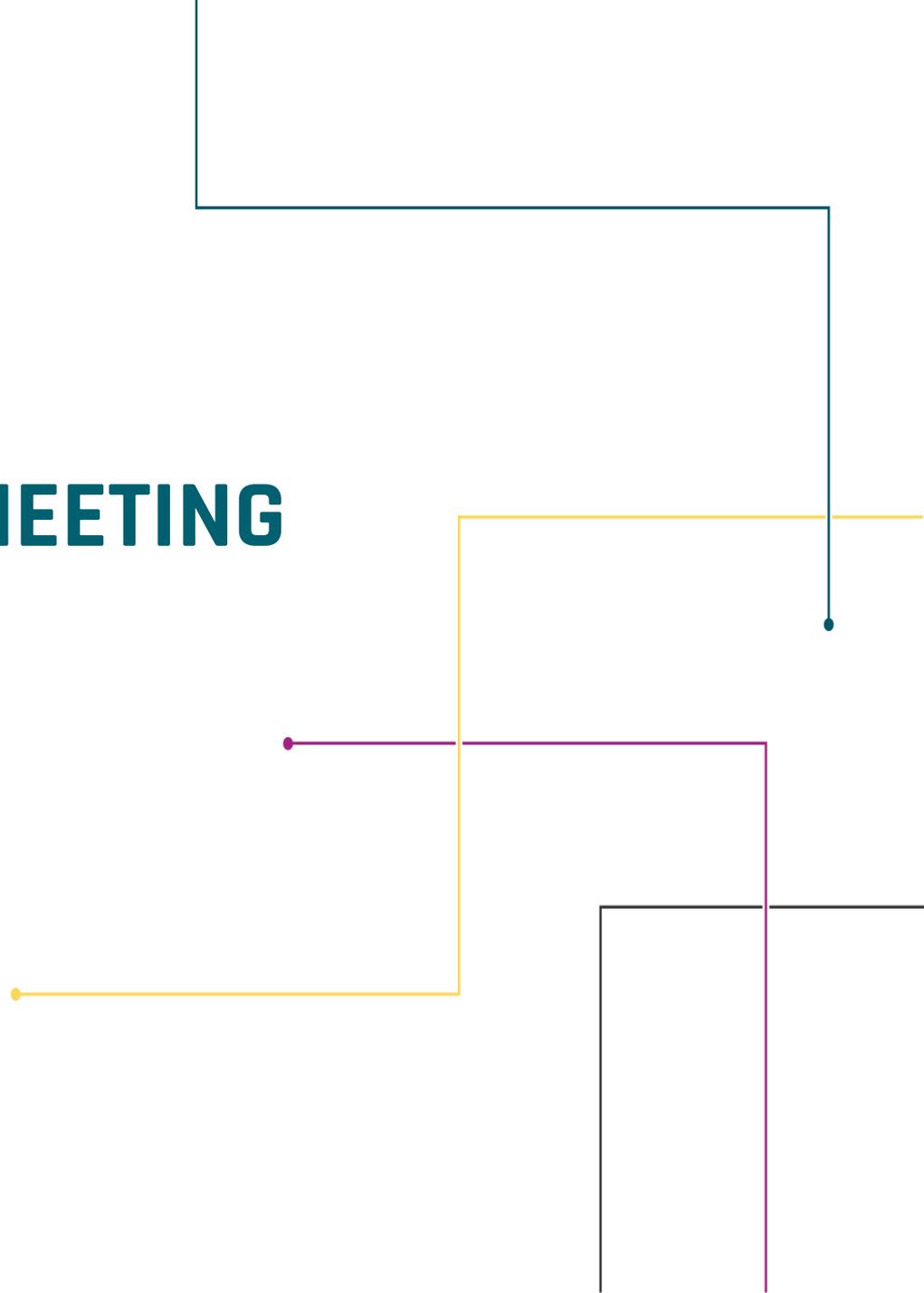


MARCH ISOAG MEETING



AGENDA

- **MANJU GANERIWALA, VA TREASURY**
 - **CHRISTOPHER COPE, FBI**
 - **JENNIFER WHITTY, GOOGLE**
 - **UPCOMING EVENTS**
- 
- A series of decorative lines on the right side of the slide. A dark teal line starts at the top right, goes down, then left, then down again. A yellow line starts at the top right, goes down, then left, then down again. A purple line starts at the top right, goes down, then left, then down again. A black line starts at the top right, goes down, then left, then down again.



VIRGINIA**TREASURY**

Stewardship • Integrity • Excellence

Executive Branch Cyber Coverage & State of the Cyber Insurance Market

Manju Ganeriwala
State Treasurer

March 3, 2021

Cyber Coverage - Agenda

- Current Placements
- Elements of Coverage
- Notable Breaches
- State of the Market
- Ransomware
- OFAC Advisory
- Mitigation Recommendations

History of Commonwealth's Cyber Coverage

- 2011 - University of Virginia
- 2013 - All other Colleges and Universities except
 - 2014 added Christopher Newport
 - 2015 added Southwest Virginia Higher Ed Center
- 2014 - Community Colleges & ABC Board
- 2015 - Data Breach Pilot Program Established by DRM
- 2017 - Retirement Systems
- 2020 - Executive Branch Agencies

Elements of Cyber Coverage

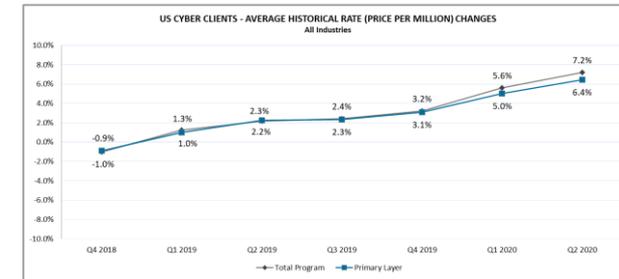
- Privacy Liability
- Security Liability
- Media Liability
- Regulatory Defense Costs/Fines/Penalties
- Incident Investigation
- Network Interruption/Extra Expense
- Data Restoration
- **Cyber Extortion/Ransomware – Claims Leader**
- Cyber Crime

Notable Government Breaches

- SolarWinds – December 2020
- Baltimore Public Schools – November 2020
- Baltimore Ransomware – May 2019
- Atlanta, Georgia – March 2018

State of the Cyber Insurance Market & Forecast 2021

1. Q1 Forecast: 25-35%+ Cyber insurance rate increases
2. Some carriers non-renewing entire cyber insurance portfolios
3. Potential continued cyber carrier exits from market
4. Ransomware and/or BIPA supplemental applications required
5. AIG implemented 50/50 coinsurance, halved ransomware event coverage sublimits, moved to non-admitted paper on top of continued rate increases
6. Chubb adding SolarWinds impact exclusion; \$1M max limit for public entity business
7. Controls that are strongly recommended for all industries:
 - Encryption, Backups, Multi-factor Authentication, EndPoint Detection and Response, Firewalls, etc.
 - Need to be in place if at all possible. Risk that do not have these controls in place are seeing drastic increases in pricing/deductibles, reduction in coverage or non-renewal.

