SAND2018-7462C

It's Raining Clouds: Maintaining Visibility in the Haze

PRESENTED BY

Gio K. Kao, Ph.D.

UNCLASSIFIED UNLIMITED RELEASE

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Overview

- Introduction
- Cloud Security Info
- Challenges
- Lesson-learned and Best practices
- Conclusions

First, why are we using cloud?

Innovation:

- Better linked to emerging technologies (e g ,devices)
- Shift focus from asset ownership to service management
- Tap into private sector innovation

Agility:

- More responsive to urgent agency needs
- Purchase "as-a-service" from trusted cloud providers
- Near-instantaneous increases and reductions in capacity

Efficiency:

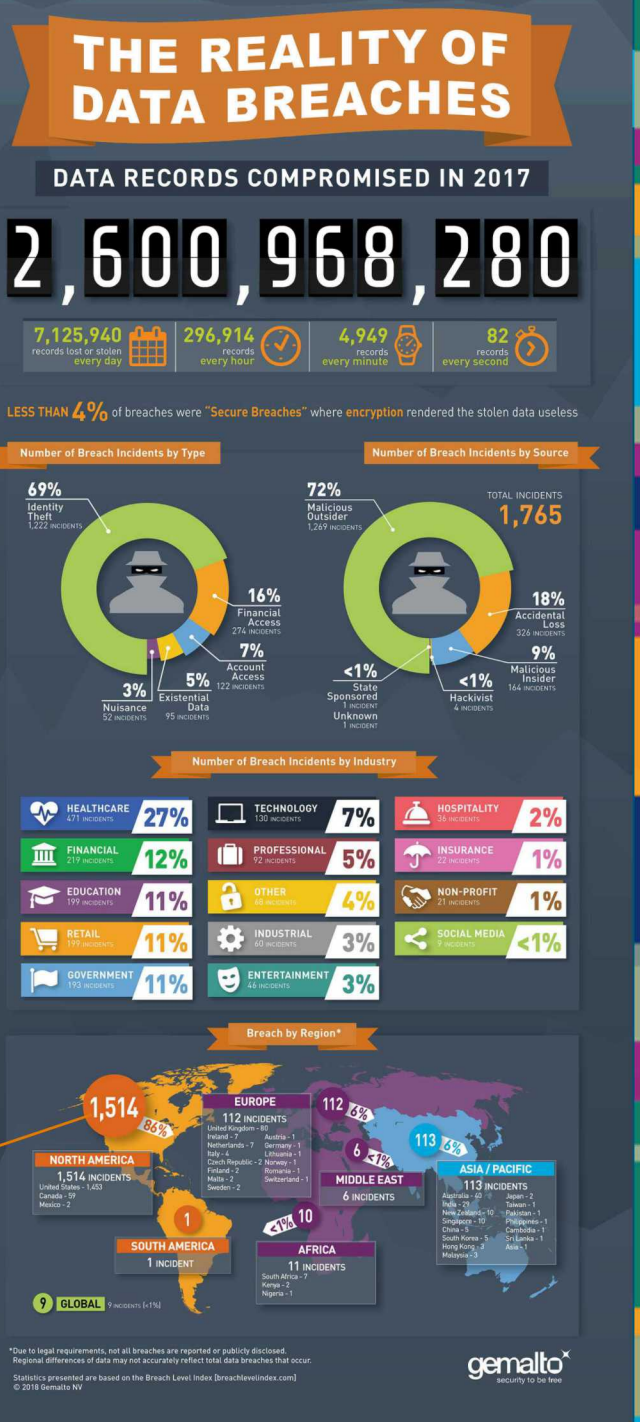
- Improved asset utilization (server utilization > 60-70%)
- Improved productivity in application development, application management, network, and end-user

… But not what this talk is about. This talk is about Security.

2017 was named “The Year of the Breach”

“Poor security practices were .. evident in the way multiple organizations mismanaged their Amazon Web Services (AWS) resources. Entities such as the National Security Agency (NSA), the Pentagon, and tech giant Accenture didn’t properly configure their S3 buckets. As a result, members of the public could read and write to sometimes hundreds of gigabytes of exposed data.”

Deep Root Analytics/ Republican National Committee	198,000,000	06/13/17	Identity Theft	Accidental Loss	United States
U.S Department of the Interior, U.S. Office of Personnel Management	22,000,000	04/01/15	Identity Theft	State Sponsored	United States
United State Voters	191,337,174	12/28/15	Identity Theft	Accidental Loss	United States



Why is security different in the cloud?

- Cloud's resources are owned and managed by Cloud Service Providers (CSPs) and customers
- Thus security is managed by CSPs and customers
  - Shared security responsibility model
- Differences Between On-Prem and Cloud:
- Difficulties arise with:
  - Ephemerality
  - Attribution
  - Geo-political boundaries
  - Data governance
  - Shared responsibilities
  - …

To the CSP: Cloud Security is an after thought

Cloud Security: There are Resources for Guidance…

Cloud Security Alliance (CSA) Guidance

- Well maintained source of security guidance for the cloud

NIST

- Cloud providers provide extensive documentation
  - Reference Architectures
  - Best Practices

FedRAMP

Will help with creating a secure cloud deployment but ultimately its up to your organization to secure your cloud deployments

Security responsibility differs based on cloud model

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

No cloud provider will take full ownership of all cybersecurity controls and requirements.

