RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: CSV-F03

Secure Innovation in Public Cloud, Myth or Reality?

Rehman Khan

Director, Cloud & Data Security
TD Ameritrade
@cryptorak
https://www.linkedin.com/in/rehmankhan/

Brajesh Moni

Sr. Security Consultant, Cloud & Data Security
TD Ameritrade
https://www.linkedin.com/in/brajeshmoni/

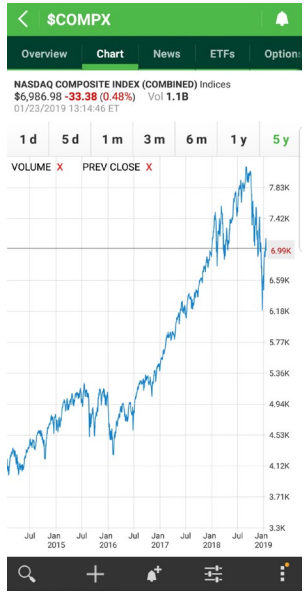
Innovation in Public Cloud

External Drivers

- Businesses continue to find ways to move at a

rapid pace due to competition, and new business models

- Aspirations of social integration, digital innovation, agility, and scale rapidly
- Acquisitions continue to pressure the markets demanding agility
- Business efficiency, reliability and margins



Innovation in Public Cloud

Internal Drivers

- Access to information anywhere from any device by authorized users
- Developers wanting to experiment with new technologies such as voice, AI, Analytics, and chat.
- Reduce IT cost – transform technology spend from capital expenditure to operational expenditure.
- Leverage cloud's agility to address internal customer needs through rapid prototyping, development and deployment product services
- Disrupt legacy competitors using public cloud economy of scale

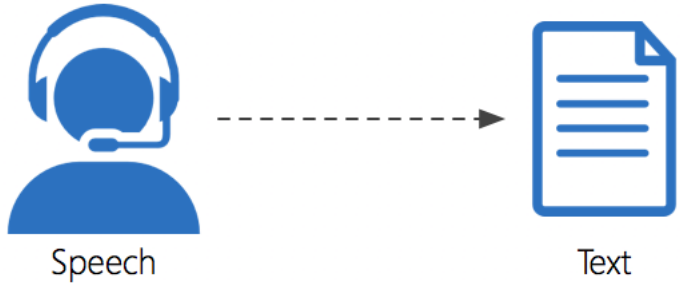
Impediments for Innovation in Public Cloud

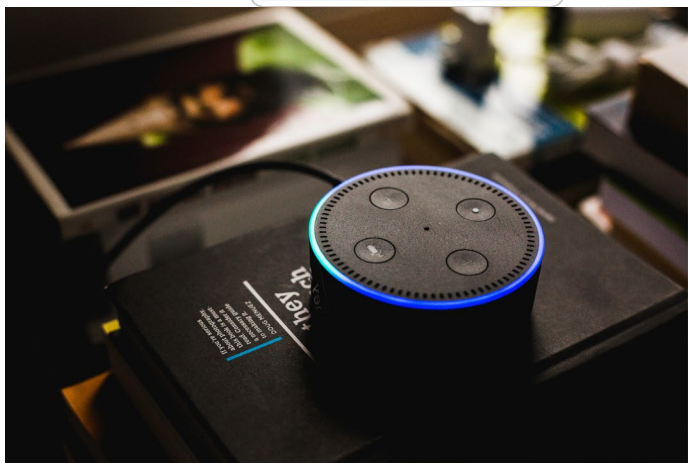
- Default answer is “No”
- Organizations culture; fear of unknown
- Lack of knowledge; public, hybrid, private, IaaS, PaaS, SaaS.
- Without understanding the business use-cases, you can’t understand what are real threats and risks to the use-case.
- Security teams are not equipped with technical skills that provide developers, data scientists with confidence.

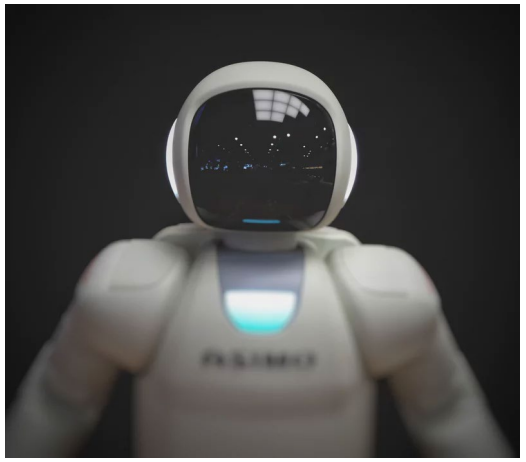
Innovation in Public Cloud – Use Cases

Business Use-cases

- Analytics in the cloud
  - Speech to text
- Mechanical Turk
  - Outsourced Data Annotation
- Artificial Intelligence & ML
  - knowledge base, Data classification
- IOTs
  - Alexa
- WeChat, Apple Pay
  - Expanded sales Channel







Foundational Components: Deliverable #1

Get Executive Buy-in First because Cloud Security is Job Zero

- Step 1: Present to Executive leadership such as CRO, CPO, CLO, CFO and even sometimes CEO about the basics of Cloud Computing Story
- Step 2: Be transparent about current realities, there are already cloud applications being used
- Step 3: Share what you are going to do to manage risk about it in the short and long term.
- Step 4: Walk-through your capability roadmap and execution delivery plan
- Step 5: Go back and present iterative progress or lack thereof

