GEORGIA TECHNOLOGY AUTHORITY

Georgia Fiscal Management Council

Annual Training Conference

David Allen – CISO
Dmitry Kagansky – CTO

OUR VISION

A transparent, integrated enterprise where technology decisions are made with the citizen in mind

—

OUR MISSION

To provide technology leadership to the state of Georgia for sound IT enterprise management

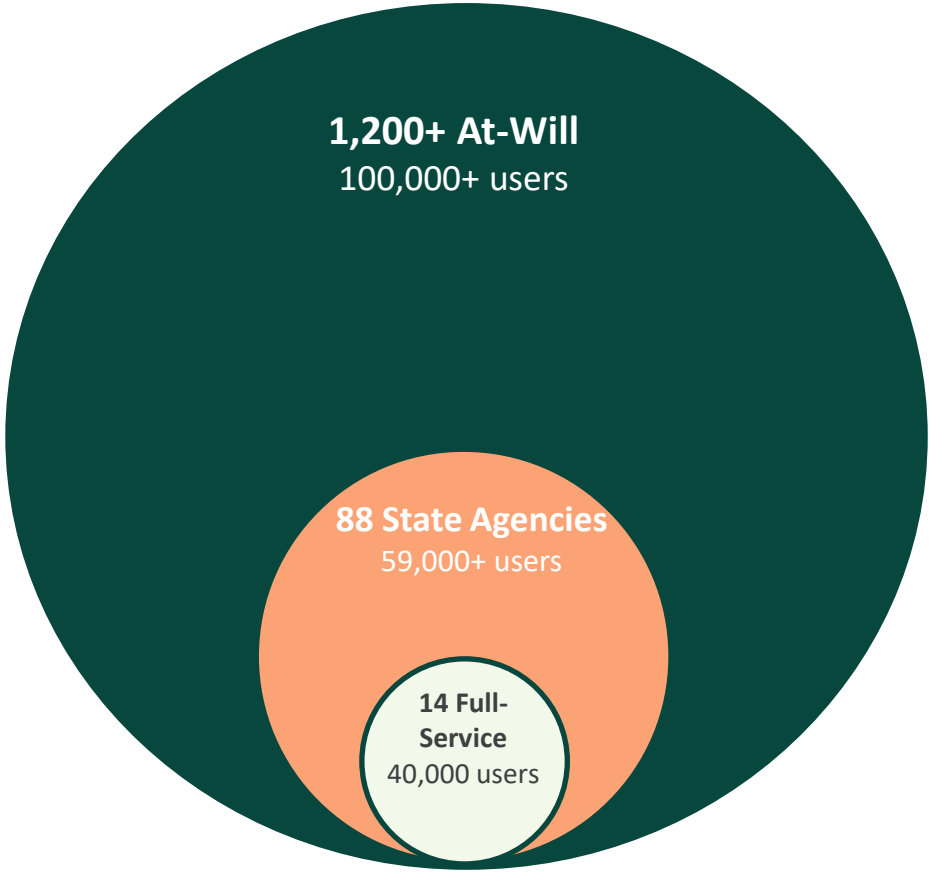
October 3rd, 2022

Agenda

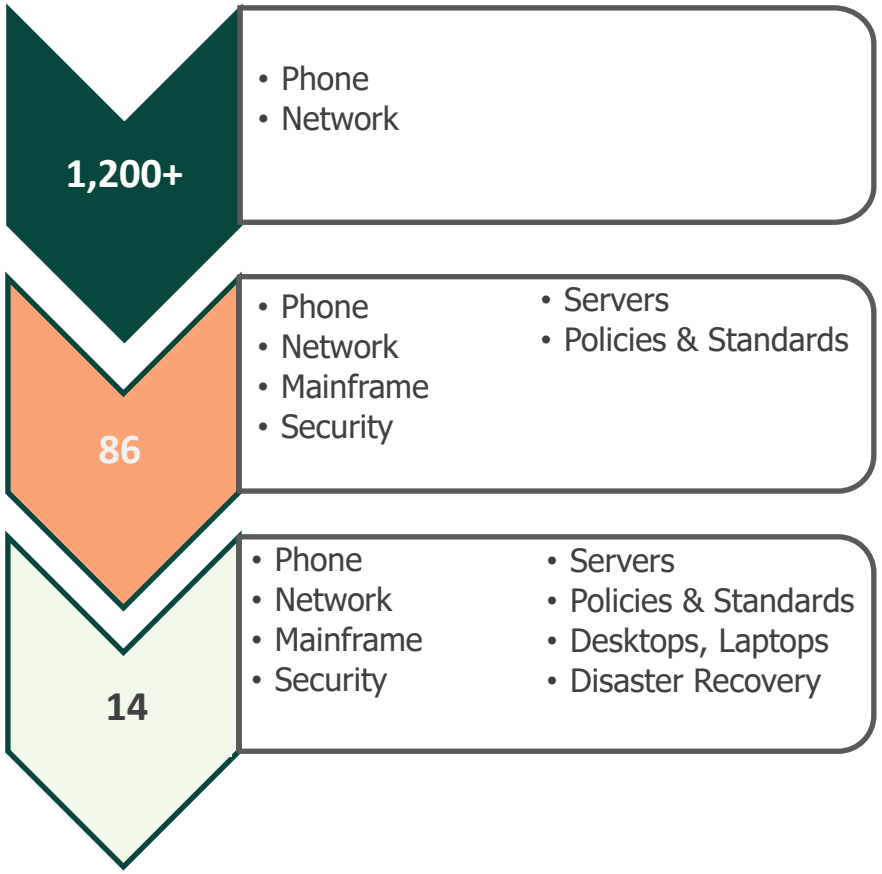
- Introduction
- GTA Overview
- Overview of Cloud Costing
- Security and Risk Mitigation in the Cloud
- “Cost of a Breach”
- Questions / Discussion

Georgia Technology Authority Scope

Which agencies are served?
(segmented by services consumed)



Which services do they get?
(varies from all services to one or two)



Cloud Costs

October 3rd, 2022

What is cloud?

What is cloud?

On-demand IT resources provided over the internet with a Pay As You Go model

What is cloud?

Elastic
Ubiquitous
Metered

Who provides Cloud?

Who provides Cloud?

Amazon Web Services (AWS)

Google Compute Platform (GCP)

Microsoft Azure

Who provides Cloud?

Amazon Web Services (AWS)

Google Compute Platform (GCP)

Microsoft Azure

Yes, there are others but at this point, they all model themselves after the above group

Who provides Cloud?

Amazon Web Services (AWS)

Google Compute Platform (GCP)

Microsoft Azure

Yes, there are others but at this point, they all model themselves after the above group

I'll refer to them collectively as CSPs (Cloud Service Providers)

Is Cloud more secure?

Is Cloud less secure?

Is Cloud more secure?

No

Is Cloud less secure?

No

Is Cloud more secure?

No

Is Cloud less secure?

No

So … Why cloud?

So why cloud?

So why cloud?

More tools

More options

No long-term commitments

So why cloud?

More tools

More options

No long-term commitments

Ability to 'fail fast'

So why cloud?