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- Based on security requirements defined by NIST 800-53 standard and provides a uniform approach to risk based management.
- Enables federal agencies to save significant time, costs and resources in their evaluation of the security of cloud providers.
- Aid Government customers implementing and documenting system-specific security controls implemented.

CSPs interested in having the U.S. Government as a consumer of their service must meet the FedRAMP security requirements and implement FedRAMP baseline security controls.

Example: Azure's Customer Responsibility Matrix (CRM) explicitly lists all NIST SP 800-53 security control requirements for FedRAMP baselines that include a customer implementation requirement.

- Includes controls with
  - shared responsibility between Azure and Azure customers,
  - fully implemented by Azure customers.

FedRAMP: Example Microsoft O365 and Azure

O365:

- O365 GCC provides compliance with FedRAMP Moderate
- O365 GCC High and DoD environments deliver compliance with DoD Security Requirements Guidelines, Defense Federal Acquisition Regulations Supplement (DFARS), and International Traffic in Arms Regulations (ITAR).

Azure:

- Azure Commercial - FedRAMP moderate
- Azure Gov – FedRAMP high

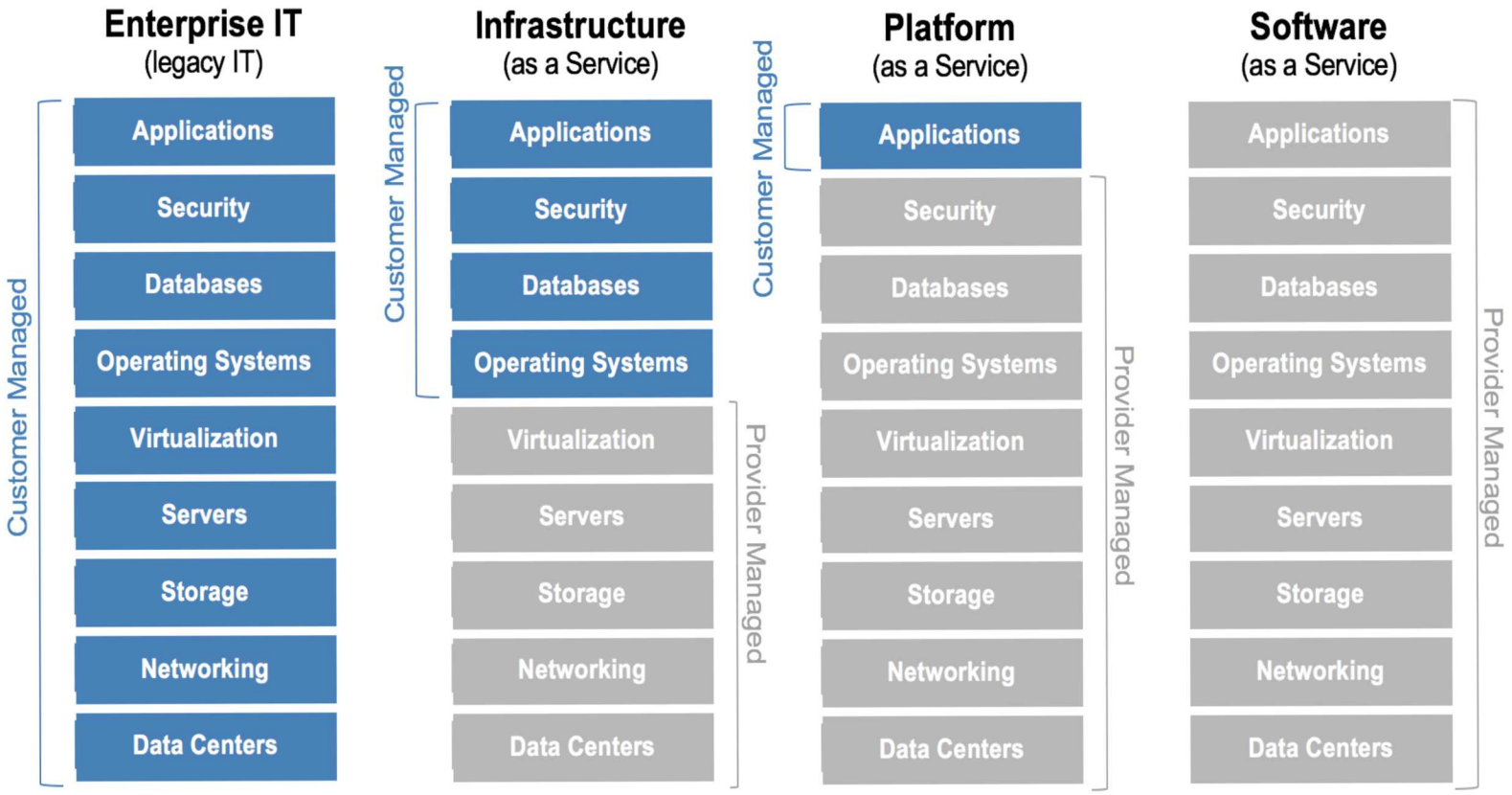
Not all CSP security modules are available in both Azure Commercial and Azure Gov

