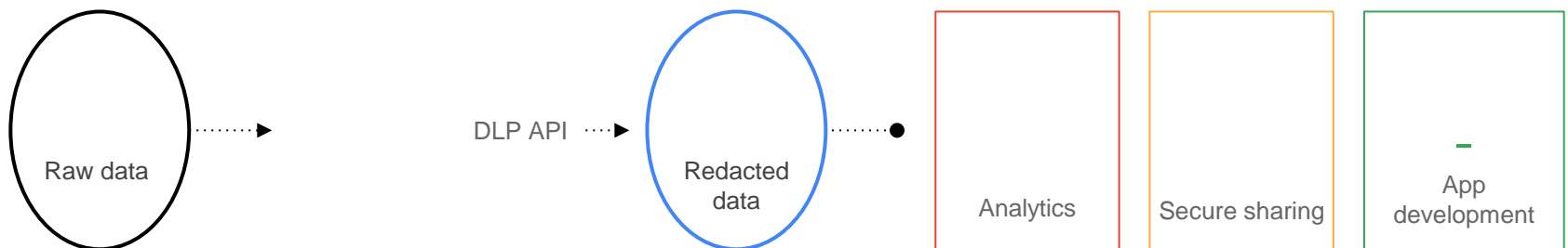


Cloud DLP API

<https://cloud.google.com/dlp/>

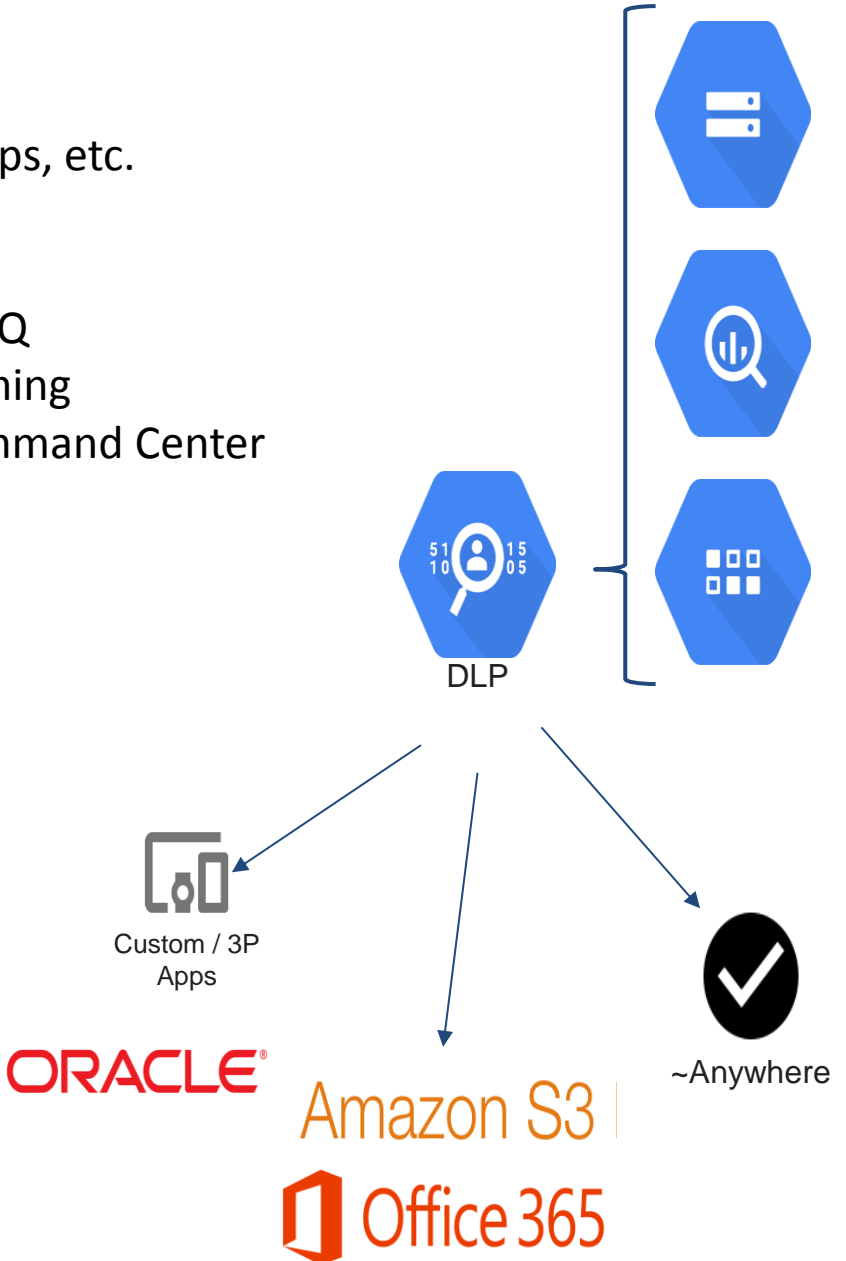
Provides capabilities:

- **Classification** of sensitive data like Personally Identifiable Information (PII)
- Data masking, format-preserving encryption, **transformations**
- Re-identification risk analysis (k-anonymity)



Use it anywhere

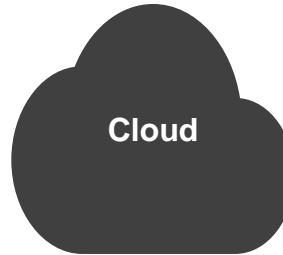
- Send content anywhere → S3, On-prem, 3P Apps, etc.
 - Processed in Cloud but no data stored.
- Scan (at scale) data stored in GCS, Datastore, BQ
 - Native support for GCP, more systems coming
 - Alpha integration with Cloud Security Command Center



Where do I have sensitive
data
in my cloud storage?



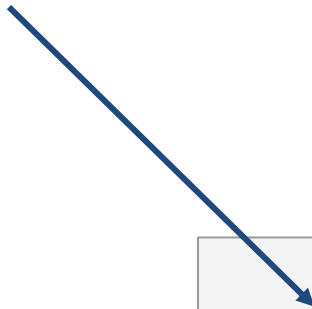
“Where do I have sensitive data in my cloud storage?”



Folders and files in Cloud Storage



Cloud tables



	COUNT	FINDINGS
st5/Flagged Customer Activity.csv	9	EMAIL_ADDRESS
st5/Customer Feedback 2017-05-01 133111.txt	2	EMAIL_ADDRESS,CREDIT_CARD_NUMBER
st5/Account Application 124vja8sje0asj.txt	2	US_SOCIAL_SECURITY_NUMBER,CREDIT_CARD_NUMBER
st5/Account Application 8jdj28s8sjd.txt	2	US_SOCIAL_SECURITY_NUMBER,CREDIT_CARD_NUMBER



(DLP) API

DeID: Dynamic Masking and Redaction



Redacting and masking

Input → “This is my phone number: (858)867-5309”

Partial Masking

Output → “This is my phone number: (858)XXX-XXXX”

Hashing or Tokenizing



Output → “This is my phone number: ga+32mx32s2as8cw38AEfknsFthc”

Format Preserving Encryption or Tokenization



Output → “This is my phone number: (858)582-6528”





Classifying data in a custom and 3rd-party apps

Original Chat

Hi! My name's Neal. What can I do for you?



My anvil doesn't work properly.



Let's get started. What's your name, contact number, and the last four digits of your social?



My name is Alice and my phone number is (415) 555-5555, and my social is 123-45-6789.



And my email is alice@imadethisup.com.



Here's my SSN card. Does that help?



Chat...

END CHAT



Original Chat

Hi! My name's Neal. What can I do for you?

My anvil doesn't work properly.

Let's get started. What's your name, contact number, and the last four digits of your social?

My name is Alice and my phone number is (415) 555-5555, and my social is 123-45-6789.

And my email is alice@imadethisup.com.

Here's my SSN card. Does that help?



Chat...

END CHAT

After DLP API redaction

Hi! My name's Neal. What can I do for you?

My anvil doesn't work properly.

Let's get started. What's your name, contact number, and the last four digits of your social?

My name is Alice and my phone number is (415) ###-####, and my social is ###-##-6789.

And my email is [EMAIL_ADDRESS].