More tools

More options

No long-term commitments

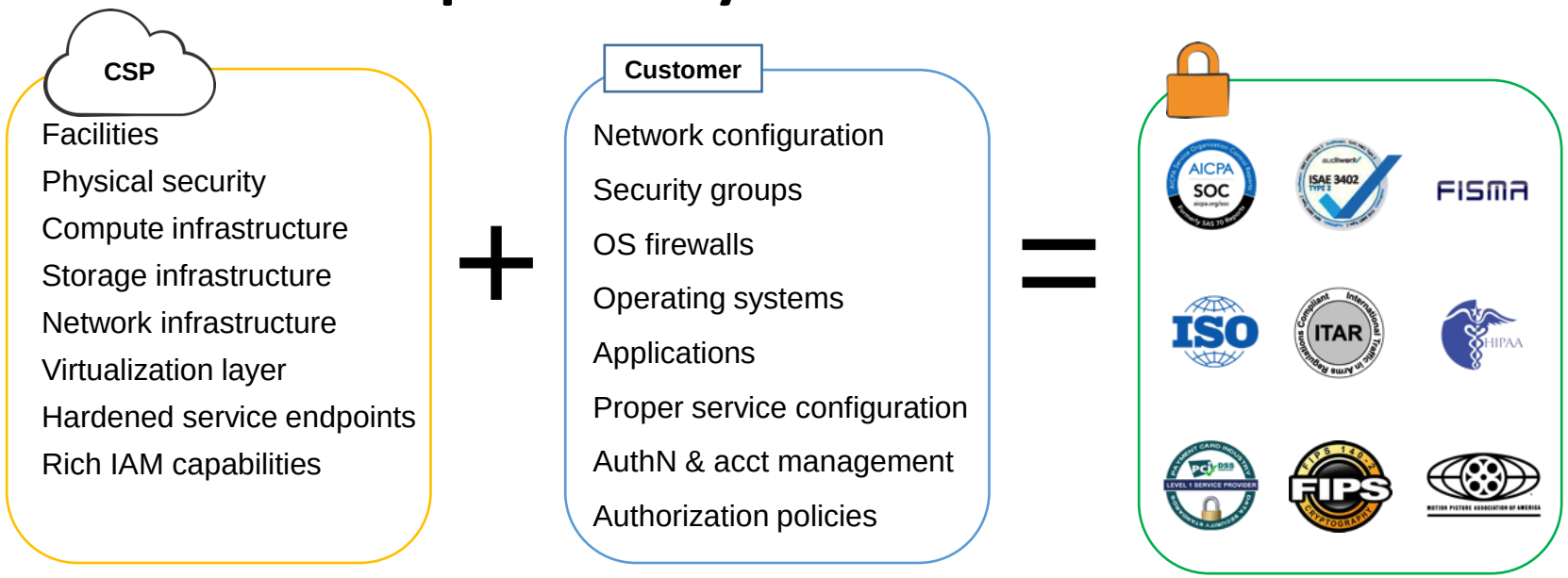
Ability to 'fail fast'

(that's not always a good thing when it comes to ***cost*** or ***security***)