- More security modules are available in CSP's Commercial

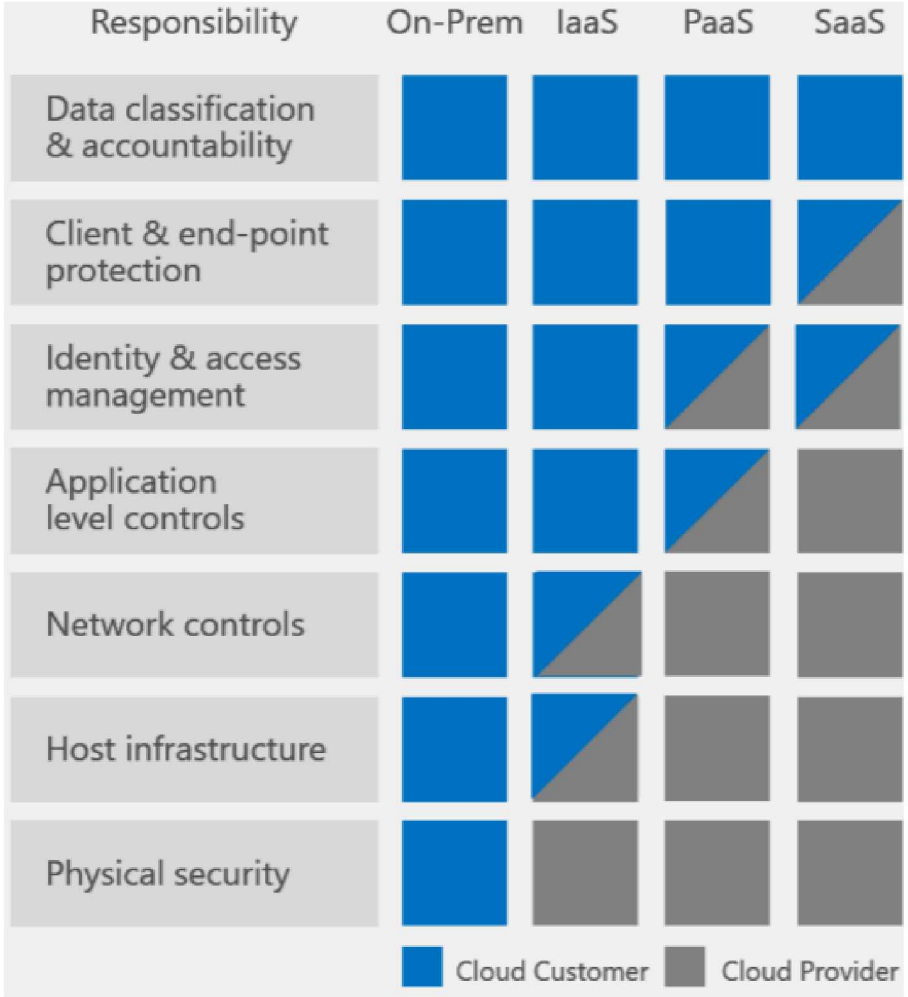
Example implementation for FedRAMP – Moderate:

- Azure commercial (rated FedRamp – moderate) for Azure Active Directory (AAD)
- O365 GCC - O365 GCC interfaces to Azure Commercial – cannot interface to Azure Govt (Azure Govt is higher protection)

Cloud Shared Security Responsibility Model



Shared Security Responsibility Model

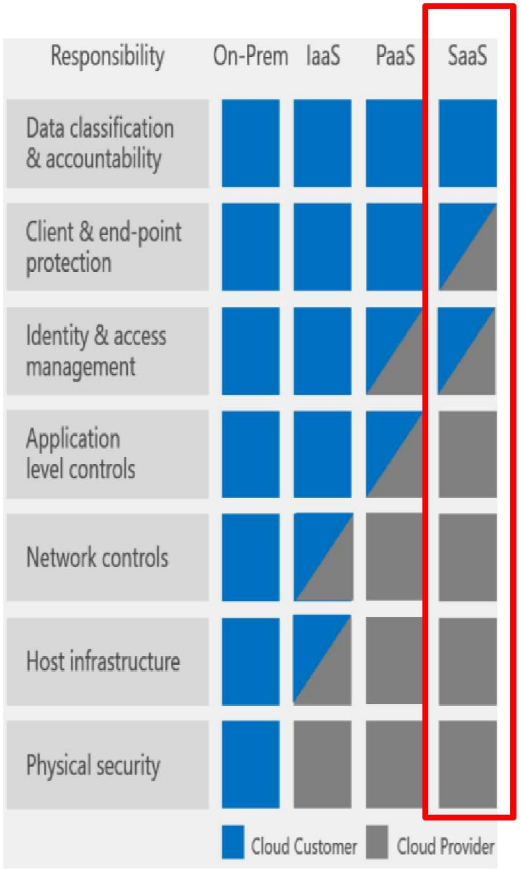


Service models determine the level of responsibility that either the customer or cloud service provider has.