Foundational Components: Deliverable #2

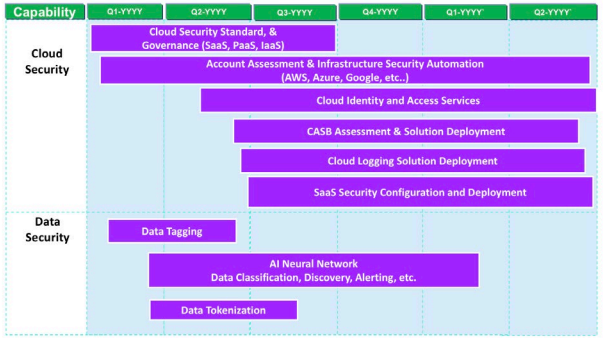
Establish a Cloud Security Department

- Bring in talent with cloud, security and technical (development) skills.
- Understand the actual business problem & use-cases, opens up the communications.
- Build relationship with Key stakeholders – Innovation, development and procurement teams.
- Establish clarity on what data is being worked on and how to protect it
- Focus on security controls that apply to use-cases instead of blanket controls

Foundational Components: Deliverable #3

Create & Communicate Cloud Security Product Goals

1. **<u>Reduce Risk:</u> Establish** an effective cloud security product to protect data and provide lite governance using complementary set of best-in-class tools and methods.
2. **<u>Agile Transformation:</u> Enable,** automate and integrate security controls day zero. Make it easy for business and developers to go fast securely in the cloud.
3. **<u>Left-Shift with Partnerships :</u> Innovate** securely with teams and make cloud secure from day zero
4. **<u>Technology specific solutions: Accelerate</u>** <u>security solution deployment</u> (e.g. Public Cloud workload, Mobile, SaaS and Vendor applications)
5. **<u>Create a nimble cloud security roadmap</u>**



Foundational Components: Deliverable #4

Cloud Security Engagement Model

- Identify and build relationships with innovation teams
- Build partnership with Supply management.
- Augment Vendor assessment with Cloud Security Specific Questionnaire.
- Communicate proactively
  - Monthly Cloud Security Tech Talks
  - Cloud Security Immersion Day
  - Create a collaborative channels for innovators and developers.

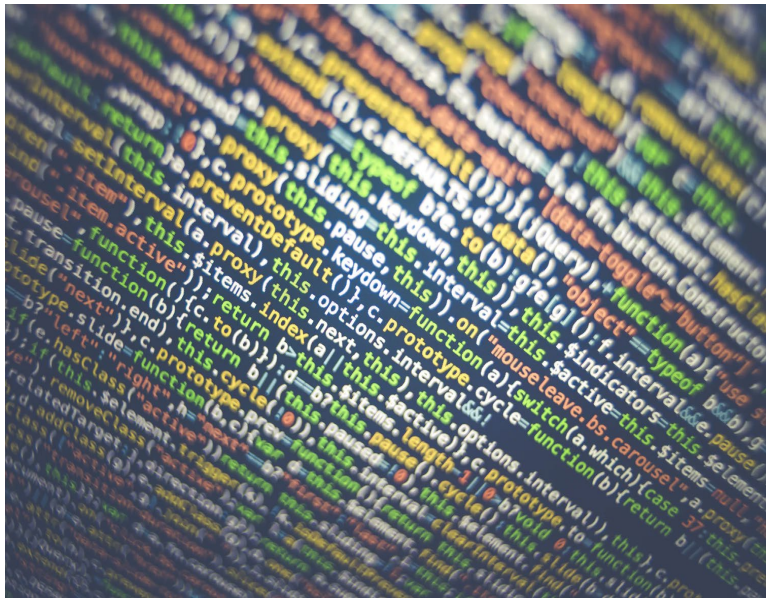
Foundational Components: Deliverable #5

Cloud Security Policy and Standards

- Set high level cloud security policy statement.
- Create Cloud Security Standards, includes
  - Identity and Access Management
  - Cloud Data security and information lifecycle.
  - Encryption and Key Management
  - Audit logging and log management
  - Security alerting and monitoring
- Leverage existing security standards

Technical Components: Deliverable #6

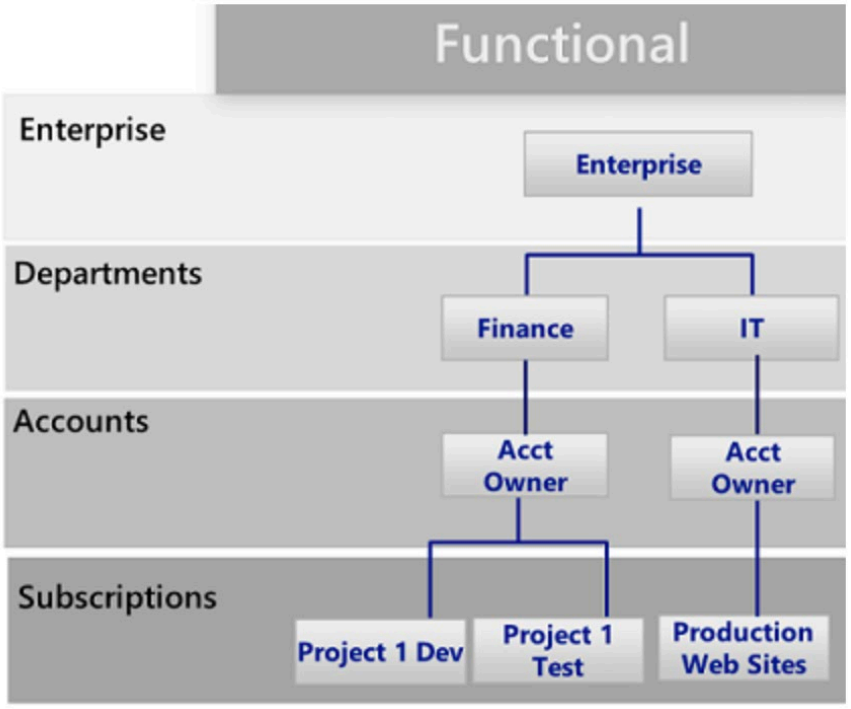
Deploy Cloud native security Platforms & security as code capabilities