Shared Responsibility Model

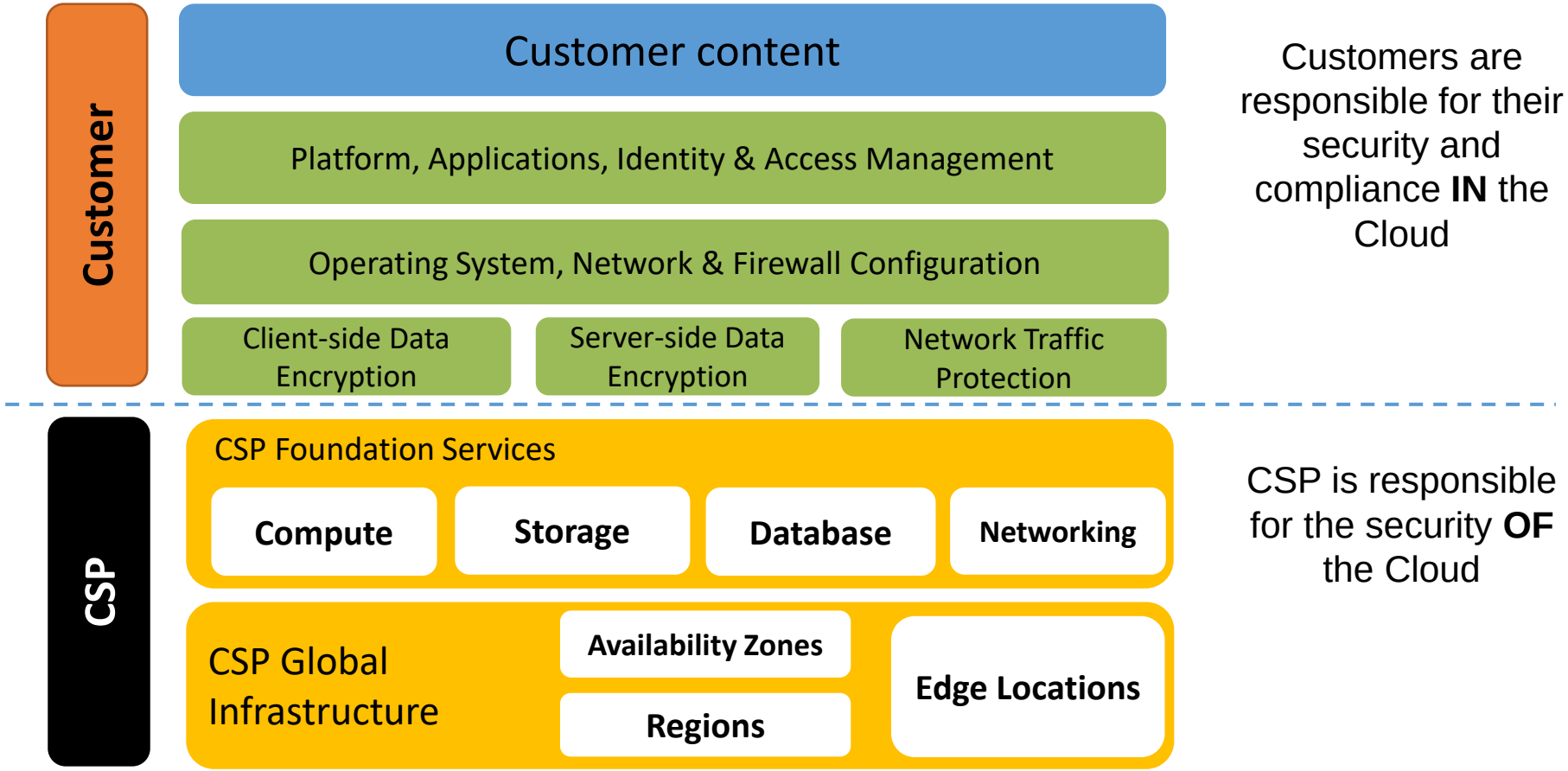
October 3rd, 2022

CSP Shared Responsibility Model



- Scope of responsibility depends on the type of service offered by CSP: **Infrastructure (IaaS), Container (PaaS), Abstracted Services (SaaS)**
- Understanding who is responsible for what is critical to ensuring your CSP data and systems are secure!

Shared Responsibility Model



Customers are responsible for their security and compliance **IN** the Cloud

CSP is responsible for the security **OF** the Cloud

CSP Responsibilities

Physical Security of Data Center

- **Amazon, Google & Microsoft have been building large-scale data centers for many years.**
- **Important attributes:**
  - Non-descript facilities
  - Robust perimeter controls
  - Strictly controlled physical access
  - Two or more levels of two-factor authentication
- **Controlled, need-based access.**
- **All access is logged and reviewed.**
- **Separation of Duties**
  - Employees with physical access don’t have logical privileges.