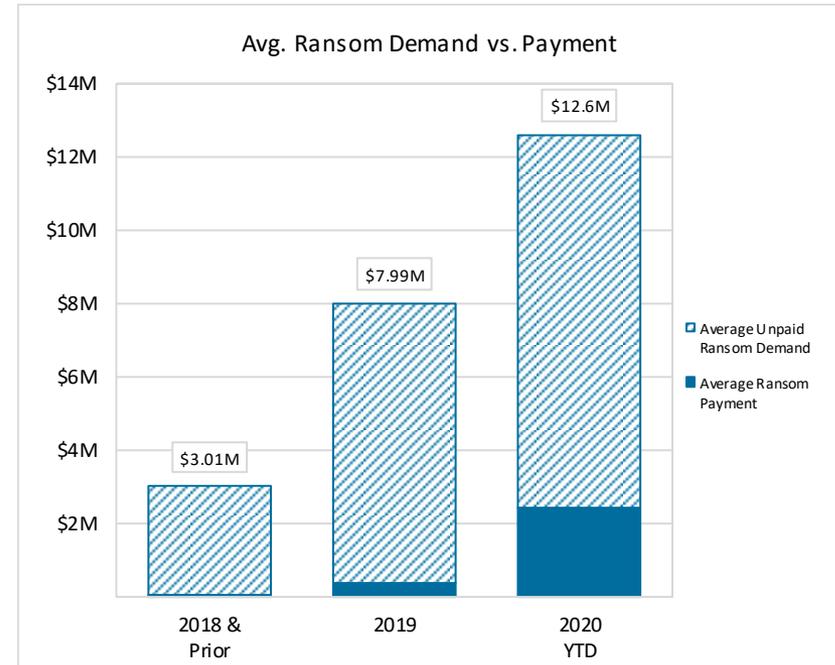
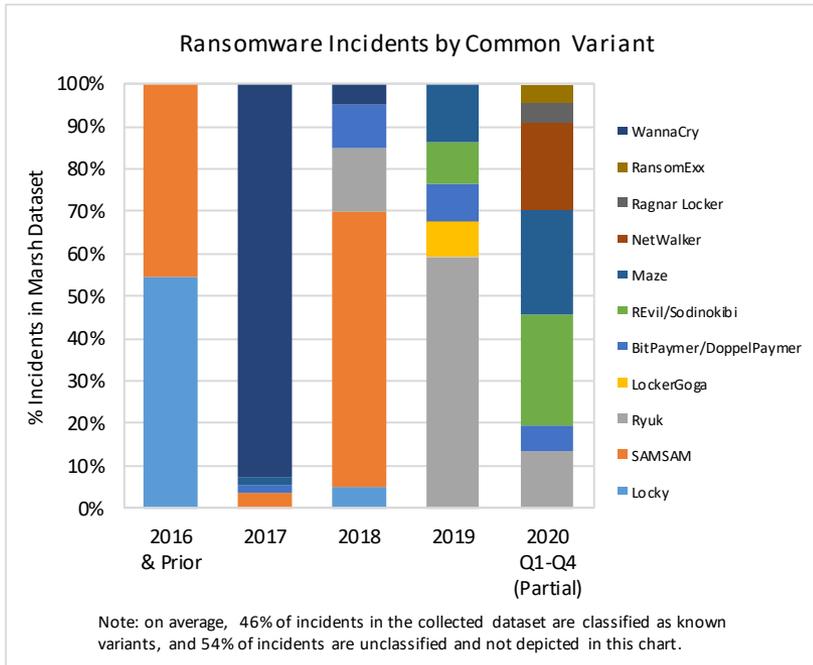


State of the Cyber Insurance Market – How Did We Get Here?

- Low Premiums
 - Result of competition among legacy cyber insurers & new market entrants
- Broad Coverage
 - Policies have become more responsive to historical exposures and newly emerging risks
 - Year-over-year broadening of coverage
- Mature Cyber Claims Data
 - Better and more developed insight into which risk factors drive cyber losses
 - Unavailable when coverage was first emerging
- Removal of “Silent Cyber”
 - Cyber exclusions on non-cyber policies, such as Property, Commercial General Liability
 - More non-buyers purchasing standalone Cyber Liability policies
- Ransomware – Leading Cause of Loss
 - Operates as an industry and every organization regardless of size is a target
 - Average amounts paid have increased to the six figures with carriers payment demands of \$10M

Ransomware Sophistication and Severity are Rising

Newer & emerging variants and increased loss costs are driving more scrutiny on cyber risk management.