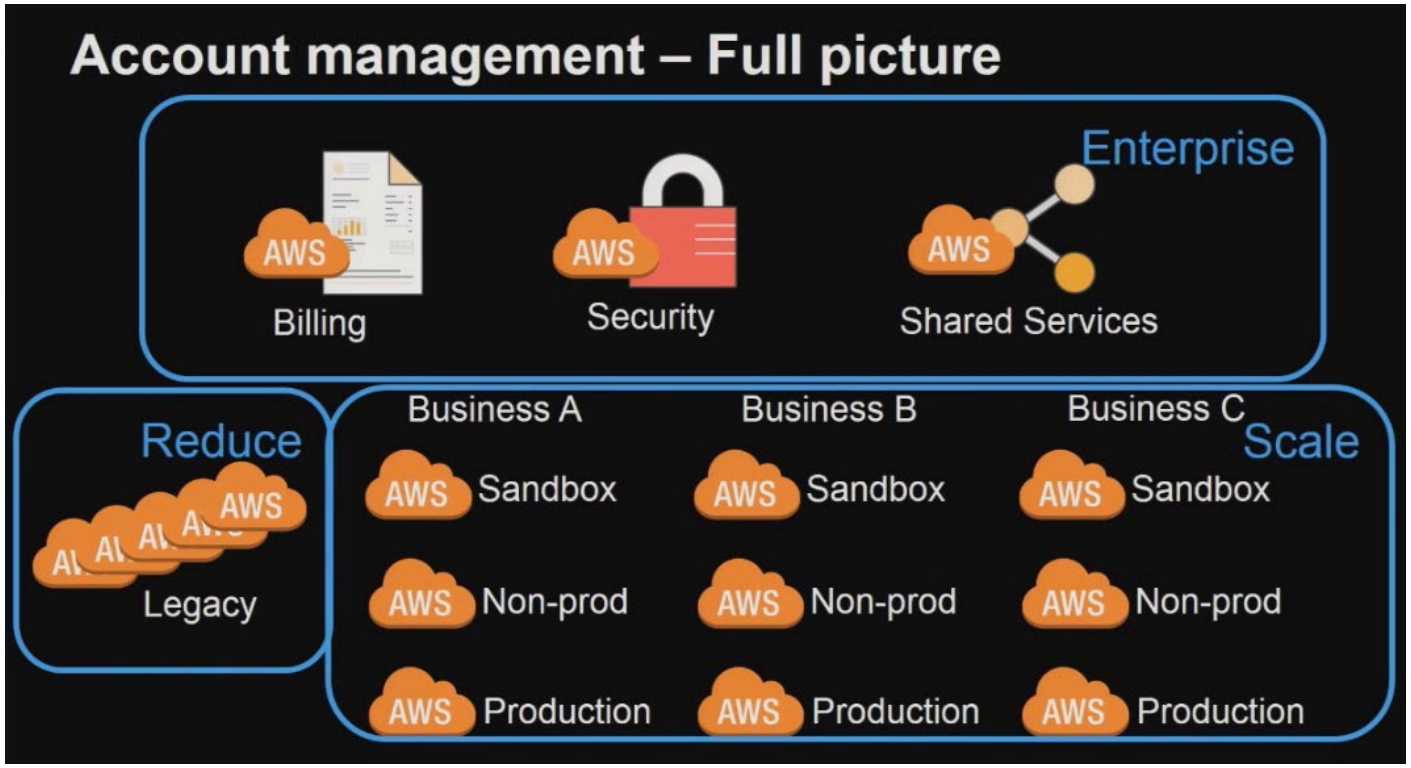


- Create your own pipeline and agile practice
- Don’t boil the security tools ocean to address the risks – start with low hanging CSP native security tools – e.g.: tenant restrictions, IP whitelisting
- Focus on key risk attributes, access flow and data elements - (Restricted, PII, PCI).
  - Scrub, tokenize/mask restricted/confidential data
- Don’t try to integrate security to the mothership for all security capabilities