CSP Responsibilities

VM Security

- **Host (hypervisor) operating system**
  - Individual SSH keyed logins via bastion host for CSP admins
  - All accesses logged and audited
- **Guest (VM Instance) operating system**
  - Customer controlled (customer owns root/admin)
  - CSP admins cannot log in
  - Customer-generated key pairs
- **Stateful firewall**
  - Mandatory inbound firewall, default deny mode
  - Customer controls configuration via firewall settings

Network Security

- IP Spoofing prohibited at host OS level.
- Packet sniffing (promiscuous mode) is ineffective (protected at hypervisor level).
- Unauthorized Port Scanning a violation of TOS and is detected/blocked.
- Inbound ports blocked by default.

CSP Responsibilities

Configuration Management

- Most updates are done in such a manner that they will not impact the customer.
- Changes are authorized, logged, tested, approved, and documented.
- CSP will communicate with customers, either via email, RSS Feeds, various service Health Dashboards and customer-specific Health Dashboards when there is a potential for service being affected.

Built for “Continuous Availability”

- **Scalable, fault tolerant services.**
- **Every region has multiple availability zones (AZs). All AZs are always on.**
  - There is no “Disaster Recovery Datacenter”
  - All managed to the same standards
- **Robust Internet connectivity**
  - Each AZ has redundant, Tier 1 ISP Service Providers
  - Resilient network infrastructure

CSP Responsibilities

Disk Management

- Proprietary disk management prevents customers from accessing each other's data.
- Disks wiped prior to use.
- Disks can also be encrypted by the customer for additional security.

Storage Device Decommissioning

- All storage devices go through process using techniques from:
  - DoD 5220.22-M ("National Industrial Security Program Operating Manual ").
  - NIST 800-88 ("Guidelines for Media Sanitization").
- Ultimately devices are:
  - Degaussed.
  - Physically destroyed.

Under the Shared Responsibility Model

CSP Responsibility? or Customer Responsibility?

Configuring the firewall rules that determine which ports are open on a Linux VM

Patching the operating system with the latest security patches

Installing camera systems to monitor the physical datacenters

Shredding disk drives before they leave a datacenter

Toggling on the Server-side encryption feature for object storage service

Preventing packet sniffing at the hypervisor level

Securing the internal network inside the CSP datacenters

Under the Shared Responsibility Model

CSP Responsibility? or Customer Responsibility?

Configuring the firewall rules that determine which ports are open on a Linux VM

Patching the operating system with the latest security patches

Installing camera systems to monitor the physical datacenters

Shredding disk drives before they leave a datacenter

Toggling on the Server-side encryption feature for object storage service

Preventing packet sniffing at the hypervisor level

Securing the internal network inside the CSP datacenters

gta
GEORGIA
TECHNOLOGY
AUTHORITY

Back to Security Costs

October 3rd, 2022

What is cloud?

On-demand IT resources provided over the internet with a Pay As You Go model

What is cloud?

Elastic
Ubiquitous
Metered

What is cloud?