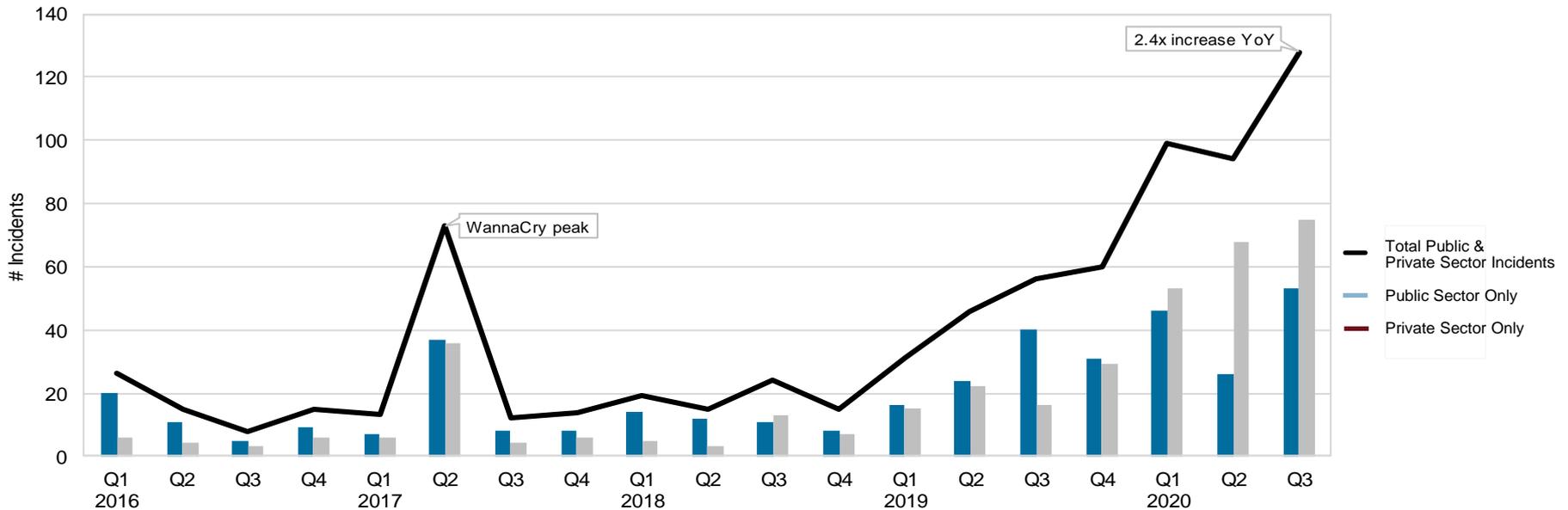


- Ransomware variants are increasing in type and sophistication, and are more accessible by bad actors than ever before with the proliferation of Ransomware-as-a Service.
- Ransom demands are increasing year-over-year, however, Q4 2020 trends from Coveware indicate average ransom payments have decreased 34% compared to the prior quarter. We note the ransom payment is only one component of event costs should companies elect to pay. 70%+ of Q4 ransom events threatened data exfiltration
- Marsh continually researches public sources & private partner databases, & leverages internal proprietary info to understand the evolving landscape & impacts of ransomware.

Ransomware Incident Frequency Has Increased Significantly

Year-over-year increase in incidents impact both public and private sectors.

Ransomware Incident Volume

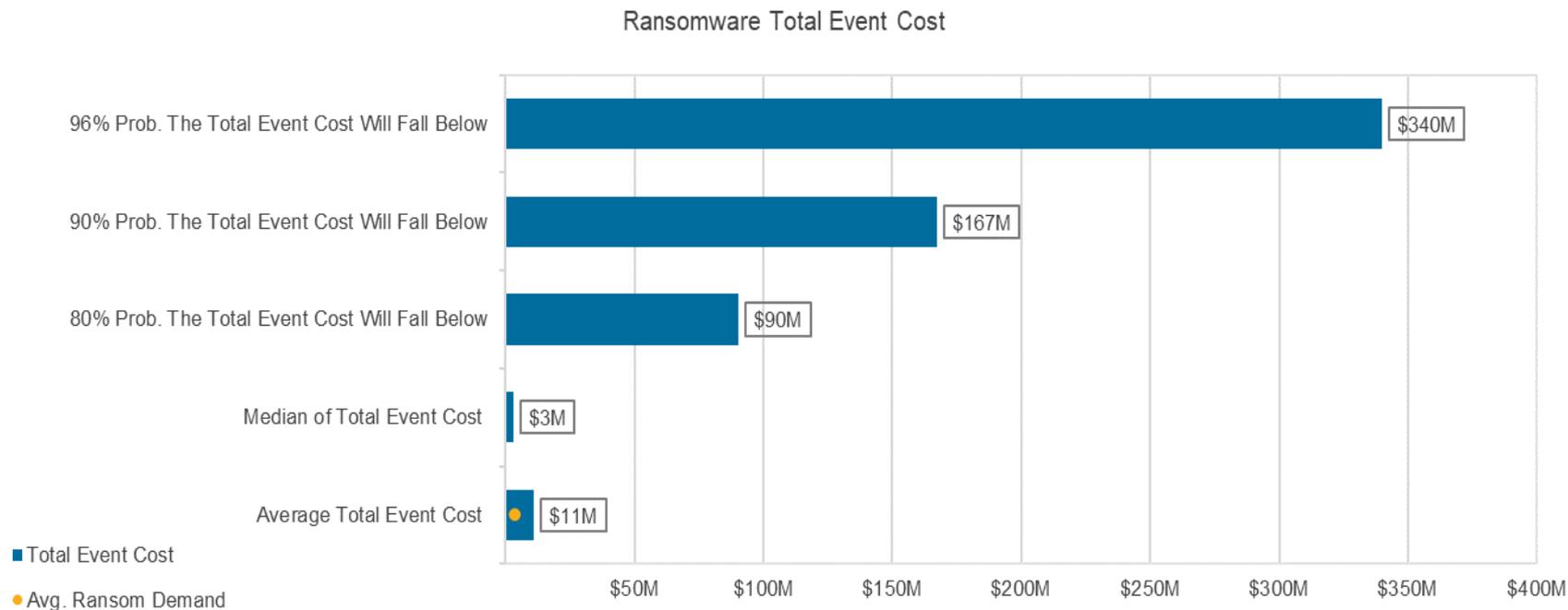


- Ransomware attacks have increased exponentially during the pandemic.
- Across all industries, bad actors pursue targets with the lowest barriers to entry, enhancing the need to focus on comprehensive cyber risk management.
- The public sector accounted for the majority of ransomware incidents from 2016 through 2018 Q2, however, public and private sector organizations have more recently experienced significant increase in incident frequency.

Public sector is defined as Healthcare, Government, Not for Profit.

Ransomware Total Event Cost Analysis

Measuring your organization's ransomware exposure



- Measuring your organization's \$x annual revenues against a regression analysis of the Marsh-collected data set of known ransomware event losses, your organization's projected average ransom demand is \$x and average total event cost is \$x.
- The bars at each predictive interval indicate that the total ransomware incident could cost that amount or less.