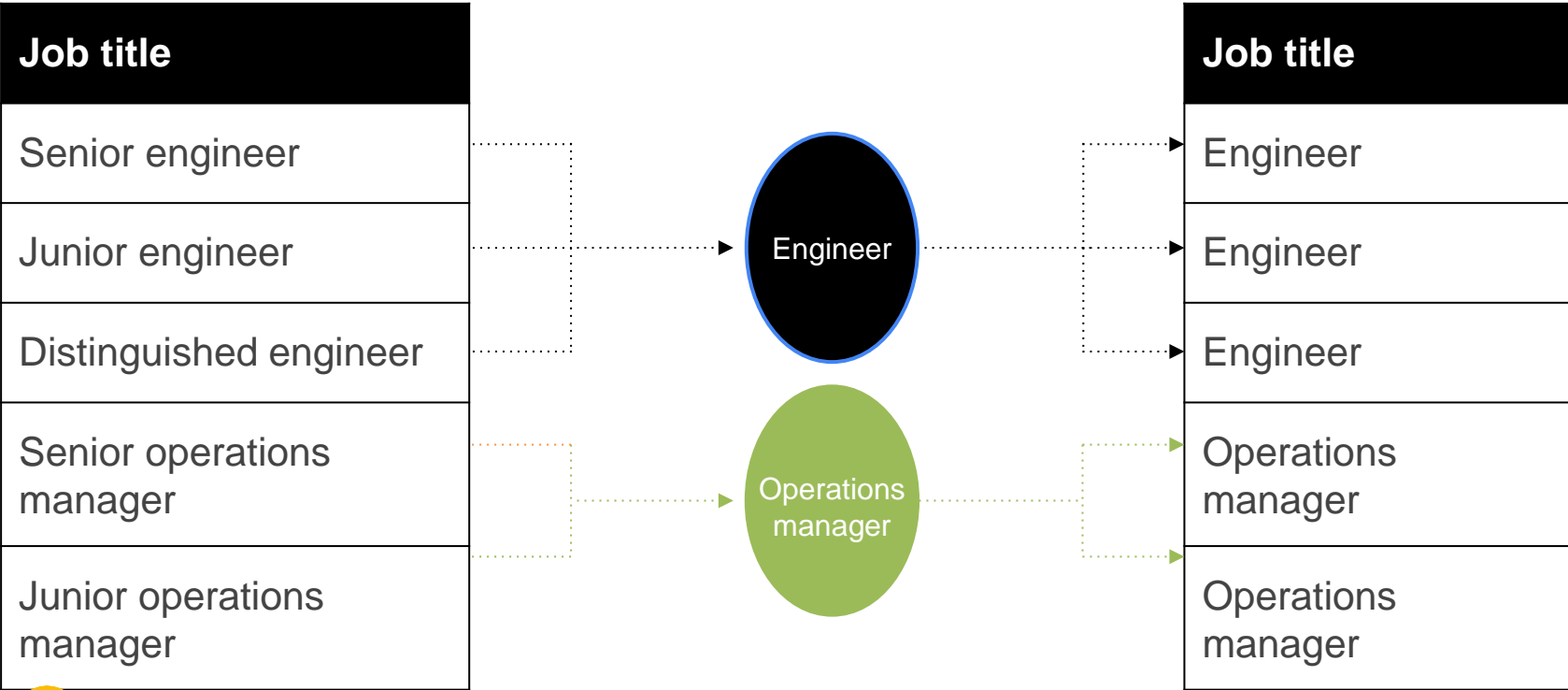
Here's my SSN card. Does that help?



DONE

Masked data on collection

De-ID: Data bucketing



More **specific** or **distinguishing** values can be bucketed into more **general** values to help retain value but reduce re-identification risk.

How quasi-identifiers can be a risk

We want to make sure that the remaining columns don't identify anyone, so we don't have combinations of age and zip that map to one person or a small group.

Maybe this is the only 81 year old in 24946 in your dataset

Row	userid	zipcode	age	happiness
1	121317763	24946	38	4
2	121317445	24946	81	100
3	121317866	24946	41	52
4	121317863	24946	41	94
5	121317241	24946	41	36

How do we measure this kind of risk?

K-anonymity

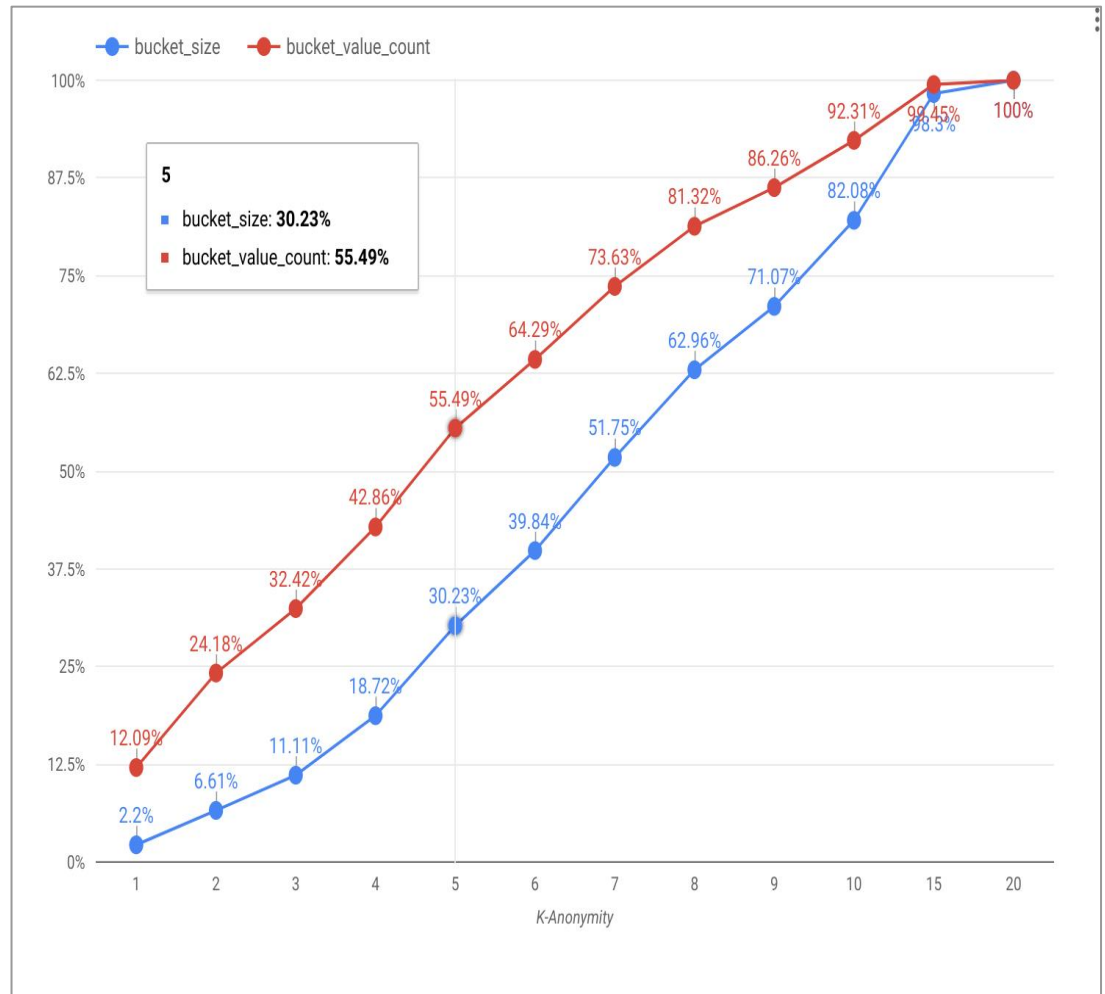
How many people share the same set of quasi-identifiers:
age and zip.

Goal

For our policy, we want a $k \approx 10$



K-anonymity results for *age + zipcode*



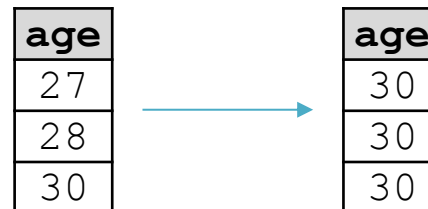
How do we fix this?

With zip + age, we clearly have a problem

- Most/all of the data maps to $k < 10$.
- If we just dump those rows we lose nearly 100% of our data.