Elastic
Ubiquitous
Metered

Security ***Costs***

Security ***Costs***

It always has except …

It is no longer a one-time charge

Security ***Costs***

It always has except …

It is no longer a one-time charge

Or even a flat-rate, monthly fee

For example …

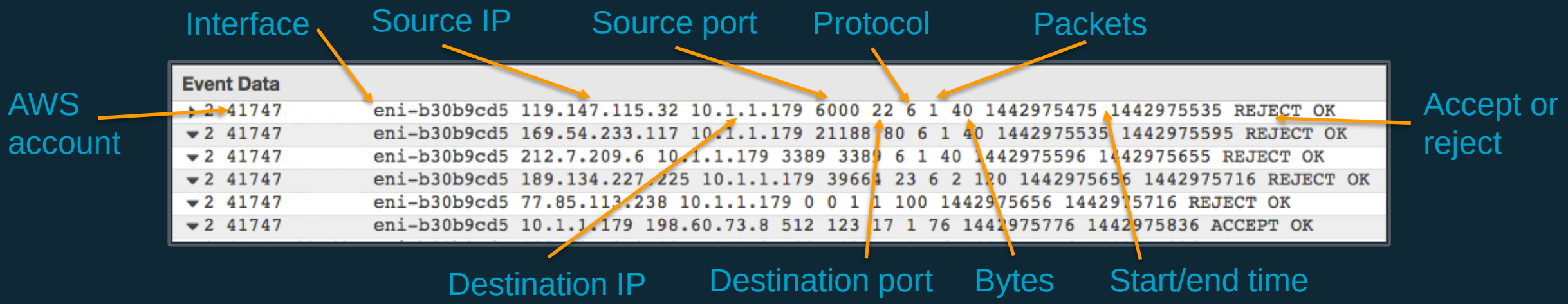
For example …

AWS has a feature called VPC Flow Logs

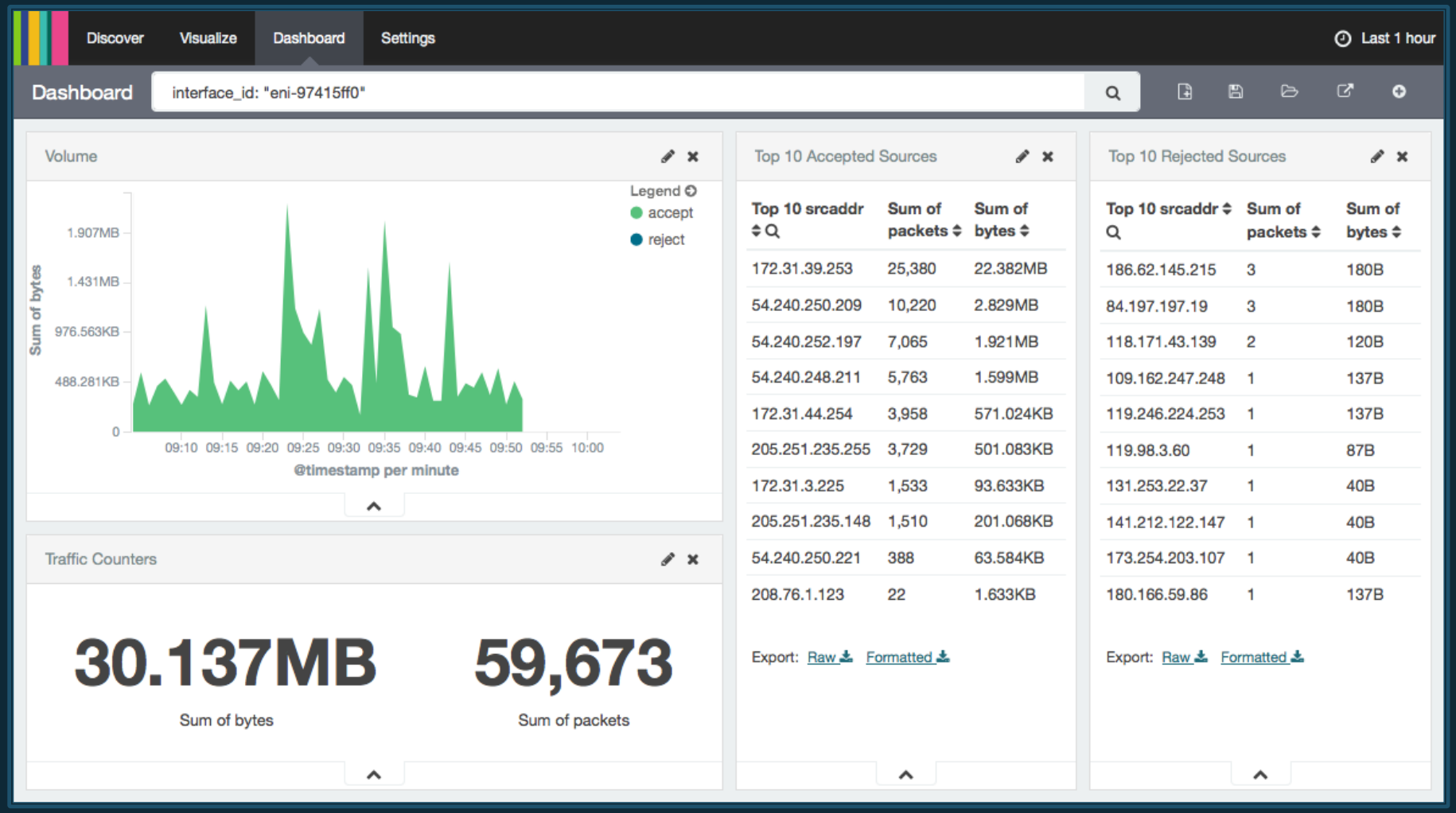
(Google and Microsoft have the same with different names)