Office of Foreign Assets Control (OFAC) Advisory

- A REMINDER - does not change any applicable laws, regulations or guidance
- U.S. businesses/persons PROHIBITED from paying funds to any person/entity on the “Specially Designated Nationals & Blocked Persons” list
- U.S. companies may be sanctioned for any violation of OFAC’s rules
- Encourages companies & their advisors to report cyber extortion attacks to law enforcement
- Contact OFAC immediately if ransomware payment may involve prohibited organization or person
- How May Businesses Reduce Risk of OFAC Sanctions Violation?
 - Complete OFAC Review prior to paying demand
 - Notify law enforcement prior to paying demand
 - Minimize Risks of Ransomware (discussed below)
 - Establish an OFAC compliance program

Minimizing Ransomware & Loss Mitigation Recommendations

- Ransomware Supplemental Questionnaire as a Checklist
- Segmentation of Back-Ups/Review Data Restoration Plans
 - May reduce risk of material data loss and business interruption in the event data or systems are infected
 - May be a factor in deciding whether to make an extortion payment
- Address Remote Desktop Protocol (RDP) Vulnerabilities
 - Close any open RDP ports
 - Move any required RDP access behind a VPN
- Reassess Data Retention & Security Practices
 - Eliminate the risk exfiltration of PII
 - Threat of disclosure of sensitive information by bad actors is frequently a major factor when deciding to pay a ransom
- Take Advantage of Pre-Loss Mitigation Tools provided by Cyber Insurer

Minimizing Ransomware & Loss Mitigation Recommendations

- Establish Relationships with Post-Breach Response Vendors in Advance/Not When “Time is of the Essence”
- Updated Plans: Incident Response & Business Continuity
- Patching: Operating Systems, Software & Firmware Upon Manufacturer’s Release
- Employee Training
- Network Vulnerability Assessments
- Leverage a Cyber Security Framework: i.e., National Institute of Standards & Technology, ISO 27001
- Consistent Meetings at the Board of Directors/C-Suite Level
- Consideration of Endpoint Security Solutions

What's Next!

- Executive Branch Cyber Program Report
 - Required by 2020 Appropriations Act (Chapter 1289) to be submitted to the Secretary of Finance by October 1, 2021
 - Report must include:
 - Initial performance the program
 - Loss experiences
 - Program structure recommendations
 - Funding mechanisms moving forward (Currently funded by Property Plan balances)
 - We want to hear from you!
 - Customer/Agency feedback on the program

Questions



There are no slides available from our
2nd speaker Chris Cope with the FBI



Hello, Virginia!

Google Cloud



WILLIS ZHANG

Customer Engineer, Google Cloud

CONTACT

 williszhang@google.com

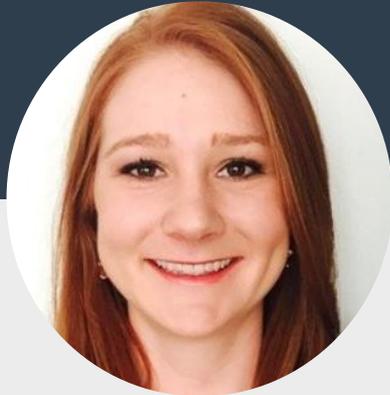
 [linkedin.com/in/zhangwillis](https://www.linkedin.com/in/zhangwillis)

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.

Google Cloud



JENNIFER WHITTY

Cloud Program Manager, Google Cloud

CONTACT

 jenniferwhitty@google.com

 [linkedin.com/in/jennifer-whitty](https://www.linkedin.com/in/jennifer-whitty)

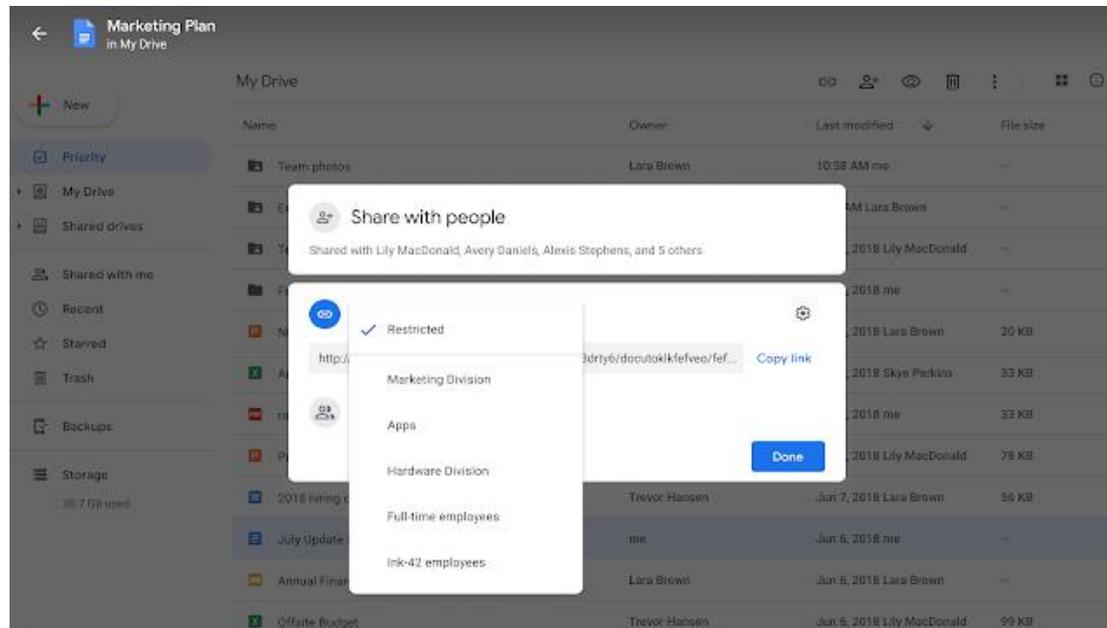
ABOUT ME

Jennifer advises state and local governments on ways to enable innovation through security and technology. She enables government officials to focus on critical goals at the scale required of our world today.

Prior to Google, Jennifer was a Senior Manager at Verizon, leading the cloud infrastructure and operations division. She contributed to many successful IT transformations focusing on retraining staff, modernizing operations and redesigning security requirements to capture deltas between on premise and cloud.

Google Cloud

Least Privilege With Google Workspace



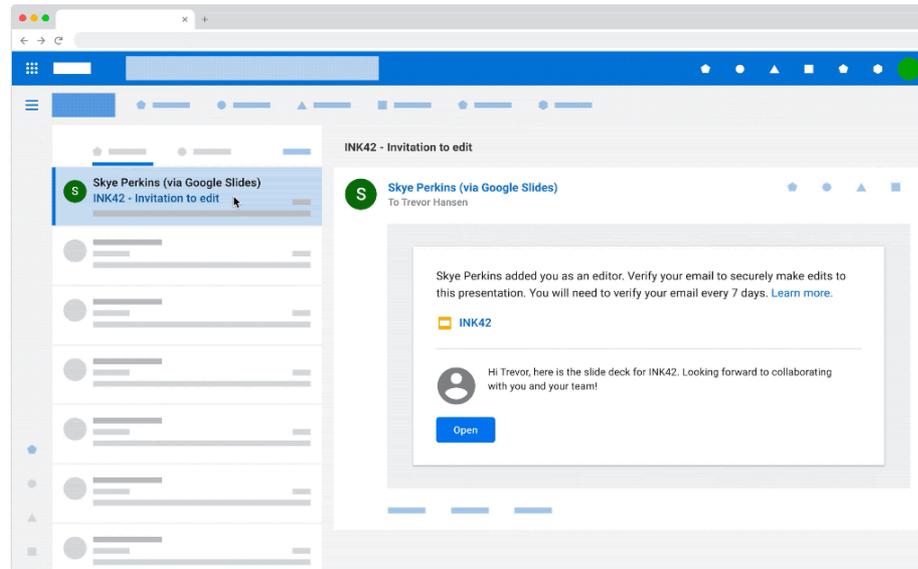
Limit Google Drive sharing to specific groups with target audiences

Admins can now define specific audiences with whom their users can link-share Google Drive files. This can help keep your organizational data secure, and make it simpler for users to share files with the right colleagues.

