

CLOUD WORKFLOWS: ACHIEVING STUDIO-GRADE SECURITY

Ted Harrington

 @SecurityTed

 ted.harrington@securityevaluators.com

Eli Mezei

 @ISESecurity

 emezei@securityevaluators.com



independent security evaluators

know thy enemy

we do.



independent security evaluators

www.securityevaluators.com

Agenda

1) Context

2) Security Models

3) Applying Principles



independent security evaluators

Agenda

1) Context

2) Security Models

3) Applying Principles



independent security evaluators

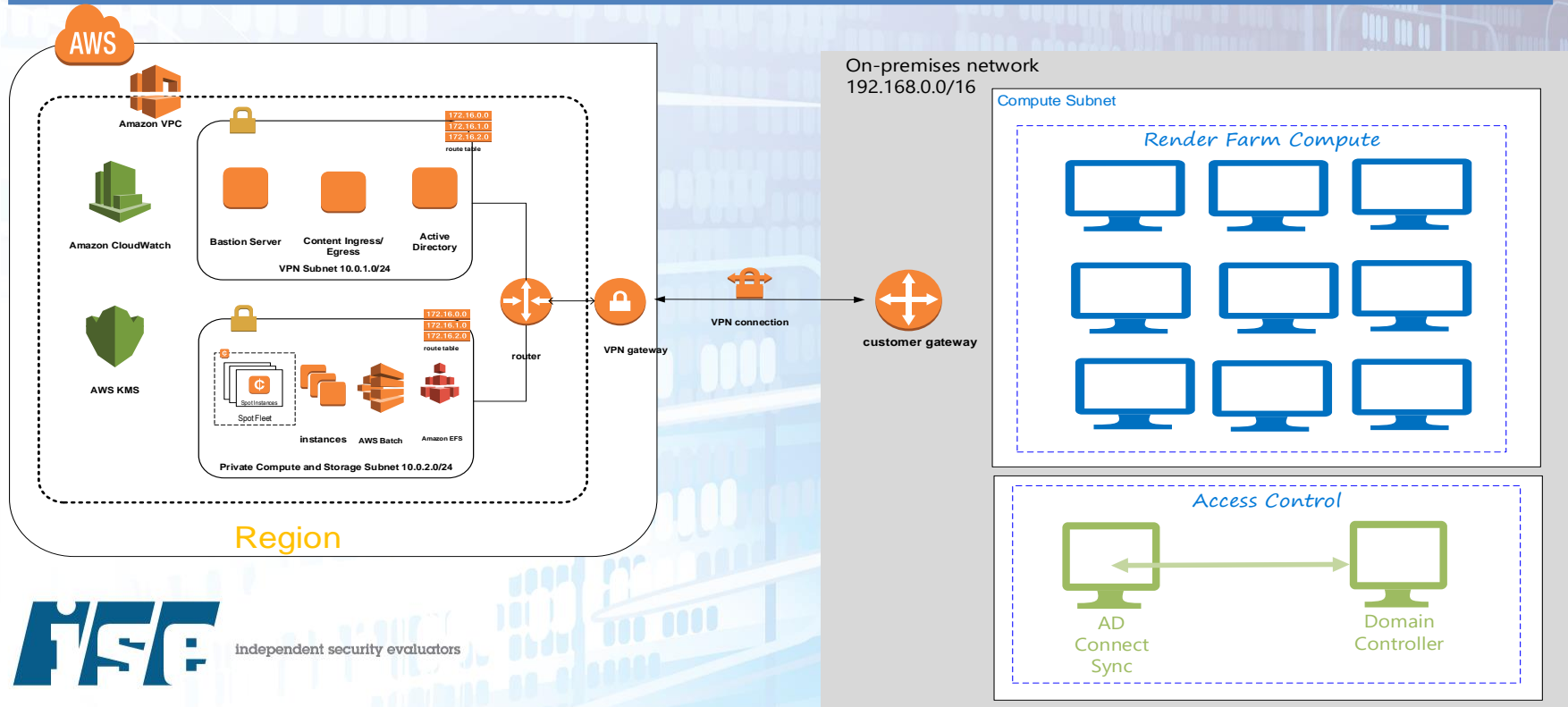
WORKFLOWS DRIVE SECURITY!