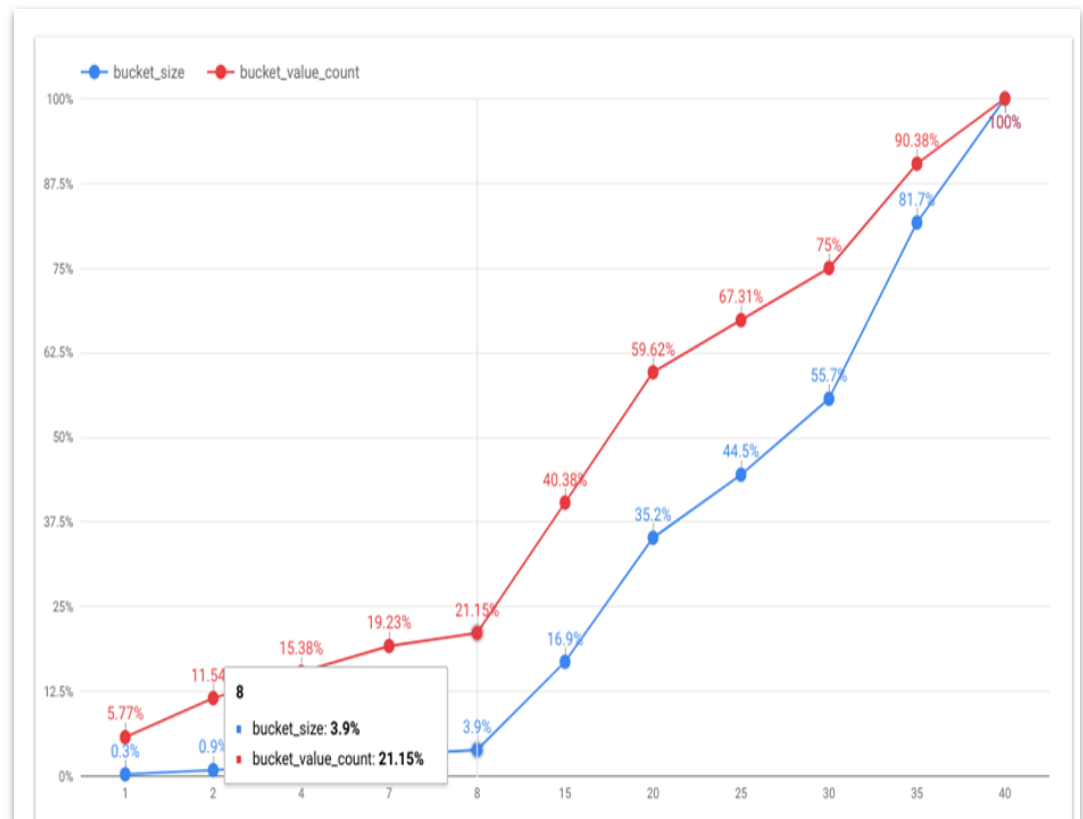
Solution

- Generalization: Using the DLP API *bucketing* transformation.



Results after bucketing for *age* + *zipcode*

After bucketing we can meet our K>10.