Shared Security Responsibility Model: SaaS

Customer has least control over security implementations

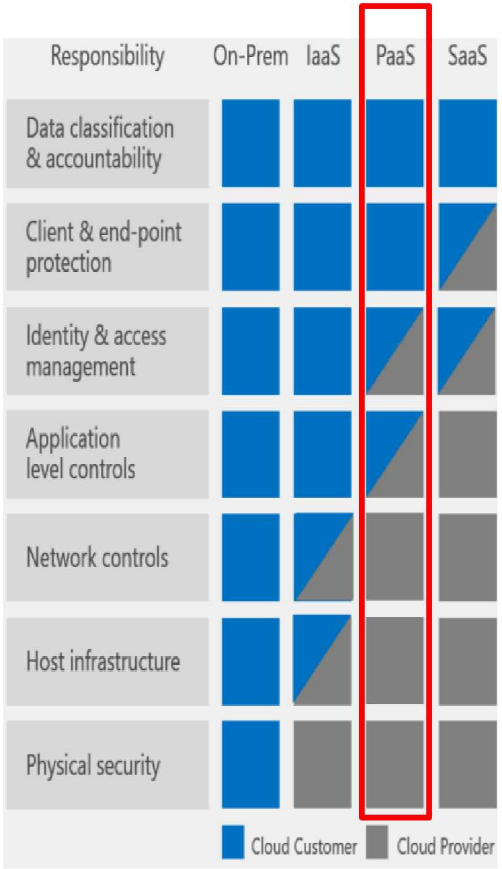
- Access control
  - Strong password policies
  - Multifactor authentication
  - Identity federation
  - Role granularity & privileged user access control
- Data Loss Prevention (DLP)



Shared Security Responsibility Model: PaaS

Includes the SaaS security concerns plus

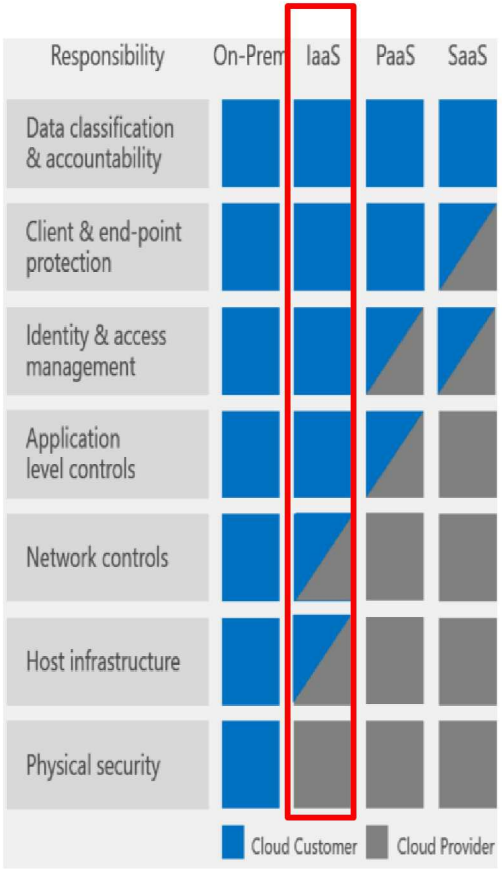
- Operating system (OS) image configuration and patching
  - Some PaaS have more limited control over OS
- Application configuration and libraries
- User and user role security
- Access authentication and authorization
  - Control access to admin consoles



Shared Security Responsibility Model: IaaS

Includes the SaaS and PaaS security concerns plus:

- OS and above
  - Hardening
  - Image integrity
  - Access roles and privileges
- Network access controls (e.g., network security groups)
- Network monitoring
- Network function virtualization



Configuration and Patch Management Responsibility

SaaS

- All applications, infrastructure, VMs and patching maintained by CSP

PaaS

- Infrastructure, VMs and patching maintained by CSP
- Applications maintained by customer

IaaS

- Back-end infrastructure and virtualization platforms maintained by CSP
- Applications, OS, VMs maintained by customer

CSPs provide some tools to help:

- for IaaS: ***AWS Config*** enables image baseline definition, monitoring, and alert on changes
- ***AWS Inspector:*** Enables vulnerability assessment of deployed system

Some Cloud Security Challenges

Challenges revolve around:

- **Identity and Access Management**
- **Logging and Visibility**
- **Policy**
- **Forensics & Incident Response**
- **Outsourcing data and possibly applications**
  - Modified threat surface
  - Shared Security Responsibility between the customer and CSP
  - Service Level Agreement (SLA)
- **Virtualization**
  - Multitenancy
  - VM Migration / VM Location
  - Forensically "sound" images