- Improve your organization's security posture by making it harder for information to be shared more broadly than is appropriate.
- Guide users to share with more specific and appropriate audiences.
- Save users time by reducing the need to manage sharing requests from multiple individuals.
- Make it easier for your users to collaborate with their colleagues simply, efficiently, and securely.

[Manage target audiences](#) (administrators)

Collaborate with people who are not using a Google account in Drive, Docs, Sheets, Slides, and Sites



PIN Code Sharing

G Suite customers often work with partners outside of their company. These external users, or “visitors,” don’t always have Google accounts, making it more difficult for G Suite and non-Google users to collaborate seamlessly and securely.

This new feature will help ensure smooth and secure collaboration with visitors through:

- Rich collaboration—including comments, edits, and more—with anyone you need to work with, regardless of whether they have a Google account.
- Audit logging for collaboration with visitors, so that all interactions are monitored and recorded.
- Ability to revoke access and remove collaborators as needed.
- Reduced need to download, email, or create separate files to work with external users who don’t have Google accounts.



Augment Email Deployments with GCP Security

Event threat detection | Log analytics | Identity- & Context-aware proxy

Google Cloud

Demo!





Investigation Tool

Security Rules



VPC Flow Logs

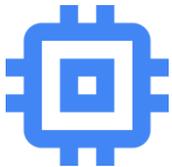
Security Command Center with
Event Threat Detection

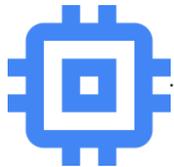
BigQuery



Bad actor (insider) SSHs into VM and infects it

1





Cloud Logging

2

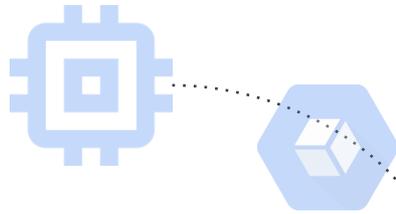
VPC packets, DNS, and syslogs immediately trigger finding



Security Command Center with
Event Threat Detection

ELAPSED TIME: < 1 second

eventTime	August 10, 2019 at 8:46:46 PM UTC-4
firstDiscovered	August 10, 2019 at 8:46:46 PM UTC-4



Security Command Center with
Event Threat Detection



3

Security team is alerted and
starts investigating logs in SCC
and BigQuery



Cloud Logging



BigQuery

Investigate by querying against multiple datasets

```
SELECT
  timestamp,
  source_packets,
  destination_packets,
  ip_address,
FROM `vpc_logs`
JOIN `threats` ON
  vpc_logs.timestamp >= timestamp_sub(threats.timestamp, 5 minute) AND
  vpc_logs.timestamp <= timestamp_add(threats.timestamp, 5 minute)
WHERE
  threats.eventTime = '2019-08-11T00:59:50.676Z'
ORDER BY
  timestamp ASC
```

JOIN two datasets: identifying packet behavior within 5 minutes of the threat event

copy-paste from SCC

PB-potential query power done in seconds.

The screenshot shows the Google Cloud Platform BigQuery interface. The top navigation bar includes the Google Cloud logo, a search bar, and a user profile. The main content area displays a query titled "Investigating traffic packets within 5 minutes of a threat incident". The query is written in SQL and involves joining data from "vpc_logs" and "threat_alerts" tables. The query execution status is "Query complete (1.8 sec elapsed, 5.7 KB processed)". The "Query results" section shows a table with job information, including Job ID, User, Location, Creation time, Start time, End time, Duration, Bytes processed, Bytes billed, Job priority, and Destination table.

```
13 vpc_logs.jsonPayload.dest_location.city as dest_city
14 FROM `govt-demo-real-time-security.subnet_logs.compute_googleapis.com.vpc_flow_20190811` as vpc_logs
15
16 JOIN
17 `govt-demo-real-time-security.threat_alerts.threatdetection_googleapis.com.detection_20190811` as threats
18 ON
19 vpc_logs.timestamp >= timestamp_sub(threats.timestamp, interval 5 minute) AND
20 vpc_logs.timestamp <= timestamp_add(threats.timestamp, interval 5 minute)
21
22 WHERE
23 threats.jsonPayload.eventtime = '2019-08-11T00:50:50.676Z'
24
25 ORDER BY
26 timestamp ASC
```

Job ID	govt-demo-real-time-security.US.bqjob_5aa65eb5_16c7e584928
User	willizhang@google.com
Location	United States (US)
Creation time	Aug 10, 2019, 9:44:31 PM
Start time	Aug 10, 2019, 9:44:31 PM
End time	Aug 10, 2019, 9:44:33 PM
Duration	1.8 sec
Bytes processed	5.65 KB
Bytes billed	20 MB
Job priority	INTERACTIVE
Destination table	Temporary table
Headname OK	false

No cluster setup. No perf tuning. Just one click.

A Leader in The Forrester Wave™: Insight Platforms-As-A-Service, (Q3 2017)



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.



Data Management

New York City (in partnership with Cloudreach)

Challenge: New York City is home to over 8.6 million citizens and receives more than 60 million visitors each year. New York City Cyber Command (NYC3) has the monumental task of defending NYC networks and infrastructure from malicious cyber attacks and online threats every second of every day.

Mission possible: security at scale in New York City

NYC3 partnered with Google Cloud to build a secure cloud-based security log for city systems, managing 330,000 city workers across 400,000 endpoints using 200,000 city-owned IP addresses. NYC3 cybersecurity professionals can access visualization and analytics for historical and real-time data – to then become predictive and make decisions at machine speed.