The public internet

Cloud
applications

Cloud
infrastructure



Infrastructure protection

Control

- IAM
- Roles
- Service Accounts

Security Solutions

Building services into secure platforms and tools

Visibility

- Logging
- Monitoring



1 Control

IAM / Cloud Identity

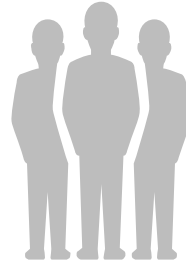


In cloud-based services the importance of roles and permissions is amplified



Identity and Access Management

Who



can do what



on which resources



Manage access to resources

... under which conditions

Use Groups, with logical names



Users

Groups

IAM roles

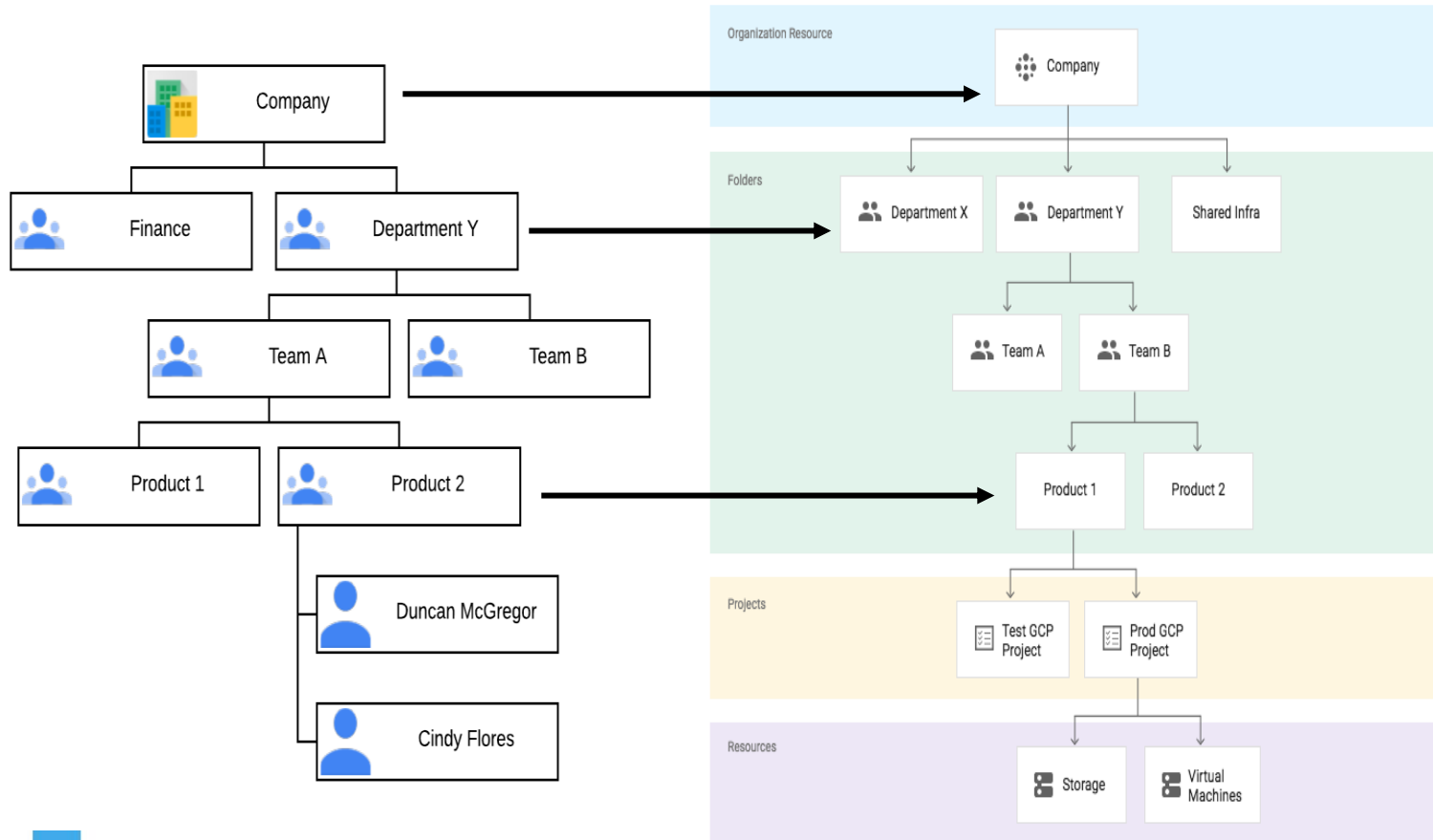
Resources

**Global
SecOps
Admins**

- **Security admin**
- **Log viewer**

**Example.com
organization**

Match resources to company structure



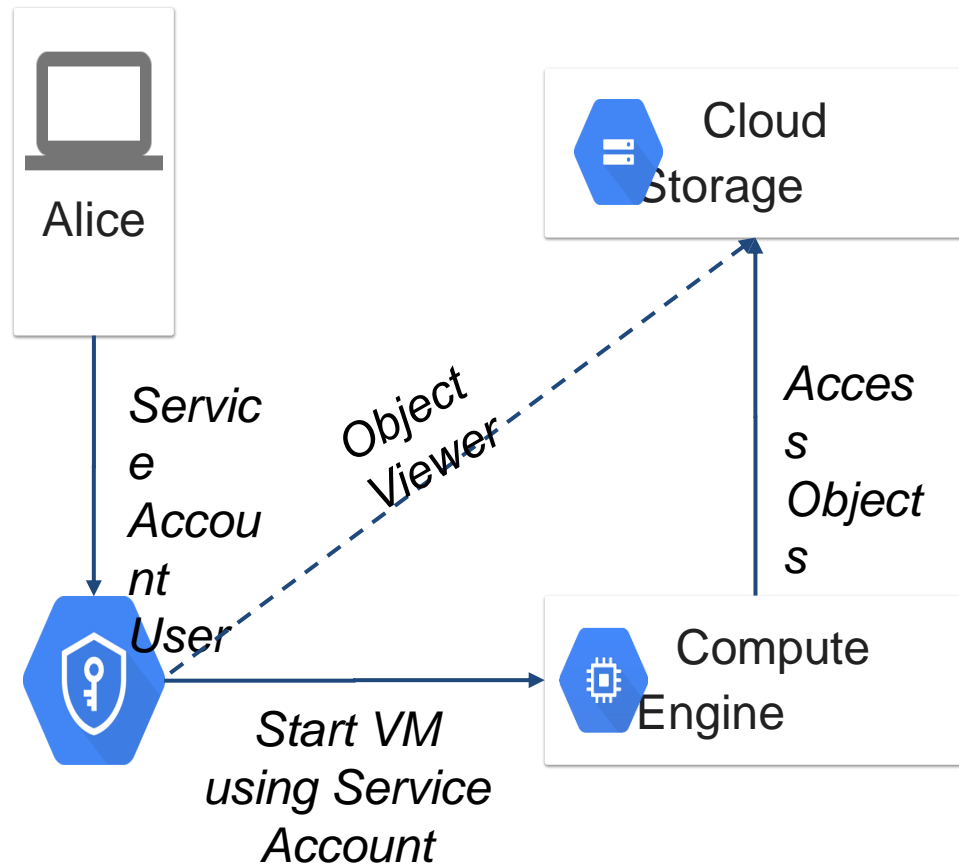
TIP

Verbose project names provide clarity on resource structure and ownership

acme-sales-clientinsight-prod

Service Accounts

Service Accounts are both an Resource *and* a Identity



Service Account Tips



- Have a naming convention
- **svc-insight-reporting-api@**
acme-sales-clientinsight-
prod
.iam.gserviceaccount.com
- Use the Display Name for the *purpose* of each Service Account

How many Service Accounts?



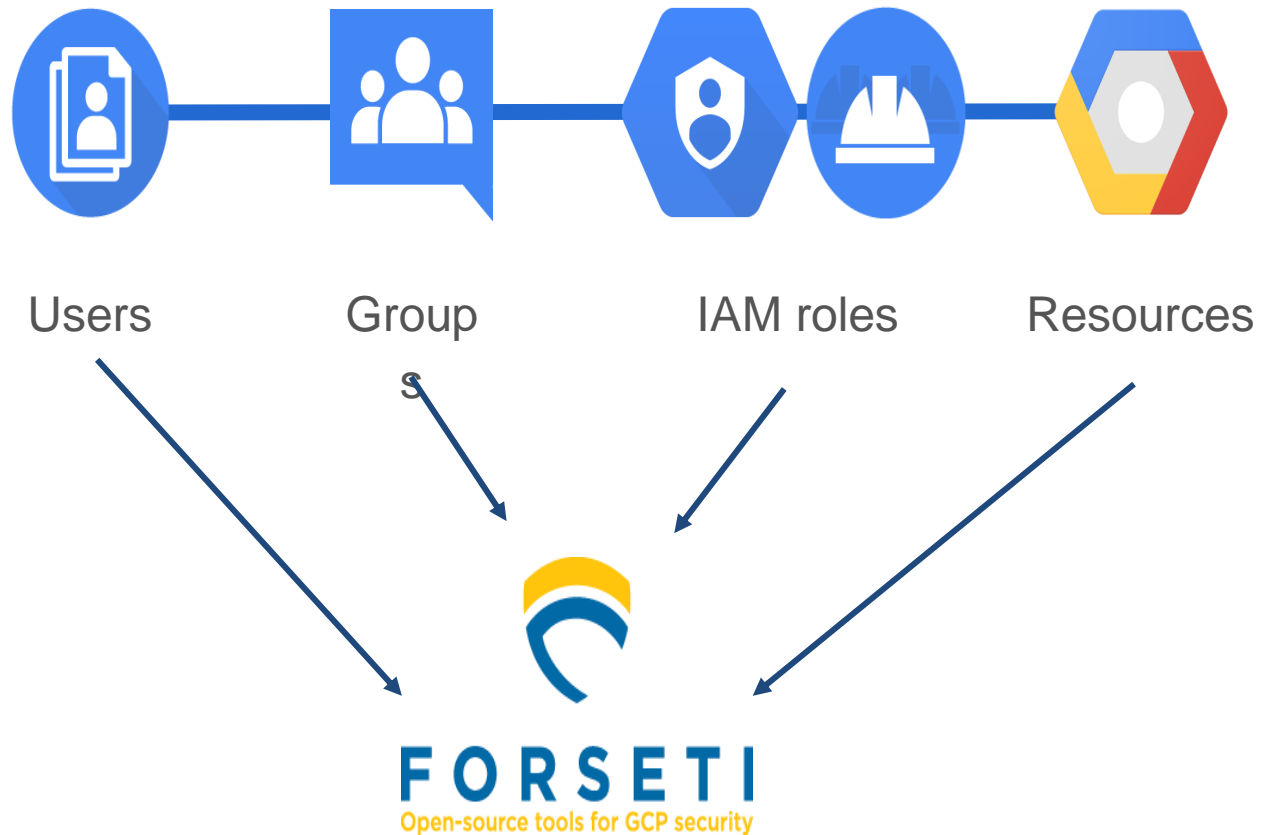
- Create one service account for each of your services
- Allow access to only the required Resources and scopes
- Needing many Roles hints at refactoring

TIP

Don't rely on default Service Accounts

Who can access which resources?

Forseti Explain shows relationship between Users, Groups, Roles, Permissions and Resources



2 Visibility

Logging and Monitoring



- Monitoring generally for Ops
- Logging used by Devs, Ops AND Security

Full Audit Logging visibility

Admin Activity Logs

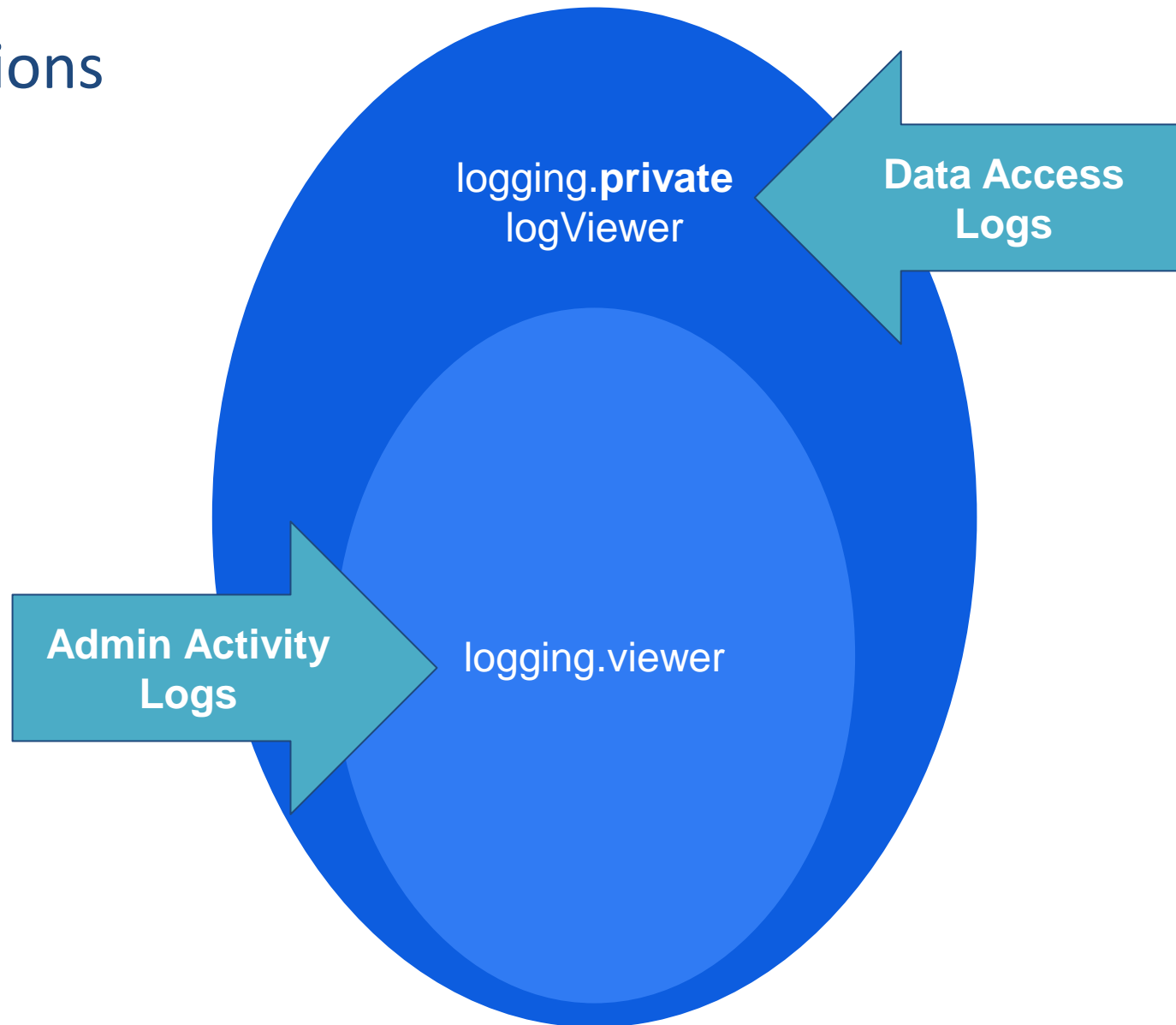
- API calls and config changes
- Always on
- \$0