VPC Flow Logs

- Agentless
- Enable per ENI, per subnet, or per VPC
- Logged to AWS CloudWatch Logs
- Create CloudWatch metrics from log data
- Alarm on those metrics



VPC Flow Logs



- Amazon Elasticsearch Service
- Amazon CloudWatch Logs subscriptions

What does a systems administrator see?

What does a systems administrator see?

More Data

More Visibility

More Control

More Options

What does a procurement or purchasing person see?

What does a procurement or purchasing person see?

More Cost

None of this is meant to scare you

None of this is meant to scare you

But you do need to have a conversation with your IT people about the on-going security costs within the cloud

None of this is meant to scare you

But you do need to have a conversation with your IT people about the on-going security costs within the cloud

Its all just a math problem

gta
GEORGIA
TECHNOLOGY
AUTHORITY

Security and Risk Mitigation in the Cloud

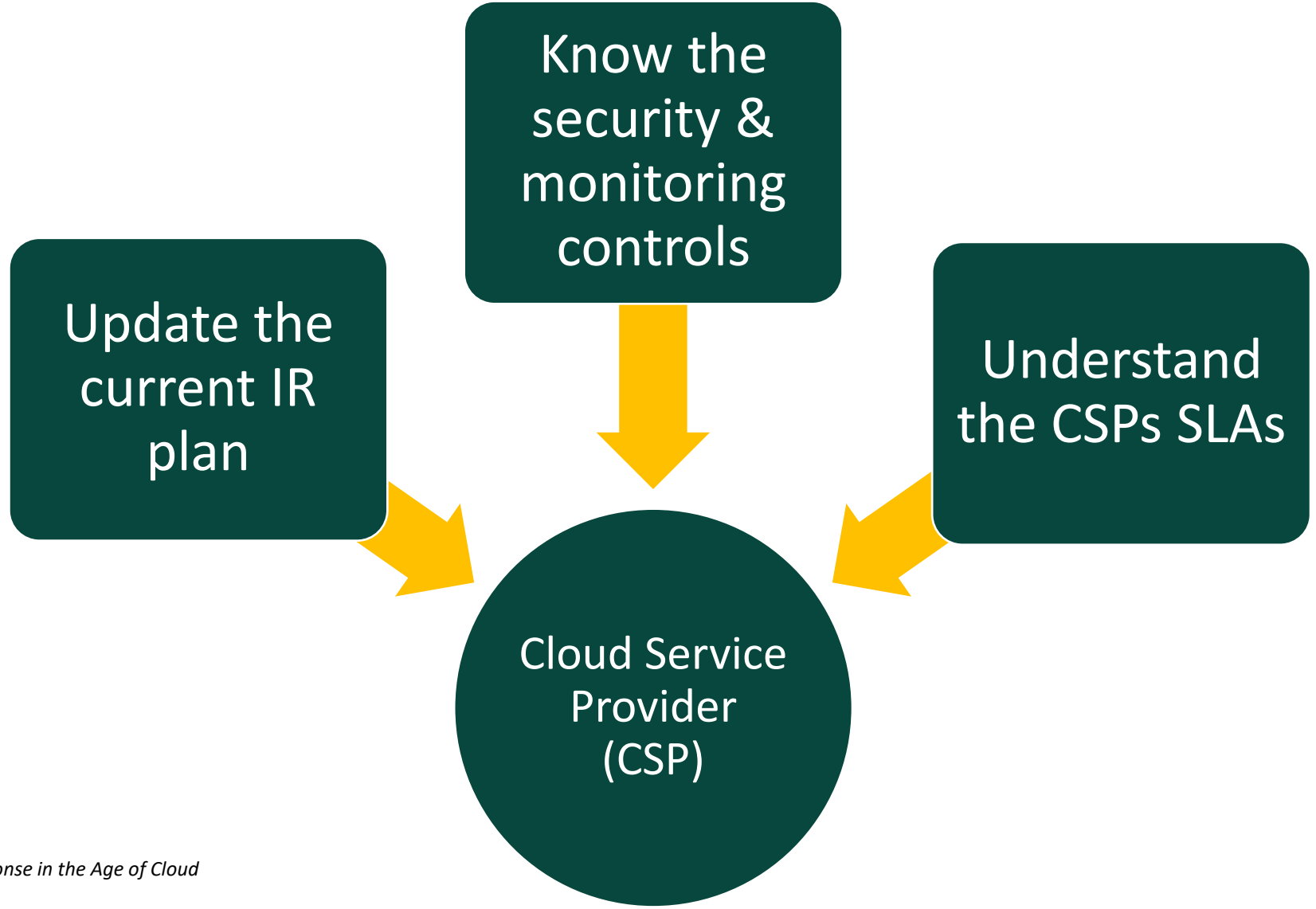
October 3rd, 2022

Key Facts

- Through 2024, workloads that leverage the programmability of cloud infrastructure will suffer 60% fewer incidents than in a traditional datacenter.
- Through 2023, at least 99% of cloud security failures will be the customer's fault.
- Through 2024, Cloud Security Posture Management (CSPM) tools will reduce incident due to misconfiguration by 80%.

Blum, 2020, Rationale Cybersecurity for Business

What to do before you move to the cloud



Ozkaya, 2021, *Incident Response in the Age of Cloud*

Top Threats Facing Cloud Systems

- Insecure Application Programming Interfaces (APIs)