Technical Components: Deliverable #7

Deploy secure account/subscription model

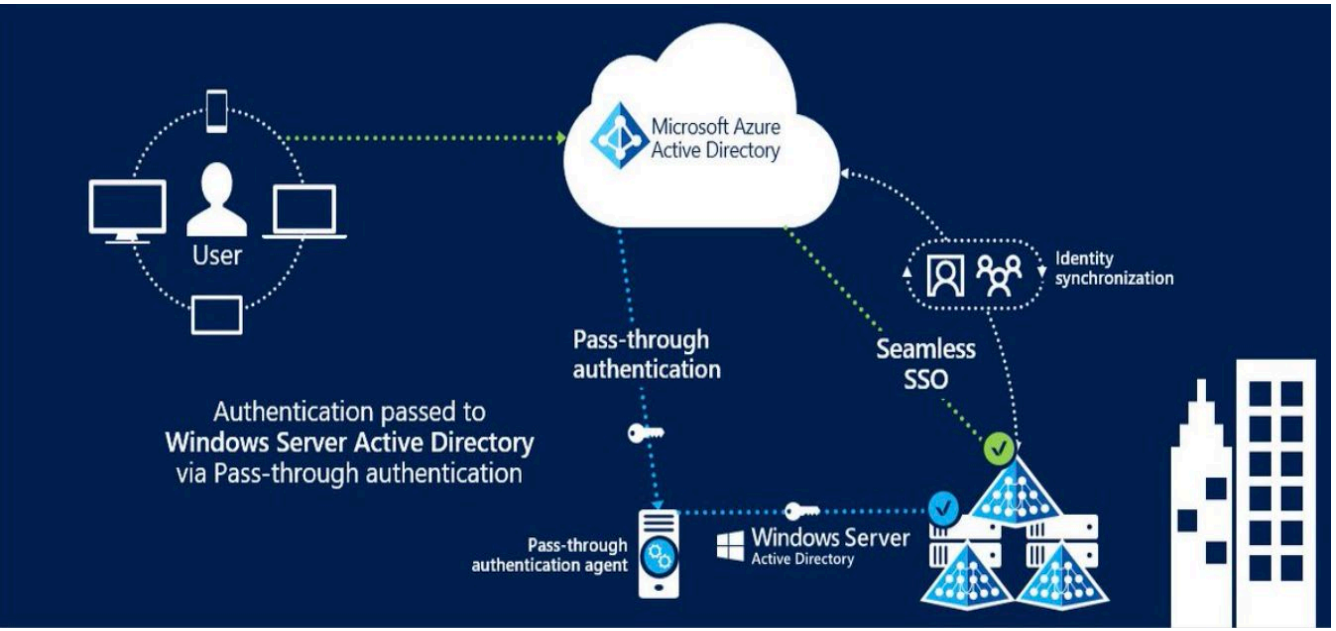


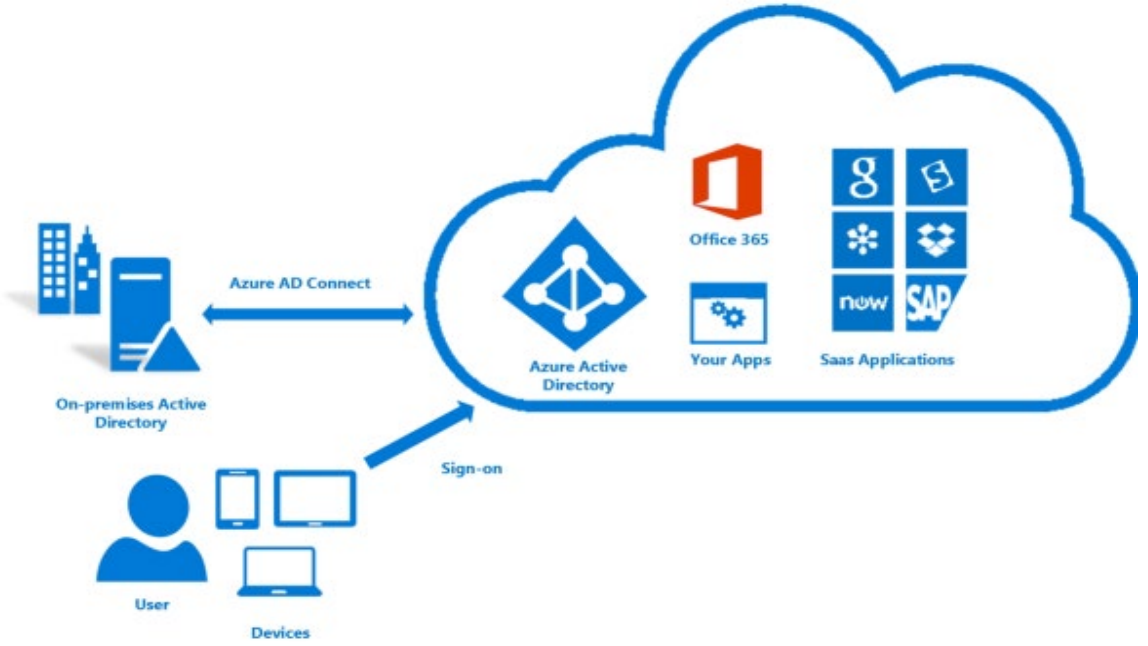


- Adopt a secure account/subscription model.
- Focus on Blast radius reduction model.

Technical Components: Deliverable #8

Establish strong Cloud Identity and Access Management

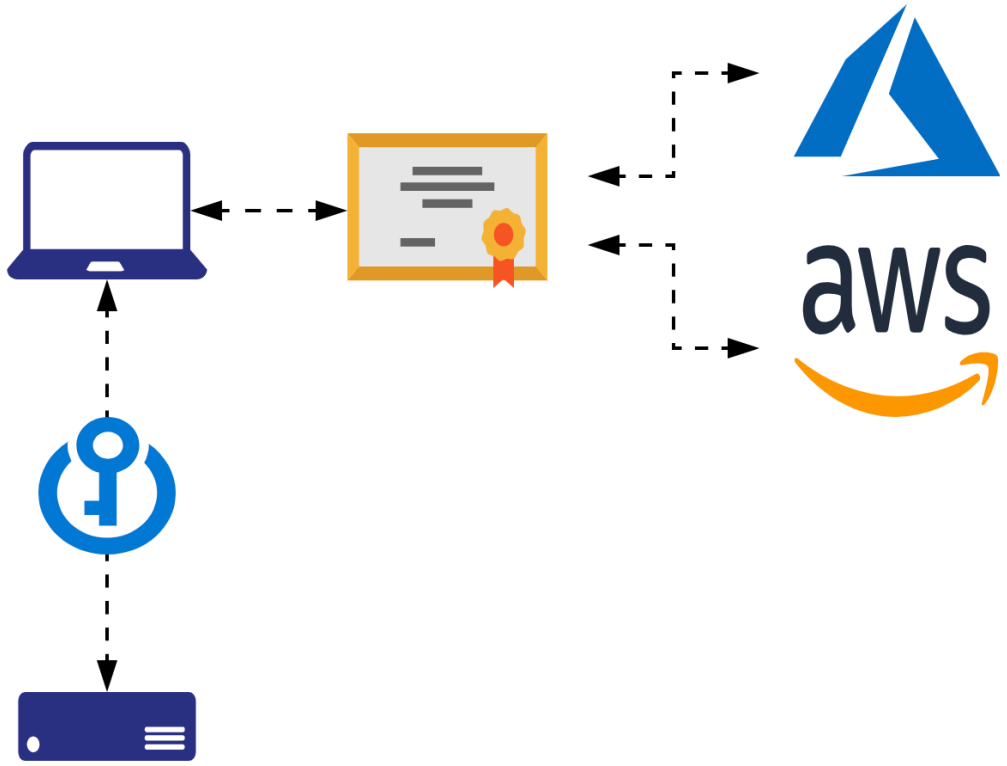




- Identity is the security perimeter and the control plane
- Establish all cloud workload authentication and authorization through enterprise identity store.
- Enable CSP native Identity protection capabilities