- Security must support the workflow, not the other way around
- The workflow must be understood in depth before security controls can be defined
- The simplest solution is generally the most secure



independent security evaluators

Example Workflow: Burst Rendering



independent security evaluators

Agenda

1) Context

2) **Security Models**

3) Applying Principles



independent security evaluators

TRUST MODEL VS. THREAT MODEL



independent security evaluators

KNOW YOUR ADVERSARY



independent security evaluators

SECURE DESIGN PRINCIPLES



independent security evaluators

Secure Design Principles

Principle: universally accepted truth

Secure Design Principle: those upon which systems resilient against attack are built



independent security evaluators

Agenda

1) Context

2) Security Models

3) Applying Principles



independent security evaluators

PRINCIPLE(S): LEAST PRIVILEGE & PRIVILEGE SEPARATION

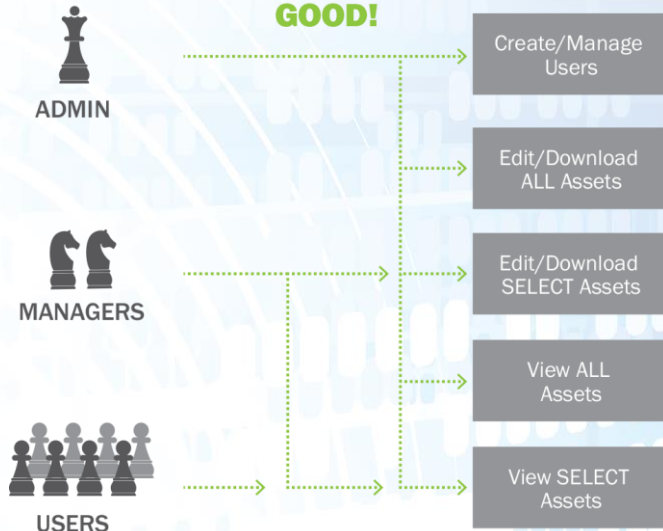


independent security evaluators

Privilege










LEAST PRIVILEGE

PRIVILEGE SEPARATION

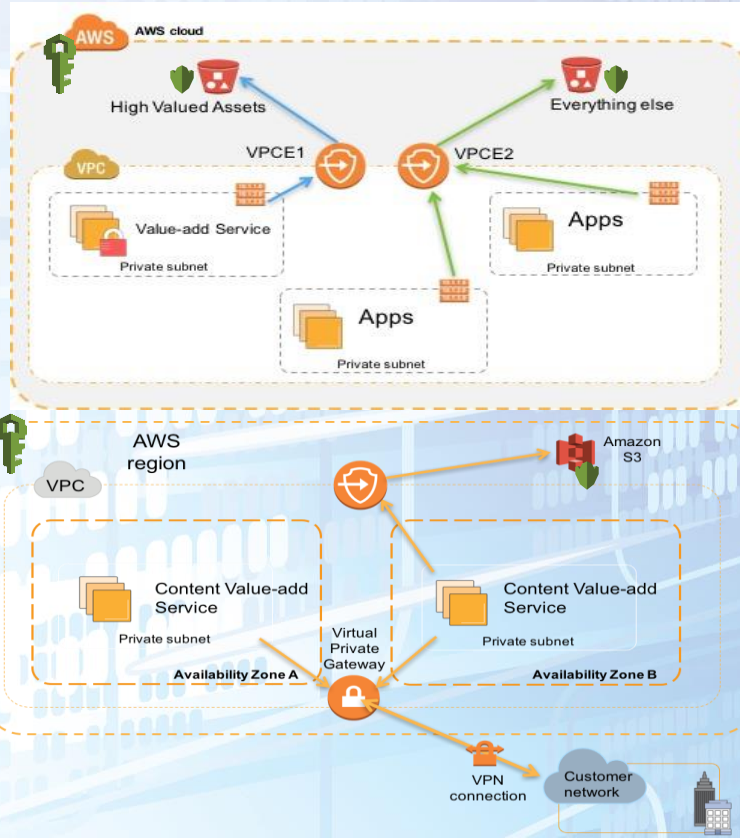


independent security evaluators

Privilege Control

Governance/Control	Identity Management	Key Mgmt/Custody	Networking
AWS	 IAM	 KMS	 VPC
Azure	 Azure AD	 Key Vault	 VPN Gateway
GCP	 IAM	 KMS	 Organizations

Example Implementation



independent security evaluators

PRINCIPAL: DEFENSE IN DEPTH









independent security evaluators

Defense in Depth

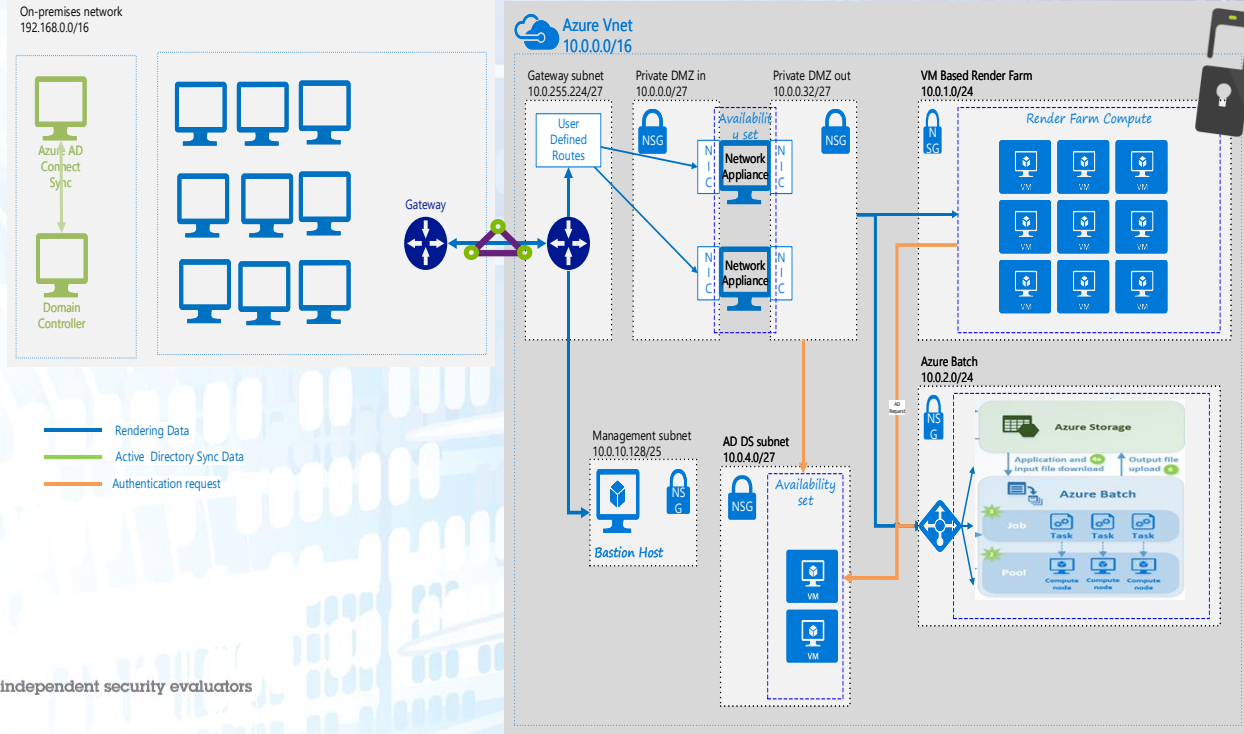


independent security evaluators

Defense in Depth

Governance/Control	Direct Connect	Account Segregation	MFA
AWS	 DirectConnect	 AWS Organizations	Multi-factor Auth.
Azure	 ExpressRoute	Azure Subscription and Service Management + Azure RBAC	 Multi-factor Auth.
GCP	 DirectConnect		 Google Authenticator