- Account hijacking
- Insider threats
- Data breaches
- Vulnerabilities
- Supply Chain

Ozkaya, 2021, *Incident Response in the Age of Cloud*

Common Factors in Recent Incidents

- Lack of Resources
- Lack of Skills
- Security as an afterthought
- Weak applications
- Weak networks
- System complexity
- Lack of visibility
- Failure to learn from past mistakes

Ozkaya, 2021, *Incident Response in the Age of Cloud*

Cost of a Breach

October 3rd, 2022

2022 Verizon Breach Report – Public Administration

Frequency	2,792 incidents, 537 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 81% of breaches
Threat actors	External (78%), Internal (22%) (breaches)
Actor motives	Financial (80%), Espionage (18%), Ideology (1%), Grudge (1%) (breaches)
Data compromised	Personal (46%), Credentials (34%), Other (28%), Internal (28%) (breaches)

Cost of a Breach - Examples

- Business e-mail compromise (BEC) in the cloud
  - $250K in 3rd party support
    - Does not include the organizational cost of a 3-month effort
- BEC + Enterprise Network
  - $1.5M in 3rd party support
- BEC + Enterprise Network + Sensitive Data Breach
  - Federal and State Reporting Requirements
  - ~$3-5M through recovery

Cost of a Breach - Insurance

- Lose flexibility when invoking the policy (legal drives the train)
- Deductibles continue to rise (most states from roughly $500K to $5M over 4 years)
- Coverage has come down in that same time to roughly equal the policy deductibles
- Many states looking to self-insure utilizing captives and possibly participating in multi-state models