Technical Components: Deliverable #9

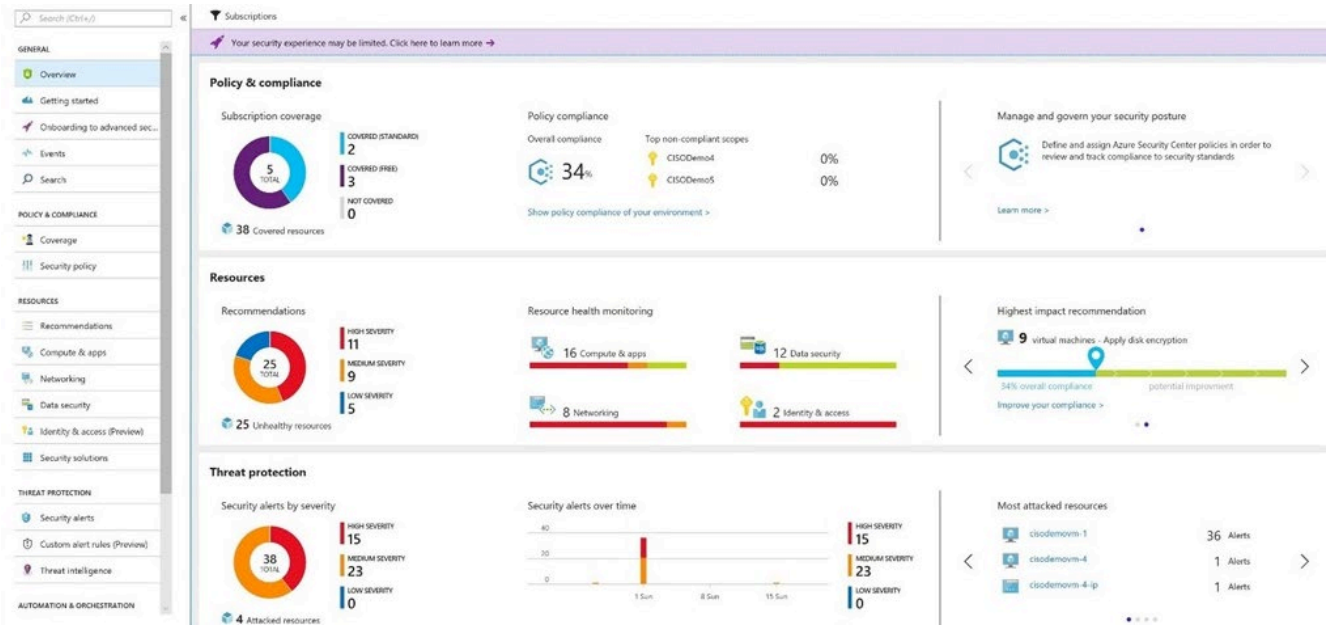
Establish strong encryption and key management solutions

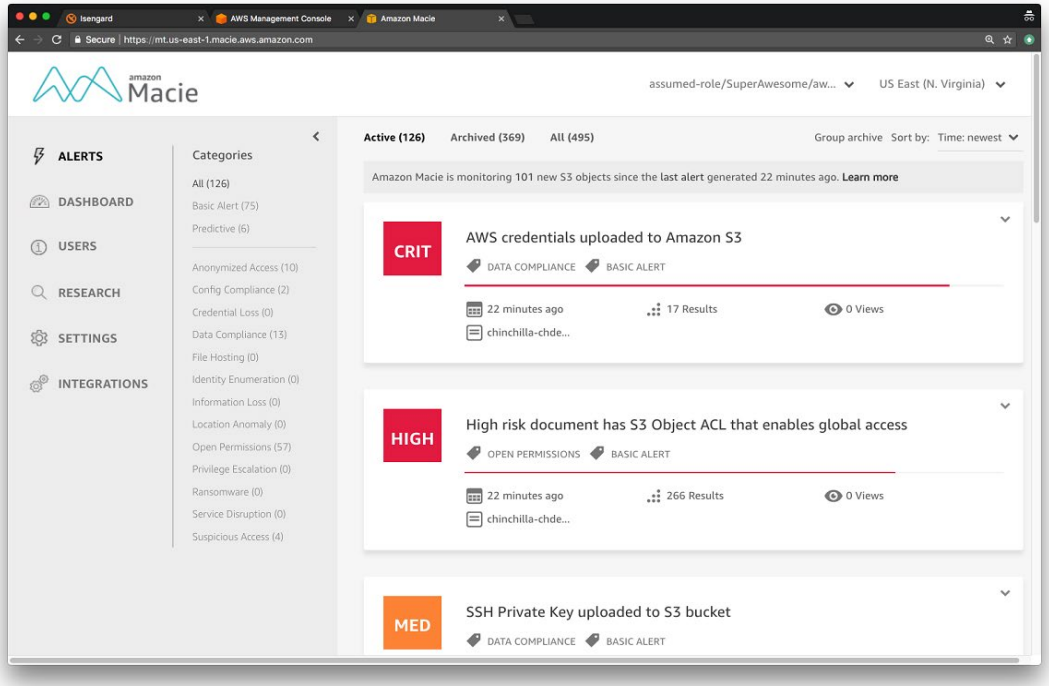


- Enable Cloud Native Key Management Solutions
  - Azure Key Vault
  - AWS Key Management Service (KMS)
- Bring Your Own Key (BYOK)
  - Protect keys using Hardware Security Modules (HSMs)
- Automate the rotation of keys
  - Develop a process/timeline for rotating keys in and out of management solutions
- Enable Data At Rest / Data In Transit Encryption
  - At Rest – Virtual Disks, Databases, Storage
  - In Transit – SSL/TLS

