Cloud Security Today

Presenter: Jason Sheffield
Topics

◊ What are the issues today?
◊ What is the Cloud?
◊ How the Cloud is delivered: Iaas, PaaS and SaaS
◊ Cloud security challenges and risk
◊ Current Cloud security report
◊ Cloud security technology drivers
◊ Common use cases for Cloud security technologies
◊ What technologies exist to address risk?
Old IT Security Architecture From Yesterday
Old IT Security Architecture From Yesterday

- Web
- SaaS
- IaaS

Data Center

Apps

FW
SWG
VPN
IPS

Endpoints
With Digital Transformation … Everything Changed
With Digital Transformation … Data is Everywhere
DATA FLOWS LIKE WATER
LACK OF VISIBILITY
COMPLEXITY
CONTROLS CREATES FRICTION
What is the Cloud?

- Gartner defines the Cloud as a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies.

- **Public Cloud**: Computing, Networking, Server and Storage resources owned and operated by a third party Cloud Service Provider and delivered over the Internet. Public Cloud resources are shared with other organizations and separated into individual tenants.

- **Private Cloud**: Computing resources used exclusively by one business or organization. In the Private Cloud services and infrastructures are maintained by your organization. Private Clouds can be physically located in your organizations data center or can be hosted by a third party service provider.

- **Hybrid Cloud**: Hybrid Clouds are a mixture on-premise infrastructure, Private Clouds and Public Clouds.
What is the Cloud?
Who in the Organization is Buying and Why?

Who’s Buying?
- Security Executives
  - Why?
  - Risk Exposure
- Compliance Teams
  - Why?
  - Audit & Compliance
- Legal Teams
  - Why?
  - Data Governance
- Business Leaders
  - Why?
  - Secure Adoption
How is the Cloud delivered: Key differences between Iaas, PaaS and SaaS
Cloud Security Challenges and Risks

Exposure
Sensitive data shared publicly
Disrupt

Access
Download to personal device
Destroy

Theft
Exfiltration via unsanctioned cloud
Extort

DATA

INTERNAL RISK

EXTERNAL RISK
Malware upload to sanctioned cloud
Ransomware via cloud
Cloud account hijacking
On average the number of cloud services in use per enterprise, there was an increase to 1,246 from 1,181 last report.

Source: Netskope Cloud Security Report, October 2018
By category in the CIS benchmark for AWS, the majority of violations are in the Identity and Access Management category at 71.5 percent. Monitoring followed with 19.0 percent, Networking with 5.9 percent, and Logging with 3.6 percent. This may indicate that while many organizations have controls around cloud services and implemented things like multi-factor authentication (MFA) and single sign-on solutions, I/PaaS identity and access policies still need to be set.
THREE QUICK WINS FOR ENTERPRISE IT

1. Place DLP policies and security controls over activities like downloading sensitive information from IaaS solutions to secure increasing use of the public cloud.

2. Assess the security of your IaaS environment continuously against best practices so you can quickly identify and remediate risks and potential vulnerabilities.

3. Consider using the same security profiles, policies, and controls across SaaS, IaaS, and web services to reduce complexity.
Cloud Security Technology Drivers

• Professionals now work from multiple devices in multiple locations
• Instantaneous sharing and collaboration happens through numerous applications
• Firewalls cannot protect data stored throughout various cloud applications
• Traditional security tools cannot provide visibility in the cloud
• Non-enterprise cloud applications are consumed by end users without regard for their risk exposure
Common Use Cases for Cloud Security Technologies

- Safely Enable Cloud Apps
- Discover Shadow IT
- Unified Cloud Policies
- Detect Cloud Threats
- Continuous Security Assessments
- Prevent Data Exfiltration
What Technologies Exist to Address Risk?