Cloud Security Challenges: Identity and Access Management (IAM)

IAM challenges

- Authentication
- Authorization
  - Use policy to determine access with Users, Roles, Groups
  - Azure uses Role-Based Access Control (RBAC)
- Federated identities
  - Extend authoritative repositories (i.e., Active Directory) to cloud and/or use token service
- Single sign-on (SSO)
- Auditing and user activity monitoring
  - Log info needed for audits

Cloud Security Challenges: Logging and Visibility

Lack of Visibility

- East/West traffic and North/South traffic.
- Ephemeral VMs (instances)
  - An instance may last 30 seconds – did we log data, did we store? Capture image?
- Traffic not logged:
  - Traffic generated by instances when they contact the cloud DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.
  - DHCP traffic

Vulnerability scans

- Virtual Machines (VMs) are being spun up and down frequently, making it more difficult for a scheduled scan to cover all assets.

Log archival considerations:

- Retention: How long does CSP retain logs?
  - How log does the customer require?
  - Customer may have to write logs to customer managed data store

Cloud Security Challenges: Policy

- Organizations will need to update their existing policies to accommodate cloud services
  - Outsourced services (Shared responsibility)
  - Service Level Agreements (SLA)
  - New issues per compliance
  - Audit policies

- Policies and how we do things in the cloud will change
  - Security assessment policies
    - Vulnerability scans, penetration testing
  - Incident Response (IR)
  - Identity and Access Management (IAM)

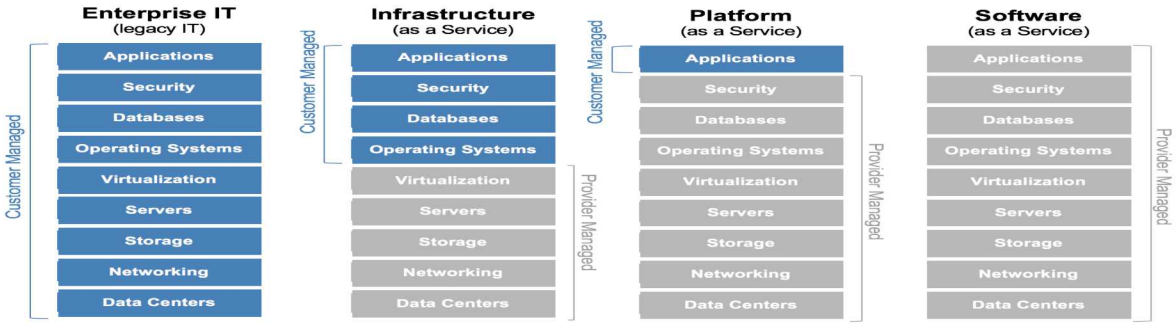
Cloud Security Challenges: Forensics & Incident Response

Digital forensics foundations:

- Identification of an incident from its source(s) and determine its type.
- Acquisition of evidence from various sources.
- Preservation of the state of evidential data
- Analysis of evidential data, reconstructing fragments and drawing conclusions
- Reporting of results and conclusions about the evidence

IR Lifecycle foundations:

- IR: preparation, detection/analysis, containment, eradication and recovery.
- Incident management includes responding to an incident (cyber), vulnerability and artifact handling, and other related services



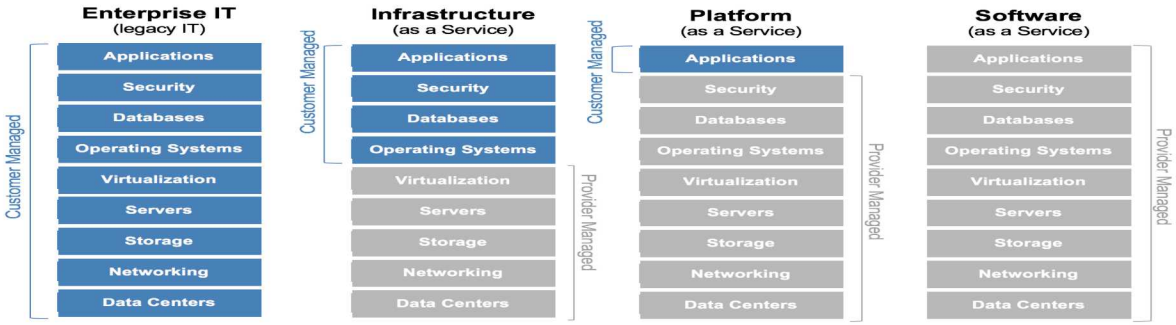
Threat Surface: Is the cloud a new attack surface?

Yes!