Near-infinite scalability for analyzing petabytes of data

Processes **billions** of events daily, processing events in **10 milliseconds**

Accelerates time to onboard **100+ city agencies**

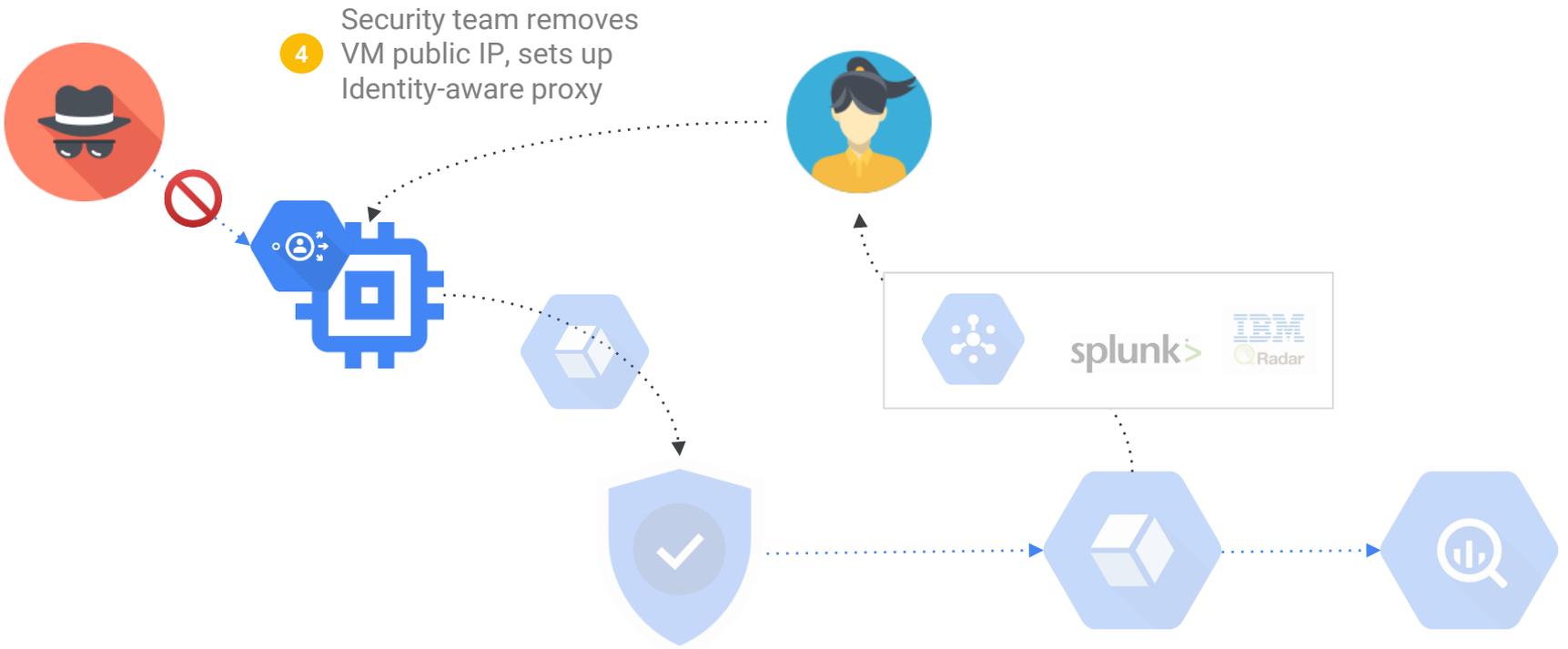


Our streets are already the safest in any big city in the country - now we're bringing that same commitment to protecting New Yorkers into cyberspace.

Mayor Bill de Blasio
City of New York

Today, NYC3 ingests more than **200,000** security log events per second, and is speeding data into GCP for analysis - with a mere **5 millisecond** delay between the time the event is created and when it's available for analysis on GCP.





Existing approaches were built for on-prem environments

They are time-consuming, complex, and not optimized for today's cloud-first world.