Data Access Logs

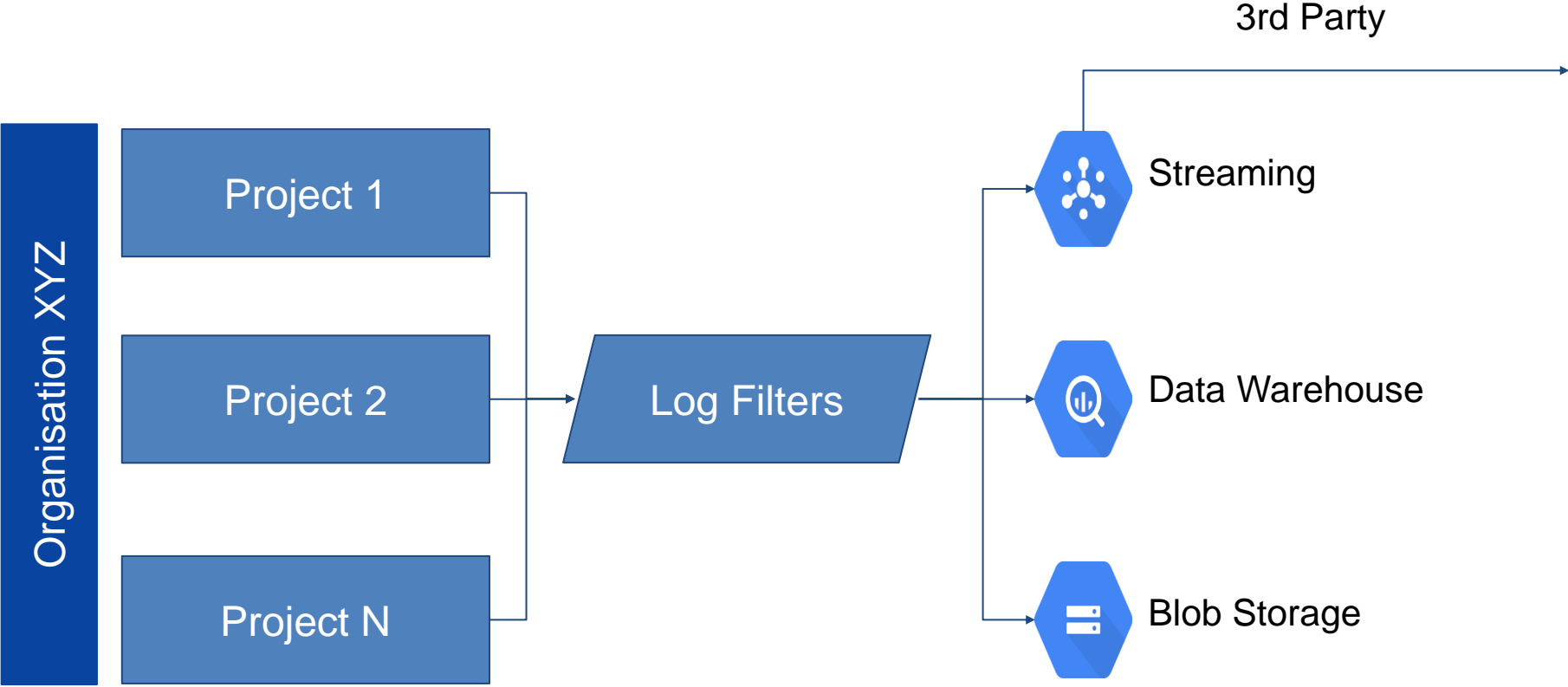
- READ/WRITE of user data
- Warning: can be large!
- **Off by default**



Permissions



Aggregated Log Exports



TIP

Protect against accidental deletion of log files in Cloud Storage using **Object Versioning**

TIP

Protect your log storage project from accidental deletion using a **Lien**

3

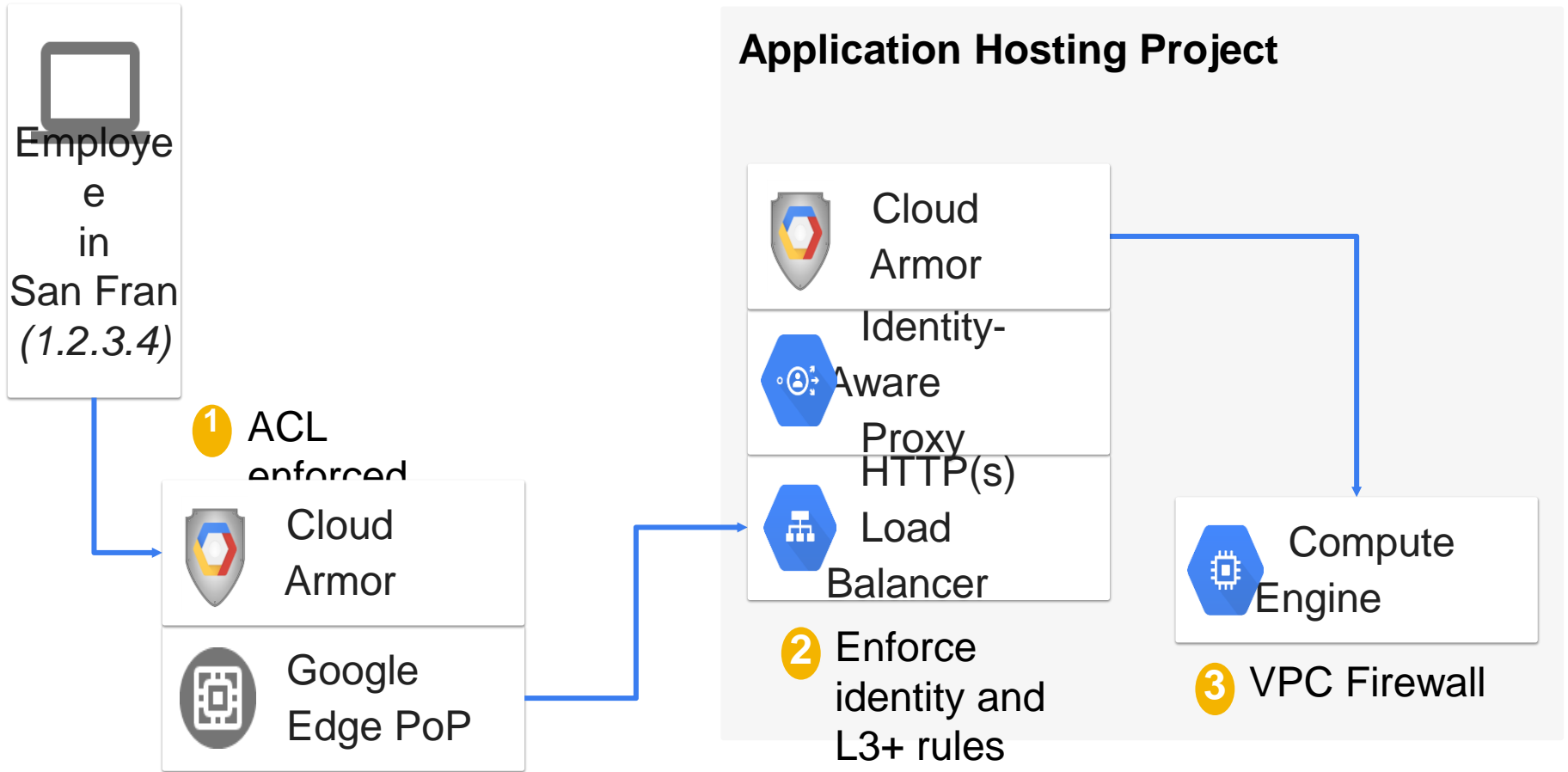
Security Solutions

How can I run corporate services without a VPN?