- But, the cloud has some of the same issues as on-prem
  - Example:Azure 0day Cross-Site Scripting (XSS) in August, 2016

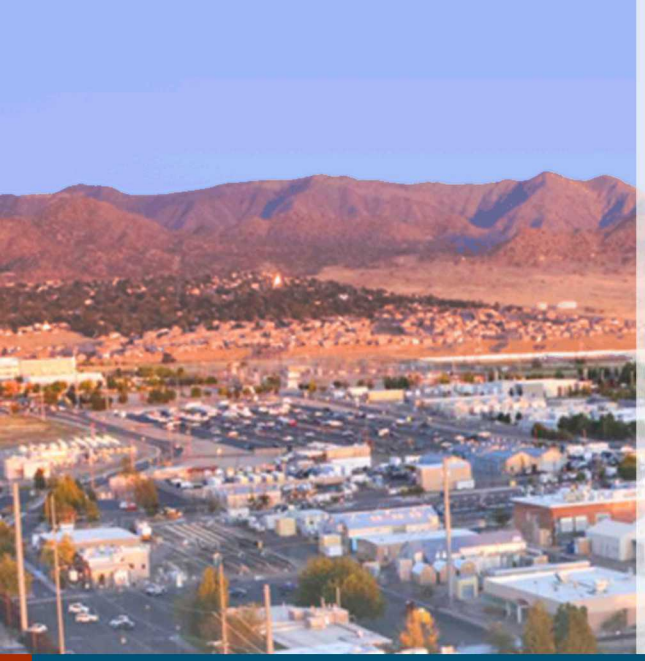
- New threats are introduced
  - Example: Red Hat instances in Azure in February, 2017
    - Exposed Admin API keys in config file
    - Allowed access to any VM within customer account

Attack surface is CSP's resources plus Customer's resources with Less Visibility



Summary of primary threats defined in cloud [per CSA]

- Data breaches
- Weak identity, credentials and access management
- Insecure APIs
- System and application vulnerabilities
- Account hijaking
- Malicious insiders
- Advanced Persistent Threats (APTs)
- Data loss
- Insufficient due diligence
- Abuse and nefarious use of cloud services
- Denial of service
- Shared technology issues



Lesson-learned and Best practices

Visibility in Cloud

Gain the visibility you need to stop threats before they impact the enterprise, improve your security posture, and reduce the risk profile of the customer's environment

Integrated visibility across various Cloud Service Models and on prem solutions are enabled by:

- Identity Management
- Logs

[find a diagram with data sources]

Obtain Visibility: Logs, logs, logs
Software-as-a-Service

Logs in SaaS:

- Example: Microsoft O365

Typical O365 Logs for user activity log, admin logs for different services

- SharePoint Online (user & admin activity)
- OneDrive for Business (user activity)
- Exchange Online (user activity)
- Azure Active Directory (admin activity)
- Sway (user & admin activity)

Obtain Visibility: Logs, logs, logs
Platform and Infrastructure as-a-Service

Logs in PaaS and IaaS should include:

- Account and admin access
- Changes to environment (e.g., group access, encryption enabled/disabled)
  - Changes to IAM
- Data access
- Access to networks and subnets
- Inbound and outbound traffic

Obtain Visibility: Logs, logs, logs
Network Flow

Can I monitor packet flow in the cloud? (applicable to IaaS)

- Forced routing and dedicated VMs to monitor traffic
  - Works for both North/South & East/West traffic
- Virtual appliance that monitor traffic in/out of cloud
  - North/South traffic
- Software-based tools from CSP
  - AWS VPC Flow Monitoring
  - Azure Network Security Groups (NSG) Flow Logs
  - Azure Network Watcher
- However, some traffic not logged
  - DHCP traffic
  - AWS EC2 instance connecting to AWS DNS server
  - Instance metadata traffic to/from specific IP address (i.e., 169.254.169.254)

Log Categories and Activities

The Audit log captures activities from multiple sources. The general sets of logged activities are grouped into the following categories:

- File and page
- Folder
- Sharing and access requests
- Synchronization
- Site administration
- Exchange mailbox
- Sway
- User administration
- Azure AD group administration
- Application administration
- Role administration
- Directory administration
- eDiscovery
- Power BI
- Microsoft Teams
- Yammer
- Exchange admin

More Visibility via Cloud Access Security Broker (CASB) platforms provide:

Inspect network traffic

Apply customer policies for controlling what data can be transferred

Apply protective controls to data per predefined policy

- Encryption

CASBs can identify cloud applications and data using:

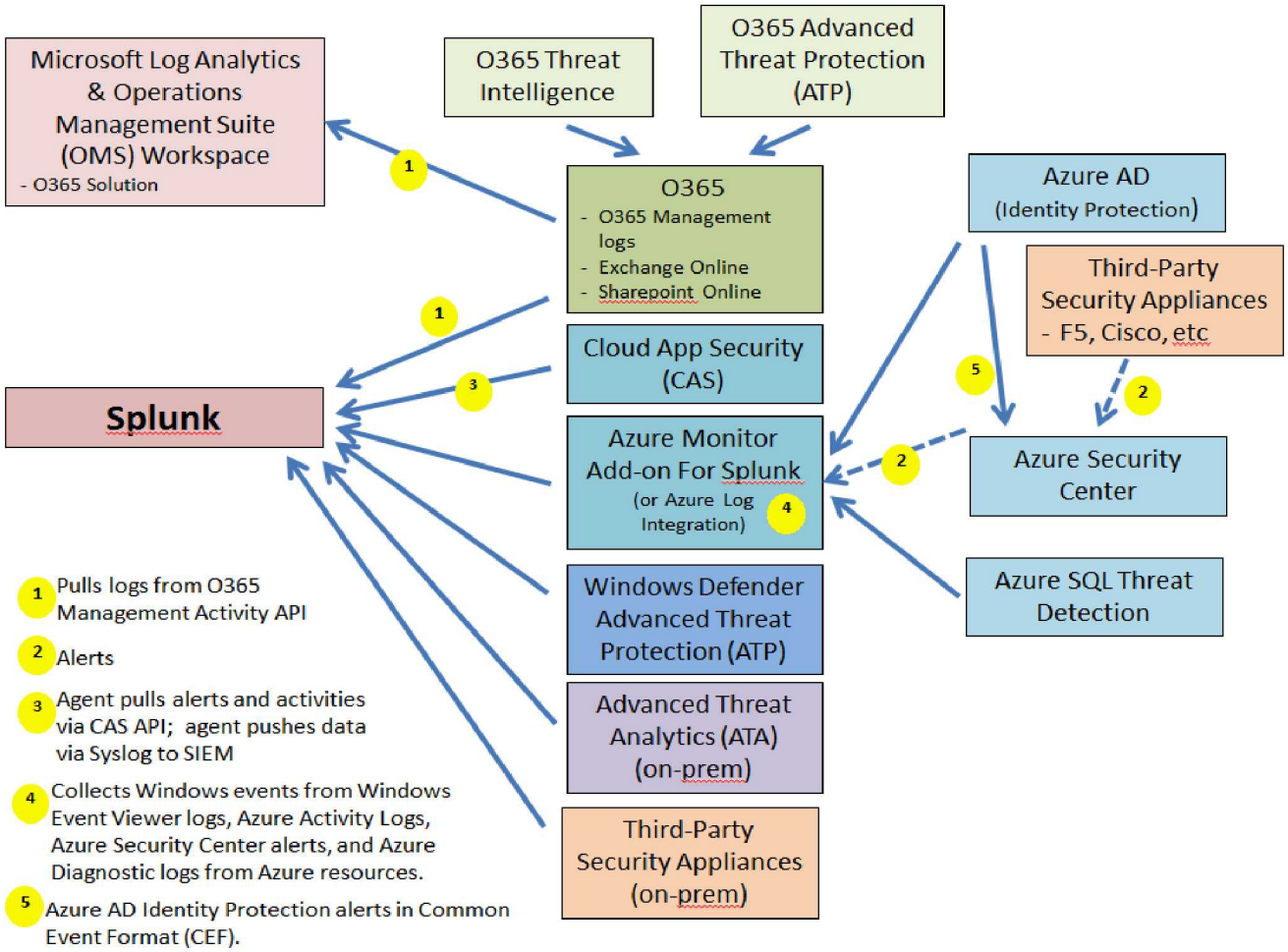
- Traffic analysis,
- Protocol analysis,
- URL inspection, and
- DLP pattern matching

Some security questions for SaaS:

- Who is accessing SaaS application?
- Where are they coming from?
  - See CASB support
- What are "normal" patterns of access and behavior?

Example: SIEM integration with Microsoft Azure and O365

Integration of SIEM (i.e., Splunk) with Microsoft and 3rd party security tools



Visibility at scale : Automation

With reduced control and visibility in cloud environments, we need to rely more on scripting and automation to deploy our tools and secure cloud assets.

- Native scripting toold
  - Azure – Powershell
  - AWS – AWS CLI
- Automation engines
  - AWS Lambda
  - AWS CloudWatch
  - Ansible
  - others

Analytics for the cloud

On going development:

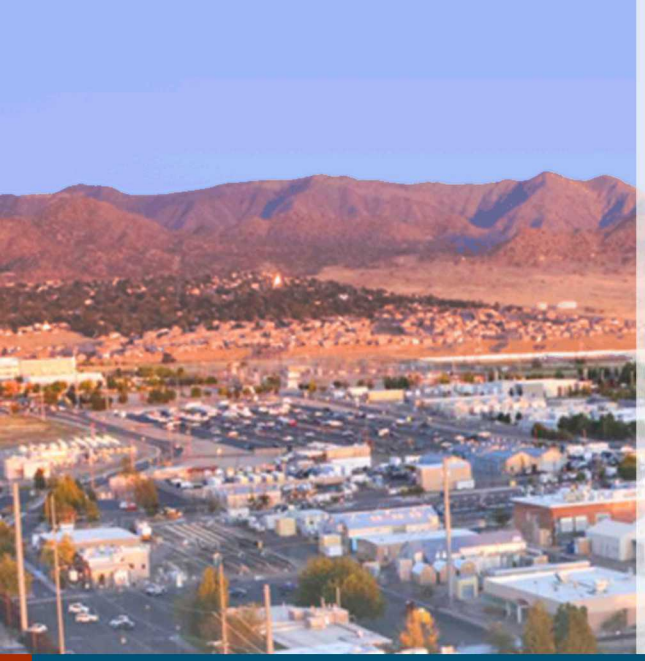
- Dashboards, reports, incident response workflows, advanced analytics, correlation searches and security indicators

- Combine on-premises and cloud deployments

- Analysis: correlation, reconstruction, time sync, logs, metadata, timelines.