Example Implementation



independent security evaluators

PRINCIPLE: TRUST RELUCTANCE (ASSUME HOSTILITY)



independent security evaluators







Trust Reluctance



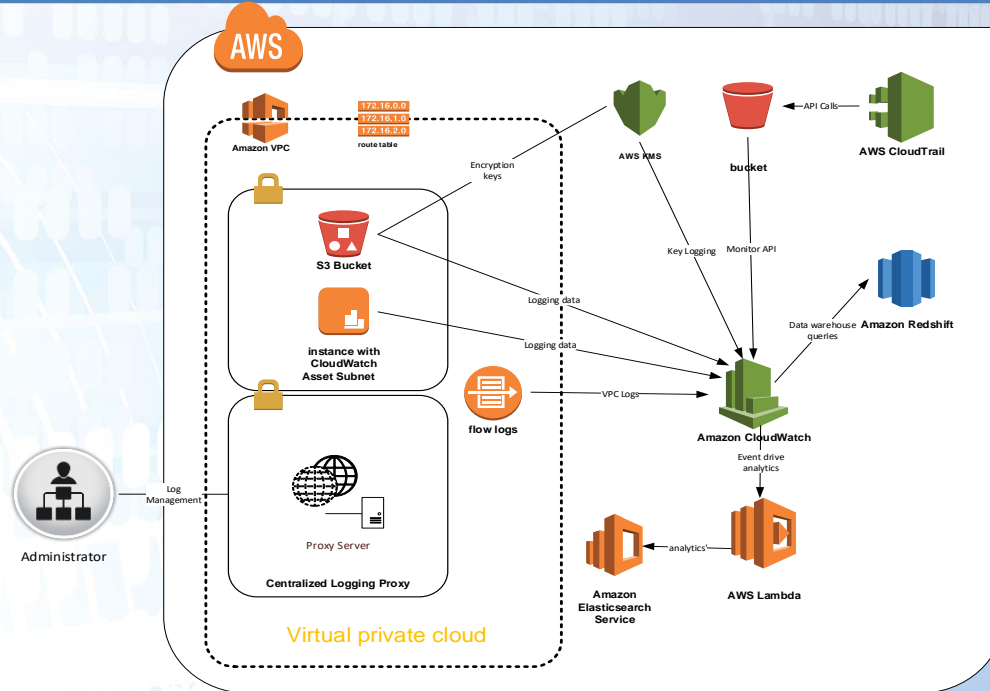
independent security evaluators

ISE Confidential - not for distribution

Logging and Monitoring Services and Intelligence

Governance/Control	Log Aggregation & Monitoring	Policy Center
AWS	 CloudTrail	 Inspector
Azure	 Log Analytics	 Security Center
GCP	 Cloud Audit Log	 StackDriver

Example Implementation



independent security evaluators

Secure Design Principles

- **Defense in Depth**
- **Least Privilege**
- **Privilege Separation**
- **Trust Reluctance**
- **Open Design**
- **Economy of Mechanism**
- **Complete Mediation**
- **Least Common Mechanism**
- **Psychological Acceptability**
- **Fail Secure**



independent security evaluators

Takeaways

- Security must support the workflow
- Build security in
- **Think like an attacker!**





@SecurityTed



ted.harrington@securityevaluators.com



@ISESecurity



emezei@securityevaluators.com