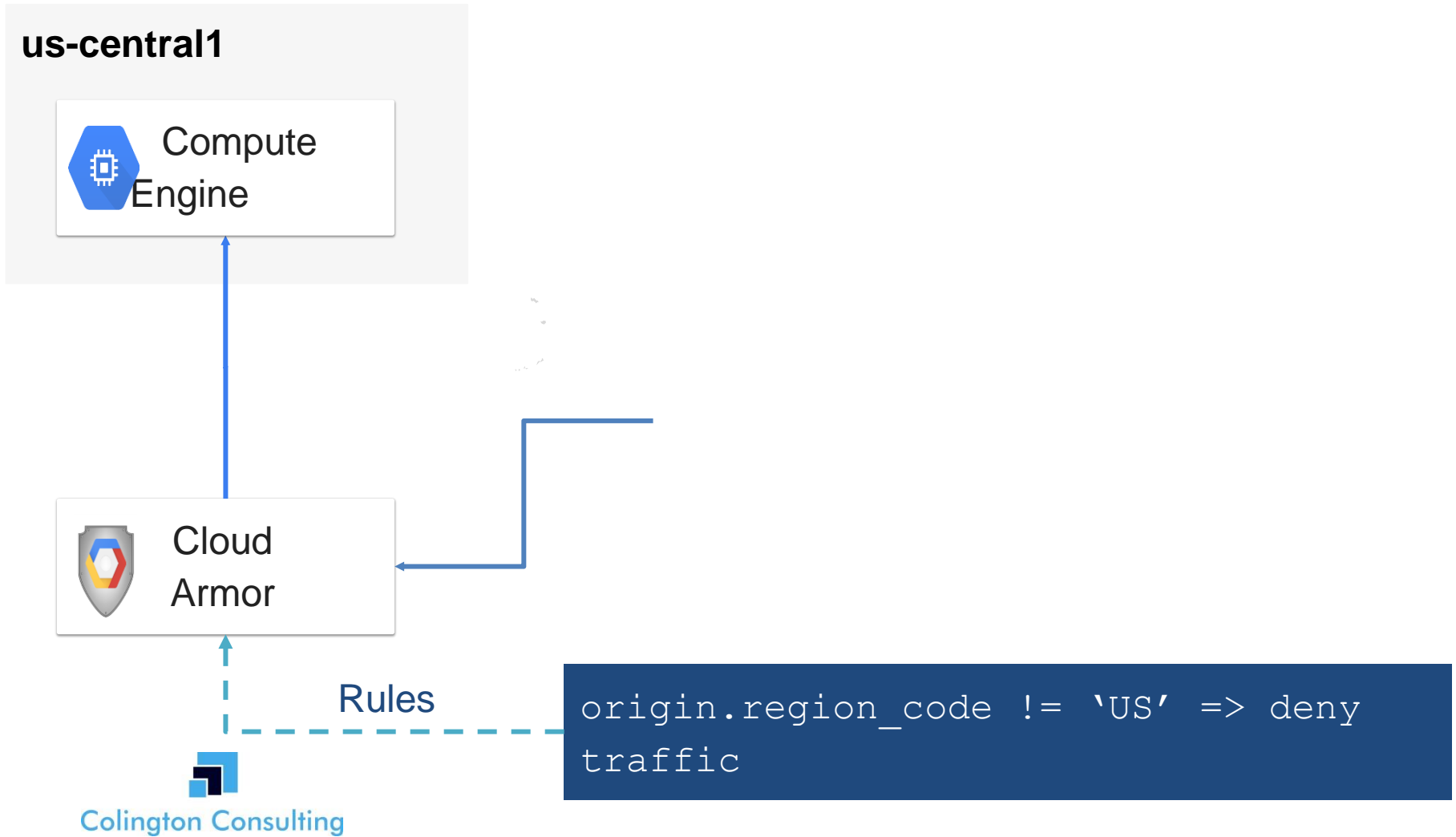
1. Cloud Armor
protects the edge
2. Identity-Aware
Proxy restricts
users
3. VPC Firewall
protects the
virtual network



Restrict services to corp users



Restrict services to specific countries



Enforce SSL/TLS Standards

You can enforce usage of minimum SSL/TLS Versions for clients with **SSL Policies**

The screenshot shows the 'Create policy' interface in the Google Cloud console. On the left is a navigation sidebar with 'Network Security' selected, containing sub-items 'Cloud Armor' and 'SSL policies'. The main content area is titled 'Create policy' and includes the following fields:

- Name**: A text input field containing 'my-tls-policy'.
- Add a description**: A link to add a description.
- Minimum TLS version**: A dropdown menu set to 'TLS 1.2'.
- Profile**: A dropdown menu set to 'Restricted'. Below it is a descriptive text: 'Sets of features used in negotiating SSL with clients. Managed profiles are maintained to support new SSL capabilities. Custom profiles require manual updates.'
- Apply to targets (Optional)**: A section with explanatory text: 'SSL policies can be attached to frontend resources using HTTPS or SSL protocol. You can apply policies here, or while creating/editing a load balancer.' Below this is a '+ Add target' button.
- Save** and **Cancel** buttons at the bottom.

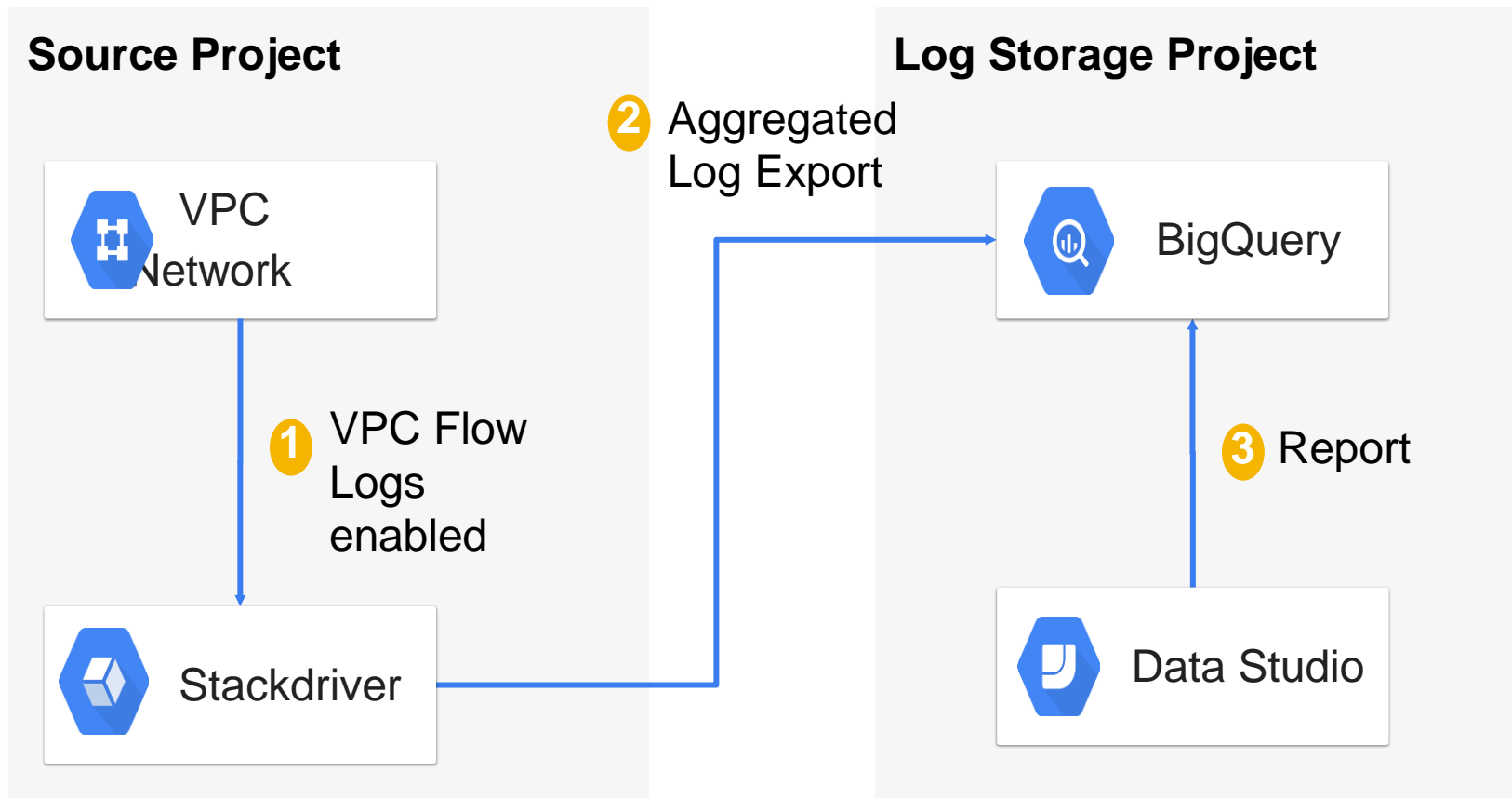
Which countries are connecting to my services?