- Analytics for the cloud require substantial development

- Hypothetically some example of advanced analytics include:
  - Impossible geographical authentication…
  - Data enrichment



Conclusions

Conclusions

- Logs are integral to success of security defender in Cloud
- Identity Management solutions must be re-evaluated when moving to cloud
  - Think of roles across multi-CSP solutions
  - Analytics will need significant development both IT and S/W dev, security workflow
    - Gap in the CSP provided data analytics

All achieve through integrated approach via Automation

IT

Security

S/W development

For additional Information:

Lin, Han Wei hwlin@sandia.gov

Han, Sil enhan@sandia.gov

Urias, Vincent E veuria@sandia.gov

Van Leeuwen, Brian P bpvanle@sandia.gov

William Stout, wmstout@sandia.gov

STOP, EOS

Preliminary Testing

Questions to ask before deploying

- Is logging done in real time? What is upper limit of logging delay?
- What happens when logging is cycled on/off numerous times? Are log file gaps noted? Are previous logs impacted?
- Interactions between logging and storage: CloudTrail supports S3 data events. If a change is made on S3 (e.g., modify ACL), does CloudTrail detect? Is it stored in an S3 bucket? Can I quickly (without loss of original ACL protection) reapply original ACL?
- How do regions impact logging?
- Configure CloudTrail logs to be encrypted. Create a policy file to modify keys for encryption but do not create decryption key. How can this be detected?
- CloudTrails are written to S3 buckets so logs can be redirected to another account; since S3 namespace is global can access global writeable buckets. Can I redirect and possibly hide logs? Can be effective in more restricted accounts.
- Use AWS Lambda to delete log files written to S3 bucket. What are the forensic artifacts produced by this? Can we detect?
- Can you retain control of instance if intruder attempts to lock you out?
- Methods exist to create temporary credentials. How can these be identified if they are created? Does CloudTrail create logs?
- Will log files identify attempts to maintain access persistence?

Considerations for Cloud-IR

Collect network flow data for any ingress/egress point.

Baked-in log collection agents that are lightweight and move data to the aggregation point as quickly as possible.

Collect cloud platform operations audit logs.

Have access to authorization data (who has what roles and what operations are allowed by those roles).

Have access to platform statistics across all tenants (for example):

- User list
- Tenant list
- Network list, bandwidth, utilization
- VM lists, uptime, CPU/disk/memory utilization
- Data high level description, level of sensitivity, utilization, ACLs, access logs, storage types, object store endpoints (and web logs for them)

Have a capability to snapshot data on demand (possibly an entire instance or tenant).

Aggregate the logs/data in central data analysis framework with approved data retention

Take Away: Design Principles for Cloud

Developing a visualization framework should be **multi-platform**: need to support at least all of Amazon AWS/EC2, Microsoft Azure, and Openstack...

Visibility into the full stack of dynamically created tenants, networks, gateways, virtual hosts, and containers.

Monitoring is important, but it should also support IT Operations – not crush it with monitoring, so: **Be as lightweight as possible**.

Monitoring capabilities should be **baked-in during provisioning** at all layers in the stack.

Monitoring data and log **aggregation should be built to scale dynamically**.

Forensic processes need to be rapidly and dynamically deployed with access to all networks and at all layers.

Automation is key to world-class cloud analysis, forensic capture, and response.

It's Raining Clouds…

Questions / Comments / Discussion

PRESENTED BY

Gio K. Kao, Ph.D.

Solutions for Cloud Breach*

- Visibility and control
- Unified cloud and on-premises security
- Context, system, and user awareness
- Detailed logging and reporting

How do we address these? Every deployment may differ, based on the service, users, data and CSP – but there are some attributes that may extend to all.

Trusted Internet Connection (TIC)

Guidance for Trusted Internet Connection (TIC) Readiness

- collaborating with a FedRAMP-certified cloud provider, an agency may be able to design a solution that meets TIC requirements while avoiding performance issues.

Cloud Security Challenges

1. Architecture: diversity, complexity, provenance, multitenancy, data segregation.
2. Data collection: data integrity, data recovery, data location, imaging.
3. Analysis: correlation, reconstruction, time sync, logs, metadata, timelines.
4. Incident first responders: trustworthiness of cloud providers, response time, reconstruction.
5. Role management: data owners, identity management, users, access control.
6. Legal: jurisdiction, laws, SLA, contracts, subpoenas, international cooperation, privacy, ethics.
7. Standards: operating procedures, interoperability, testing, validation.
8. Training: forensic investigators, cloud providers, qualification, certification