Technical Components: Deliverable #10

Establish ML enabled data classification



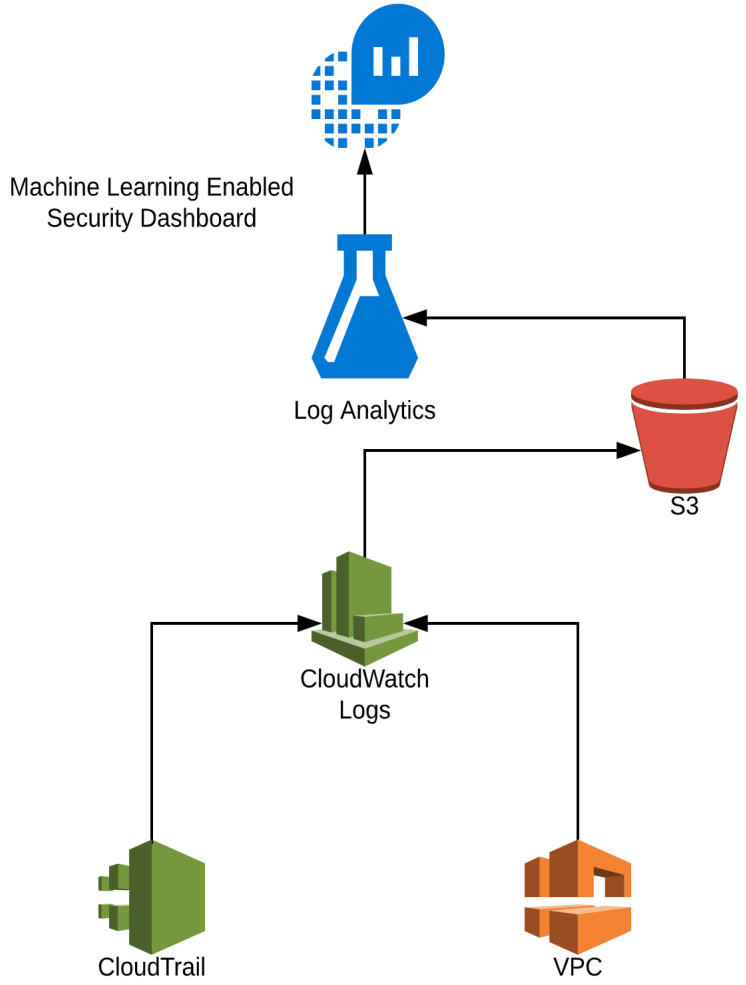


- Enable Cloud Native Data Classification solutions
  - Azure Information Protection (AIP)
  - Amazon Macie

- Classify
  - Automate data classification(AIP, Macie)
- Label
  - Automate data labeling
- Protect
  - Apply policies based on the data risk level.