VPC Flow Logs are a valuable source of intelligence

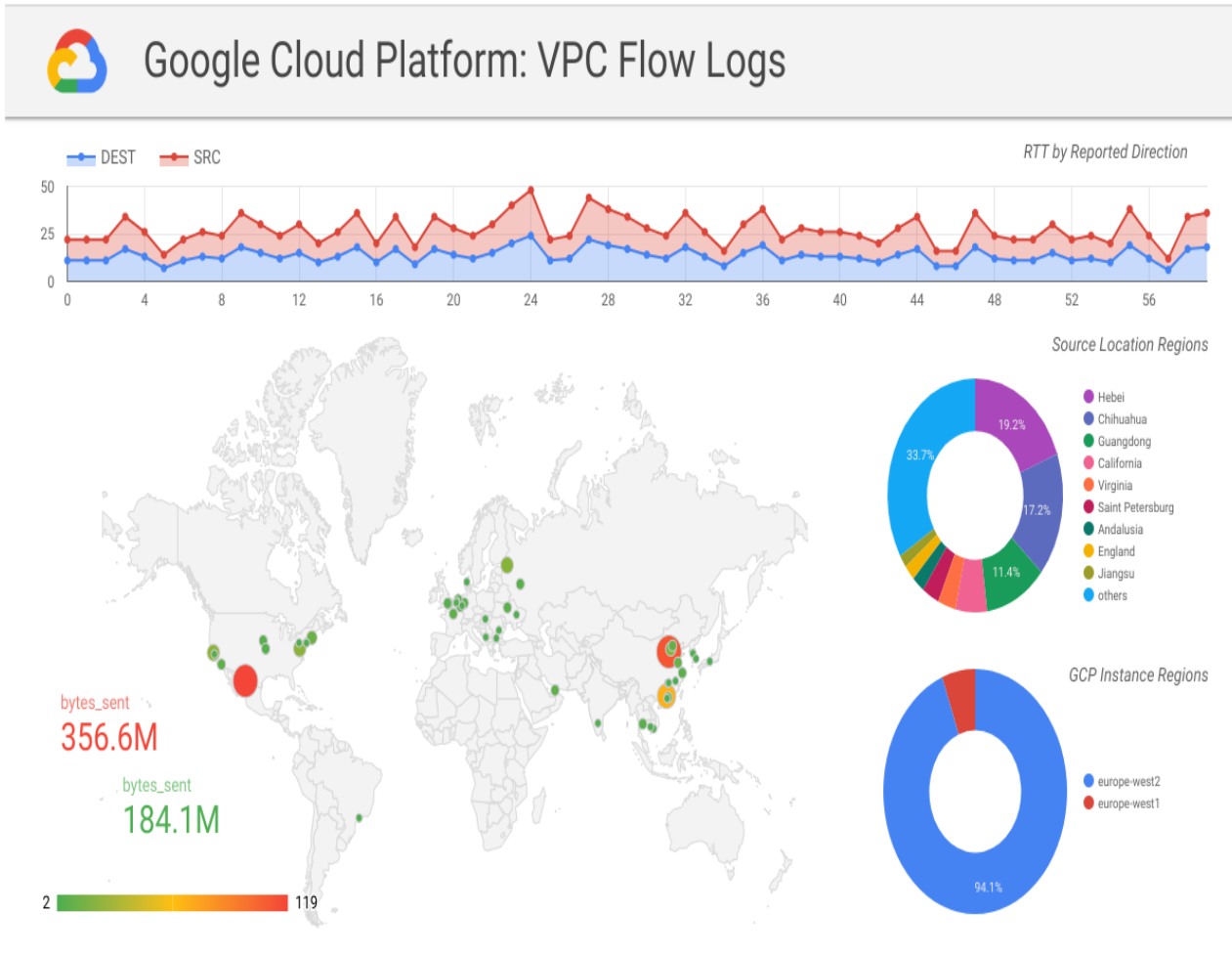
- VPC Flow Logs records network flows inter-VPC, intra-VPC, Google services and Internet traffic
- Appear in Stackdriver Logging
- Enable/disable per VPC network subnet



Visualise VPC Flow Logs



Example VPC Flow Logs dashboard



Bonus: Which services talk to each other?

Illuminate how applications are connected and communicating

- With VPC flow logs we can examine inter-service communication
- Lock down VPC Firewalls to only required flows
- Could be automated



How do I keep my secrets, secret?

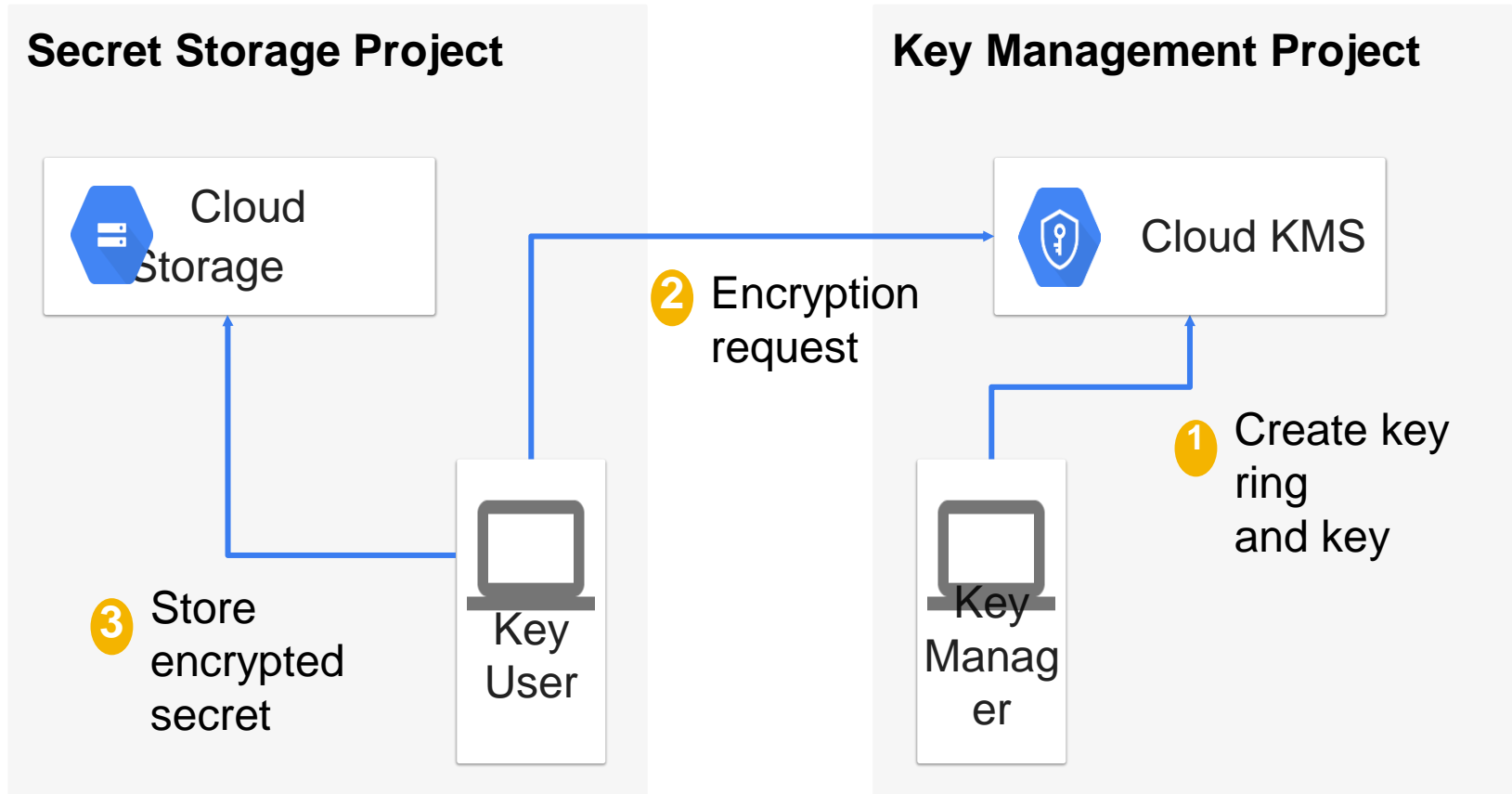


Cloud KMS can encrypt secrets to be stored elsewhere - such as Google Cloud Storage.