Limited device access



Cumbersome VPNs

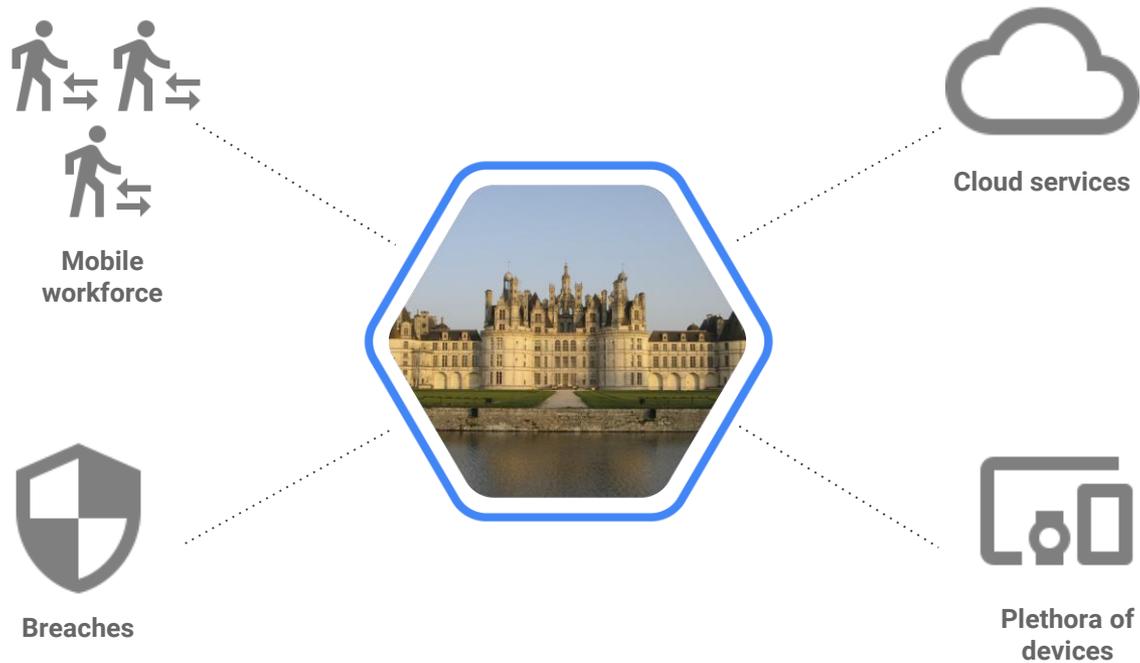


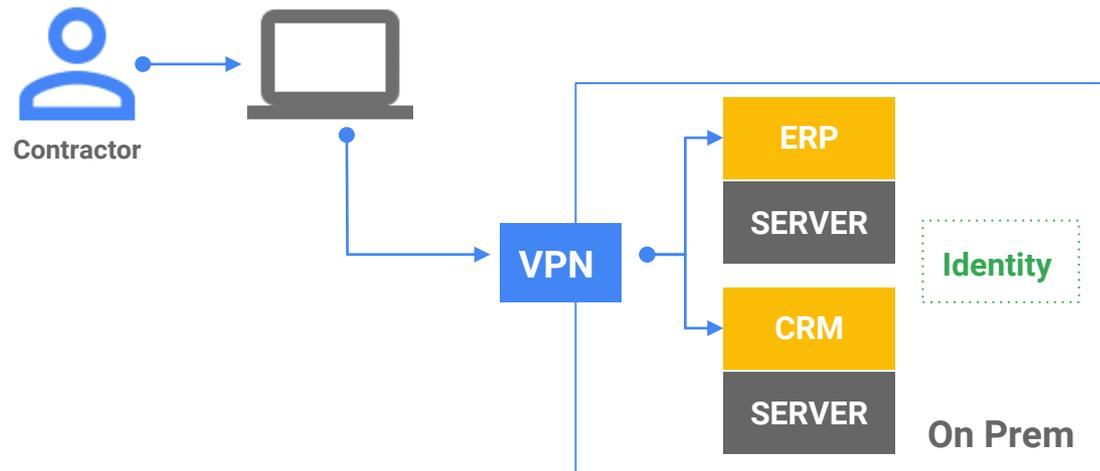
Inconvenient authentication

Our approach to security in two words

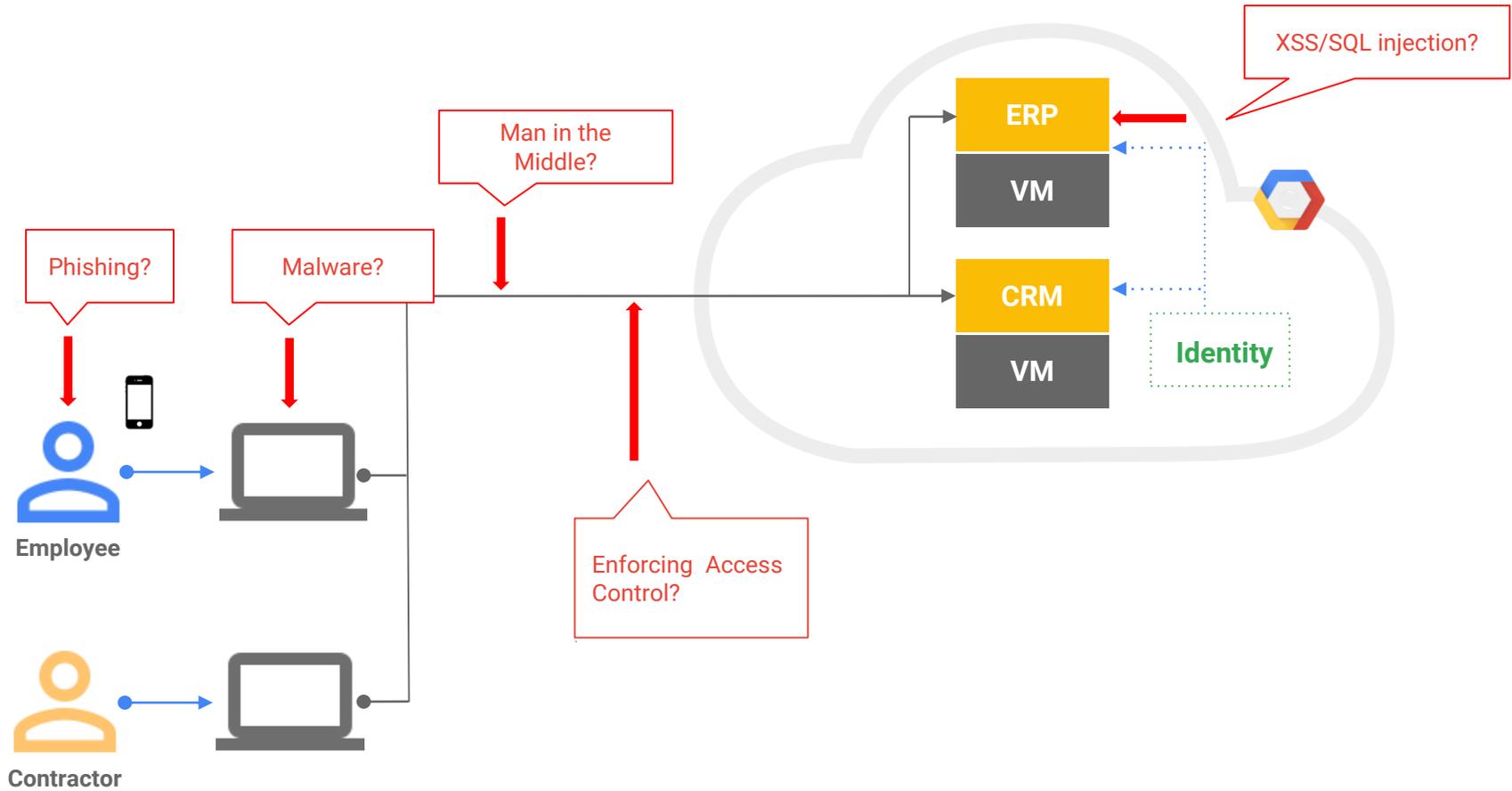
Trust Nothing

Four issues that are wrecking the castle approach





Proprietary & Confidential

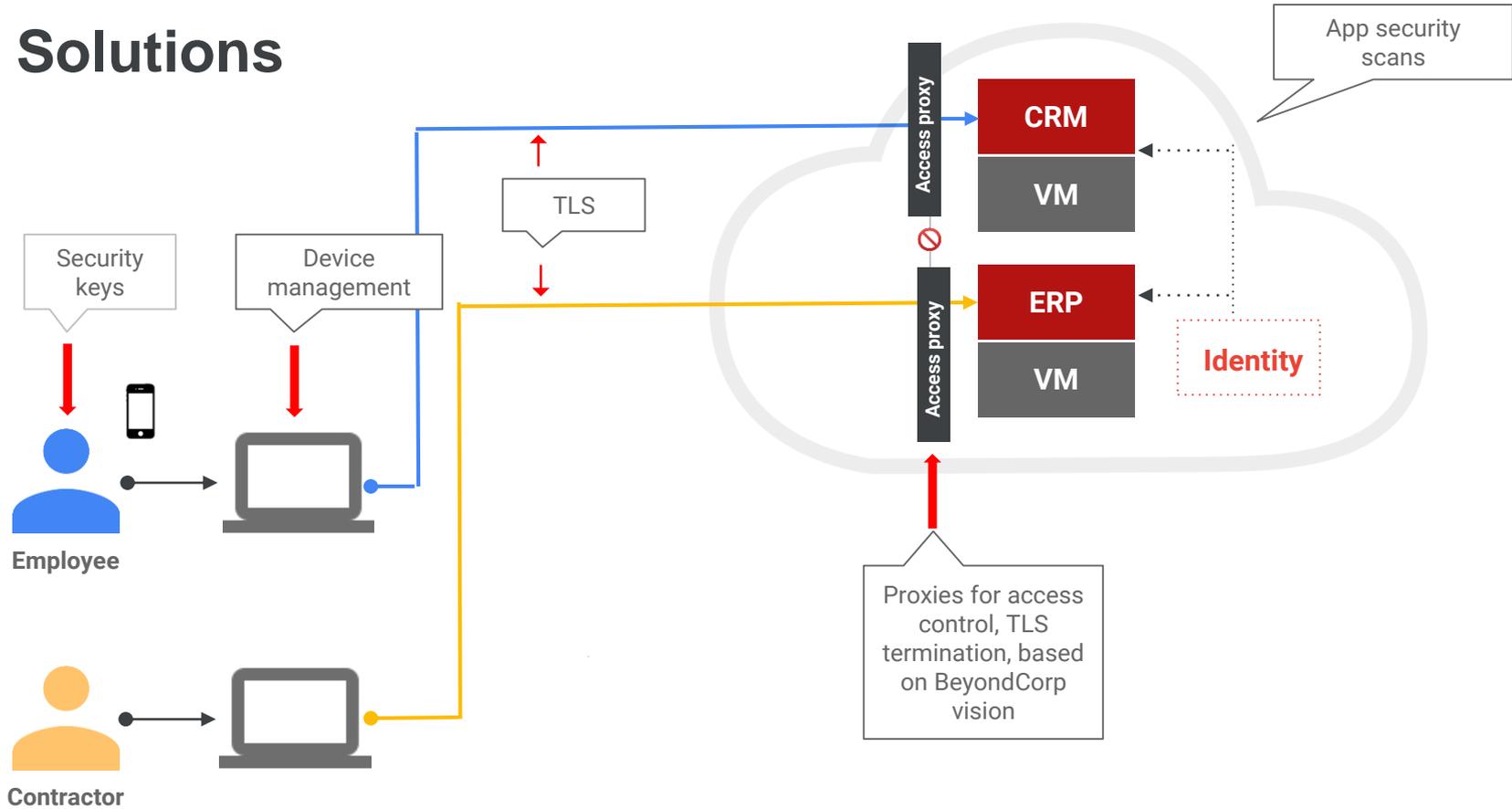


Proprietary & Confidential

Google's seven year BeyondCorp mission (2011-2018)

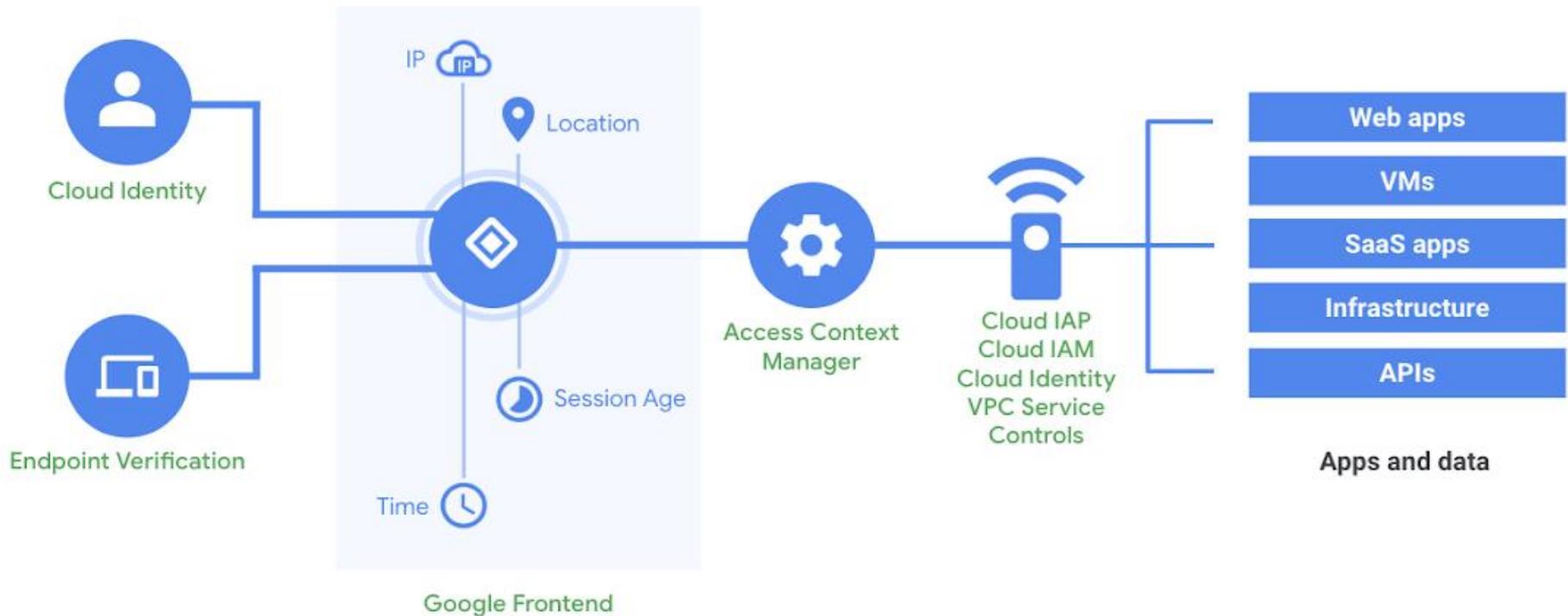
**To have every employee work
from untrusted networks
without a VPN**

Solutions



» So what's the ideal?

Enabling BeyondCorp with **context-aware access**



Thank you



UPCOMING EVENTS

IS ORIENTATION

The next IS Orientation will be held on

March 31, 2021

Presenter: Marlon Cole (CSRM)

Registration link:

<https://vita2.virginia.gov/Events/chooseSession?MeetingID=10>

VIRTUAL INFORMATION SECURITY CONFERENCE JUNE 24, 2021

MORE DETAILS WILL BE FORTHCOMING

APRIL 2021 ISOAG

April 7 from 1- 4 p.m.
Webex

- Doug Powers & Loucif Kharouni, Deloitte
- Juergen Bayer, HP
- David Finley, Dell Technologies
- Nick Christensen, VITA



**THANK YOU FOR
ATTENDING**