Technical Components: Deliverable #11

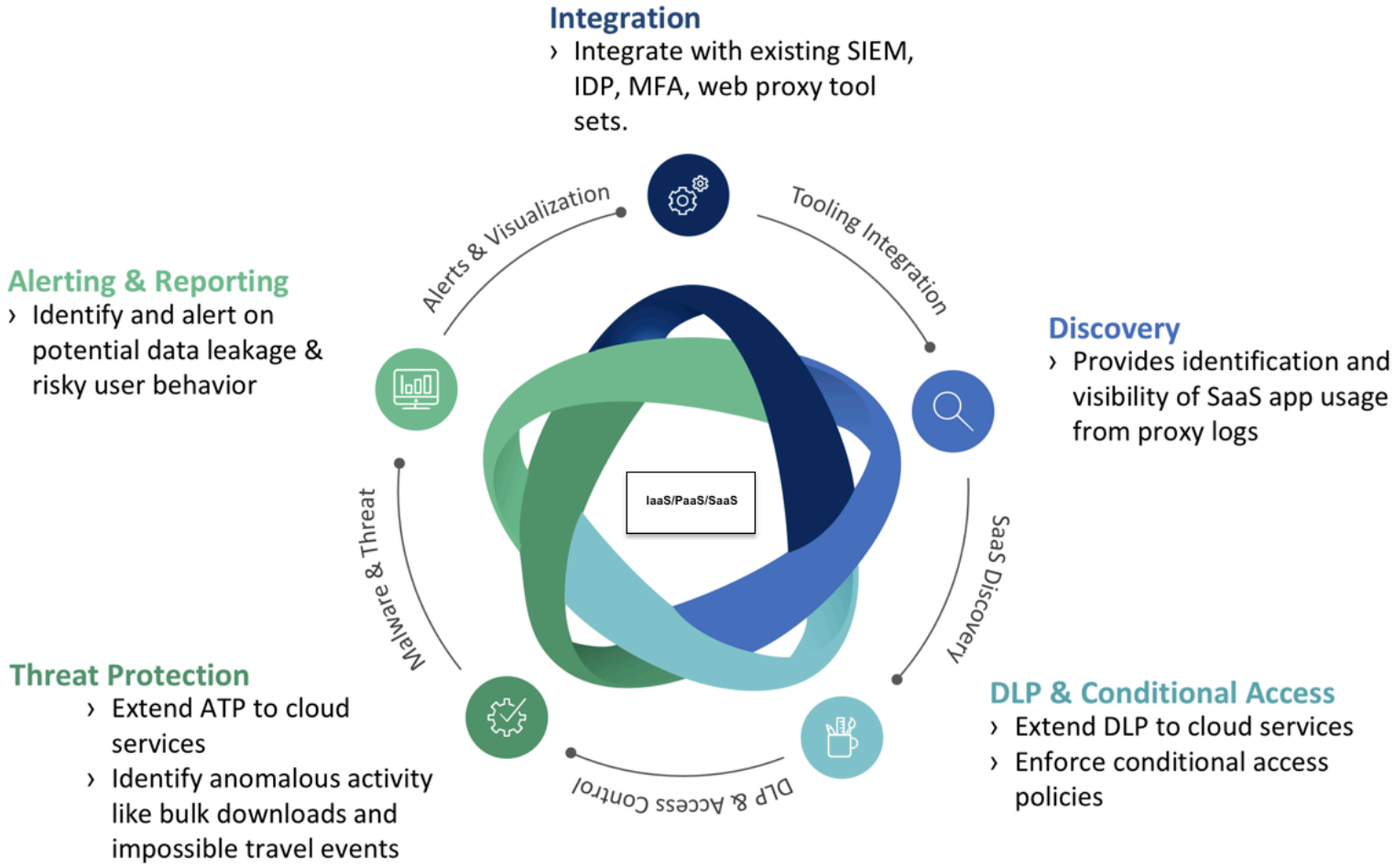
Cloud logging & Monitoring



- Centralize & Ingest Cloud Log Data
- Explore the data – for critical operational & security insight.
- Define alerts, security events
- – categorize & Score risk events
- – collaborate and provide visibility to Incident response and Vulnerability teams.
- Enable native logging and monitoring dashboards – Azure Security, AWS Security
- Automate event response and apply ML by enabling native CSP and SIEM tool sets.
- Evaluate the results and iterate logging and monitoring deployment model.