CASB & Cloud Security Platform

Any User

Analytics

Policy

Data Protection

Any Device

Threat Protection

Any Location

SaaS

IaaS

Web

Any User

Any Device

Any Location
# Mapping of Cloud Security Controls

<table>
<thead>
<tr>
<th><strong>ON-PREMISES</strong></th>
<th><strong>AWS</strong></th>
<th><strong>AZURE</strong></th>
<th><strong>GOOGLE</strong></th>
<th><strong>ORACLE</strong></th>
<th><strong>IBM</strong></th>
<th><strong>ALIBABA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application Firewall (WAF)</td>
<td>AWS WAF</td>
<td>Application Gateway</td>
<td>Cloud Armor</td>
<td>Oracle Dyn WAF</td>
<td>Cloud Internet Services</td>
<td>Cloud Application Firewall</td>
</tr>
<tr>
<td>Antimalware</td>
<td>3rd Party Only</td>
<td>Azure Monitor</td>
<td>Stackdriver Logging</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged Access Management (PAM)</td>
<td>3rd Party Only</td>
<td>Azure AD Privileged Identity Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Loss Prevention (DLP)</td>
<td>Amazon GuardDuty</td>
<td>Information Protection (IP)</td>
<td>Cloud Data Loss Prevention API</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>Amazon Inspector</td>
<td>Azure Security Center</td>
<td>Cloud Security Scanner</td>
<td>Security Vulnerability Assessment Service</td>
<td>Cloud Security Advisor</td>
<td>Server Guard</td>
</tr>
<tr>
<td>Email Protection</td>
<td>3rd Party Only</td>
<td>Office Advanced Threat Protection</td>
<td>Various controls embedded in G-Suite</td>
<td>3rd Party Only</td>
<td>3rd Party Only</td>
<td>Server Load Balancer (SLB)</td>
</tr>
<tr>
<td>SSL Decryption</td>
<td>Elastic Load Balancer</td>
<td>Application Gateway</td>
<td>HTTPS Load Balancing</td>
<td>3rd Party Only</td>
<td>3rd Party Only</td>
<td>VRF Gateway</td>
</tr>
<tr>
<td>Revenue Privacy</td>
<td>VPC Customer Gateway</td>
<td>Virtual Network (VPC)</td>
<td>Dynamic Routing Gateway (CRG)</td>
<td>IPsec VPN Secure Gateway</td>
<td>Key Management Service</td>
<td>Object Storage Service</td>
</tr>
<tr>
<td>VPN</td>
<td>AWS Transit Gateway</td>
<td>Key Vault</td>
<td>Google VPC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Management</td>
<td>Key Management Service (KMS)</td>
<td>Cloud Key Management Service</td>
<td>Cloud Infrastructure Key Management</td>
<td>Cloud Infrastructure Block Volume</td>
<td>Key Protect Cloud Security</td>
<td></td>
</tr>
<tr>
<td>Encryption At Rest</td>
<td>Elastic Block Storage</td>
<td>Storage Encryption for Data at Rest</td>
<td>Part of Google Cloud Platform</td>
<td>Cloud Infrastructure Block Volume</td>
<td>Hyper Protect Crypto Services</td>
<td></td>
</tr>
</tbody>
</table>

*Note: The table above highlights the mapping of cloud security controls across various cloud providers, focusing on key security features and services.*
### Mapping of Cloud Security Controls cont.

<table>
<thead>
<tr>
<th>Cloud Security Control</th>
<th>AWS Shield</th>
<th>Built-in DDoS defense</th>
<th>CloudArmor</th>
<th>Built-in DDoS defense</th>
<th>Cloud Internet Services</th>
<th>Anti-DDoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Logging / Auditing</td>
<td>Elastic Load Balancer / CloudFront</td>
<td>Azure Load Balancer</td>
<td>VPC Flow Logs Access Transparency</td>
<td>Oracle Cloud Infrastructure IAM</td>
<td>Log Analysis with LogDNA</td>
<td>Log Service</td>
</tr>
<tr>
<td>WAN</td>
<td>Direct Connect</td>
<td>ExpressRoute / MPLS</td>
<td>Virtual Private Cloud Network (VPC)</td>
<td>Virtual Cloud Network (VCN)</td>
<td>VLANs</td>
<td>Virtual Private Cloud (VPC)</td>
</tr>
<tr>
<td>Endpoint Protection</td>
<td>3rd Party Only</td>
<td>Microsoft Defender ATP</td>
<td>Dedicated Interconnect</td>
<td>FastConnect</td>
<td>Direct Link</td>
<td>VPN Gateway Express Connect</td>
</tr>
<tr>
<td>Container Security</td>
<td>Amazon ECS Container Service (ECS)</td>
<td>Azure Container Service (ACS)</td>
<td>Kubernetes Engine</td>
<td>Oracle Container Services</td>
<td>Container - Trusted Compute</td>
<td>Container Registry</td>
</tr>
<tr>
<td>Governance Risk and Compliance Monitoring</td>
<td>AWS CloudTrail, AWS Compliance Center</td>
<td>Azure Policy</td>
<td>Cloud Security Command Center</td>
<td>Oracle Container Services</td>
<td>ActionTrail</td>
<td>ActionTrail</td>
</tr>
<tr>
<td>Backup and Recovery</td>
<td>AWS Backup, Amazon S3 Glacier</td>
<td>Azure Backup</td>
<td>Object Versioning Cloud Storage Nearline</td>
<td>IBM Cloud Backup</td>
<td>Hybrid Backup Recovery</td>
<td>Hybrid Backup Recovery</td>
</tr>
</tbody>
</table>

Source: Peerlyst Post – Adrian Grigorof, Marius Micanu, February 2019
What Technologies Exist to Address Risk

Technical capabilities needed to address today's risk

- Data Loss Prevention
- Encryption
- Adaptive Access Control
- Visibility into Cloud Application Use
- Continuous Security Assessment
- Anomaly Detection
- Threat Protection
- Web Security
Questions?
Appendix

• Netskope Cloud Report:
  https://resources.netskope.com/cloud-reports/netskope-cloud-report-october-2018
Thank You!