Uses IAM for access control and Audit Logging for monitoring.



Separation of duties



Are my machines up to date?

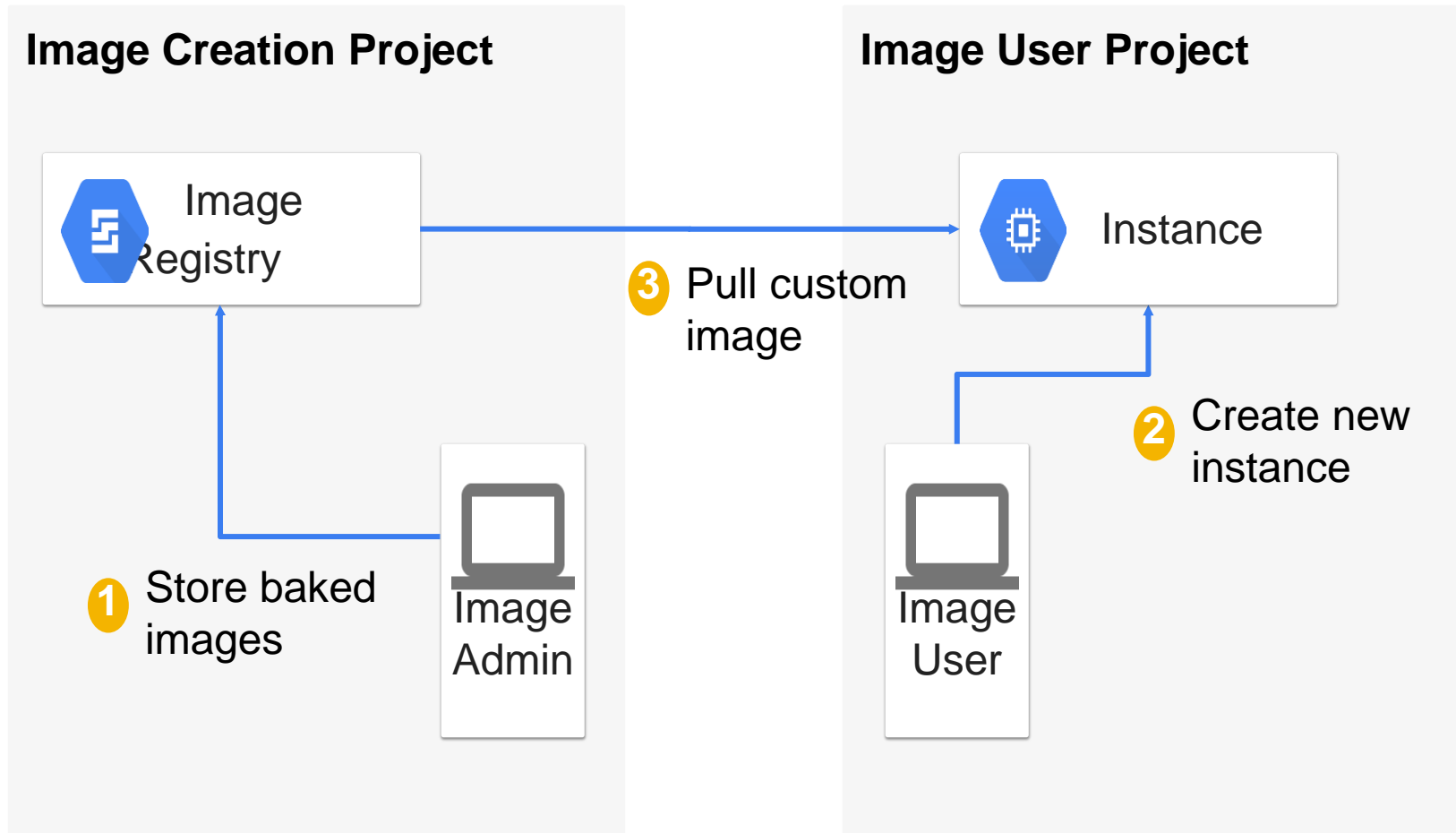
Define a Golden Image
with security and
configuration applied

Common questions:

- If a vulnerability is discovered how can I ensure my estate is patched and consistent?
- How do I stop users building VMs without hardening applied?



Sharing Custom Images



Trusted Images

Ensure VMs only
use approved base
image

Deny access to non-Custom Images using a
Resource Manager Constraint

```
constraint:  
constraints/compute.trustedImageProjects  
listPolicy:  
  allValues: DENY
```



Image Lifecycle



Active

Deprecated

Obsolete

Deleted

Available to use
by anyone with
permissions

Users can still
launch

Warning they
are not using
latest version

Cannot be
launched, will
throw **failure**

Marked deleted
to be removed.



Automated obsolescence

Keep images
current with
automated baking
and deprecation

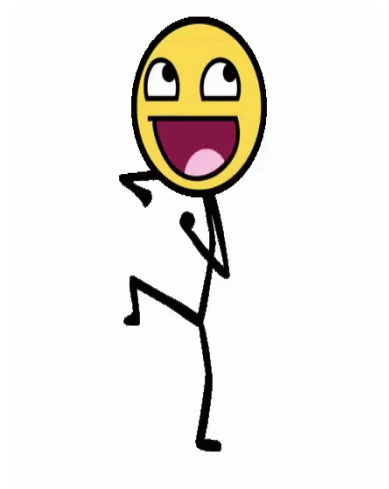
DEPRECATE now, then OBSOLETE in 7 days, then
DELETE in 14 days

```
gcloud compute images deprecate IMAGE --state  
DEPRECATED --obsolete-in 7d --delete-in 14d
```



Summary

Data loss prevention:
Scan, redact, and de-ID



End-user:
Prevent,
detect,
remediate

Infra:
IAM, Logging,
Cloud controls



2019 COV Security Conference

2019 Security Conference Registration and Call for Papers

Registration for the 2019 Commonwealth of Virginia (COV) Information Security Conference is now open. The 2019 conference will be held April 11-12 at the Altria Theater in Richmond. The call for papers has been issued and the conference committee is now accepting submissions through Feb. 15.

Conference and registration information can be found on the link below.

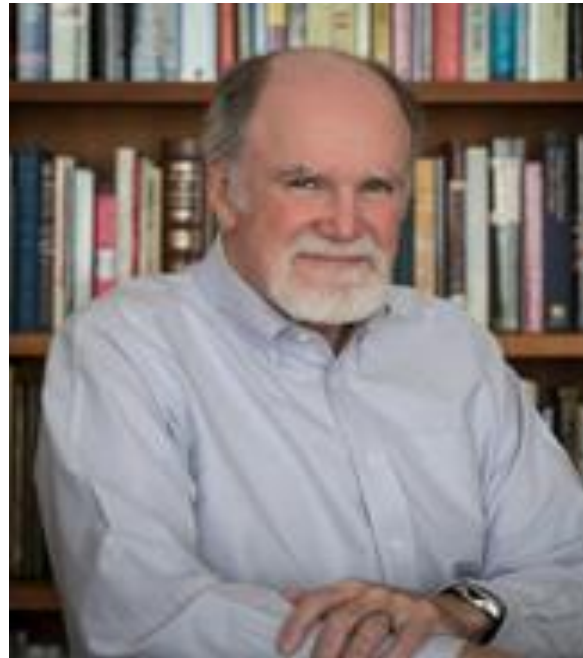
<https://www.vita.virginia.gov/commonwealth-security/cov-is-council/cov-information-security-conference/>

Send your call for papers questions to: isconferencecfp@vita.virginia.gov

For all other conference questions: covsecurityconference@vita.virginia.gov

Keynote Speaker – Day One

- Steve Uzzell – Internationally renowned photographer and inspirational speaker





ISO/AITR Approver List

- CSRM is trying to make sure the ISO/AITR approver list for the agencies are accurate.
- If you have questions or want to verify the approvers listed for your agency contact:

Tina.Harris-Cunningham@vita.virginia.gov



IS Orientation

The next IS Orientation will be held on March 28 from 1-3 p.m. in multipurpose room 1221 (CESC).



Future ISOAG

March 6 , 2019 @ CESC 1-4 p.m.

Speakers: Rick Tiene and Dave Jordan, Mission Secure, Inc.

Barry Davis, DSS

John Craft, VITA

Bob Auton, VITA

ISOAG meets the 1st Wednesday of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING