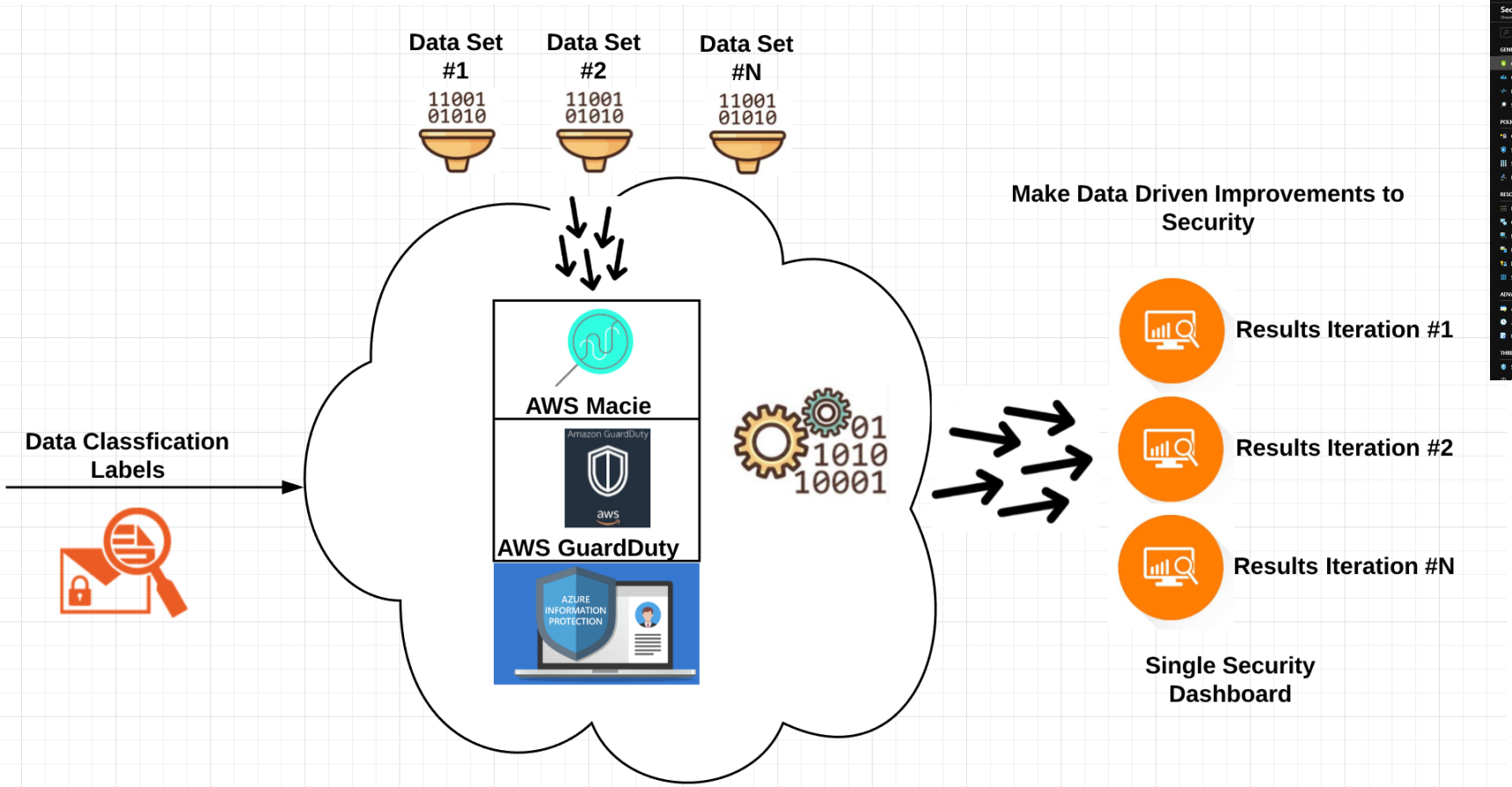
Technical Components: Deliverable #12

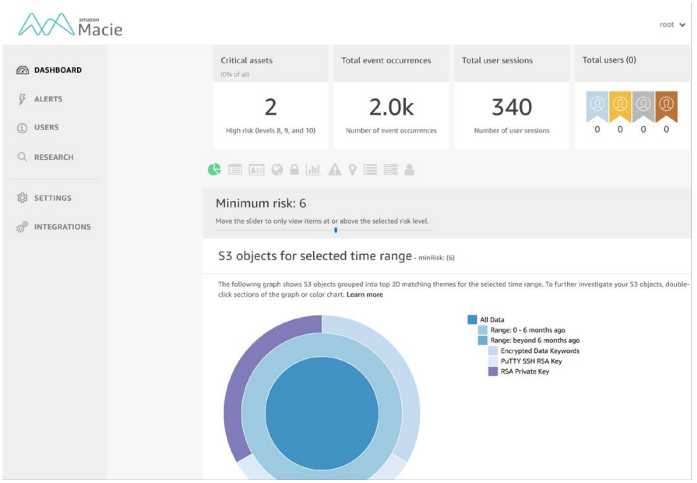
Cloud Access Security Broker



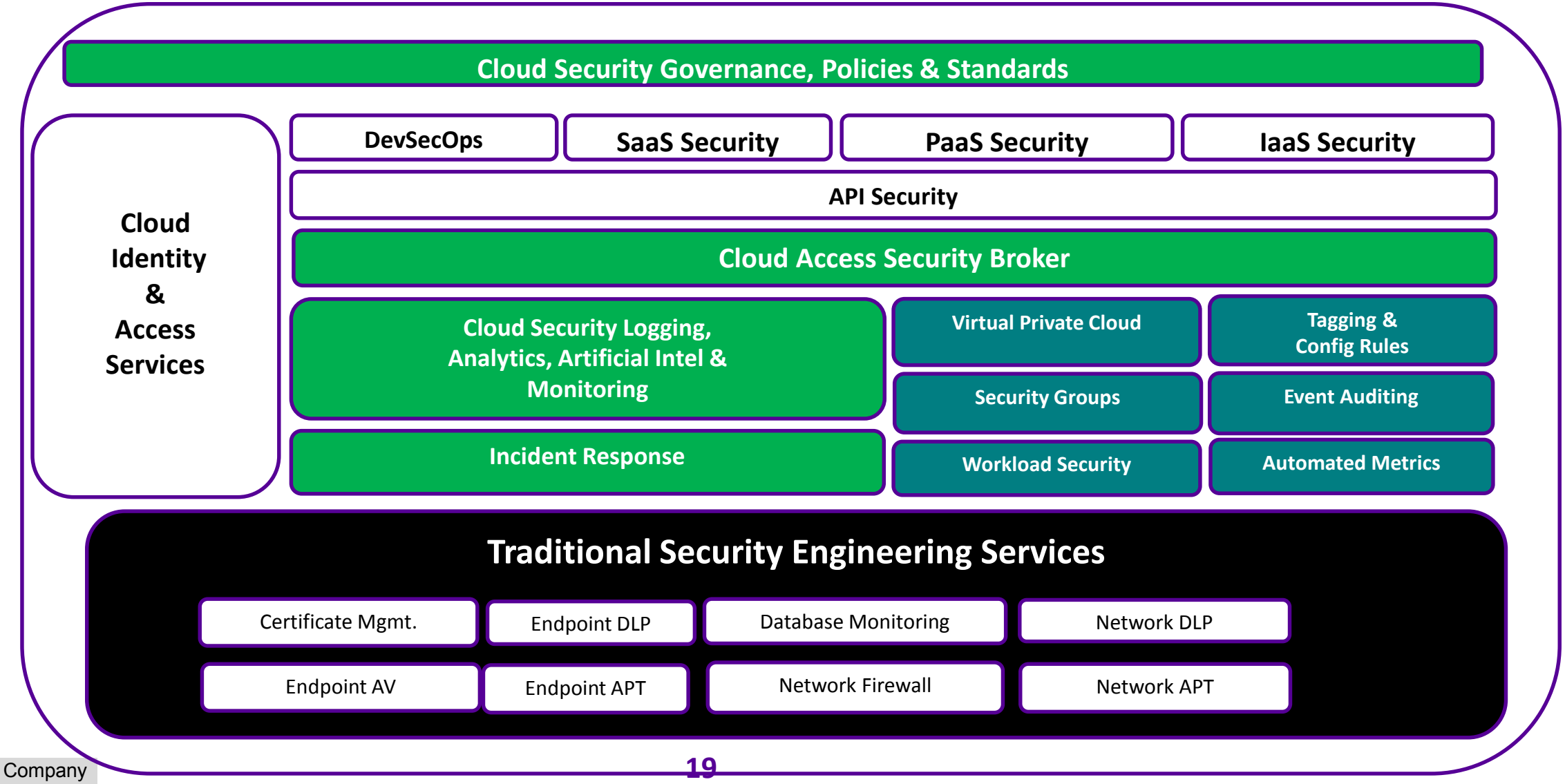
- Discovery & Visibility
- Granular Identity access control.
- Tighten integration with on-perm tools
- Threat Protection
- Data Loss Prevention

Cloud Security Insights Matter





Putting it all Together Cloud Security Platform !



Presenter's Company Logo – replace or delete on master slide

Leverage Cloud based Security solutions

Key Benefits:

Cloud Service and Application Providers are fast, better equipped with advanced security tools, automation and security engineering resources than traditional IT organizations

- Builds trust model with the business results into more engagements
- Remove traditional IT obstacles by partnering early with infrastructure organizations
- Enable Automated Cloud management security solution.
- Start integrating with enterprise solutions such as aggregated Cloud logging solution or SIEM Integration.
- Risk Information sharing across the Security organization for visibility and actions/exceptions that are required for an innovation

Reality Checklist

- Get Executive Buy-in First
- Establish a Cloud Security Organization with a Governance program
- Communicate Cloud Security Product Goals
- Cloud security engagement model
- Cloud Security Policy and Standards
- Deploy Cloud native security Platforms & security as code capabilities
- Deploy secure account/subscription model
- Establish strong Cloud Identity and Access Management
- Establish strong encryption and key management solutions
- Establish ML enabled data classification
- Cloud logging & Monitoring
- Cloud Access Security Broker(CASB)

Useful Links

- **Cloud Security**

  https://aws.amazon.com/products/security/?nc2=h_m1

  https://azure.microsoft.com/en-us/product-categories/security/

  https://cloud.google.com/security/

  https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Data Monitoring & Protection:

- Azure Information Protection – https://azure.microsoft.com/en-us/services/information-protection/
- GCP StackDriver – https://cloud.google.com/monitoring/
- AWS Macie – https://aws.amazon.com/macie/

APPENDIX