RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Cloud Trust. Redefined:
8 Essential Steps in a Strong Defense

SESSION ID: CDS-T09

Davi Ottenheimer

Senior Director of Trust
EMC Corporation
@daviottenheimer

Cloud Trust. Redefined

Transparency

Relevance

Resilience

Cloud Breach Example Types

1. **Iceberg**
   - CardSystems
   - Sony

2. **Evil Maid**
   - Google
   - Shionogi
   - City of SF

3. **SLA-urprise**
   - Salesforce
   - Amazon
   - Google

4. **Barn Door**
   - LinkedIn
   - Groupon

Lessons Learned

1. Remove (Regulated) Data
   - World
   - Large
   - Named
2. Define Boundary
   - Services, Ports, Listeners, Interfaces
   - Privileges, Processes and Patterns
3. Secure Identities for Access
4. Monitor Change, “Breaches” and Human Behavior
5. Protect Data

Essential Steps

1. Reduce Target Area
2. Manage I and M
3. Monitor and Alert
4. Maintain Availability

5. Orchestrate (Automate)
6. Test Security
7. Respond to Incidents
8. Backup and Restore (Exit)

1. Reduce Target Area

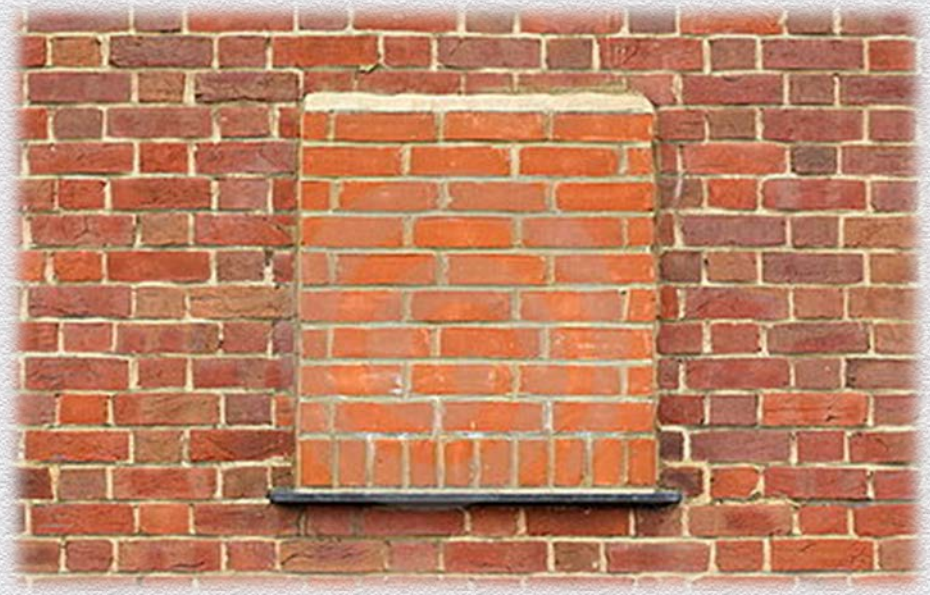
- Hardened Images
- Only Install From Trusted Sources
- Check Package Signatures
- Multi-Factor Authentication for Management

  (APIs with Multi-Factor Can be Tricky)

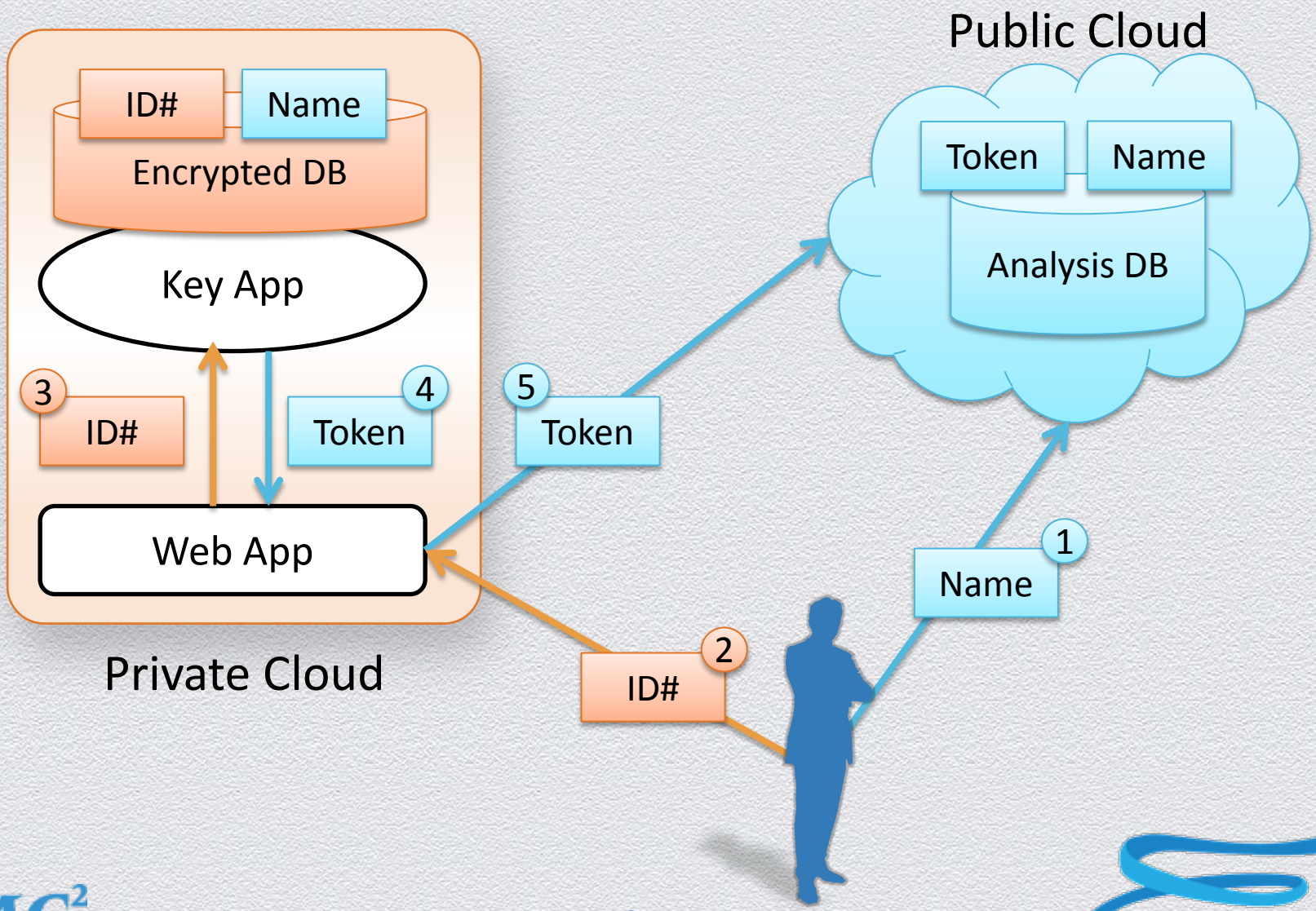
1. Reduce Target Area

- Make Risk Manageable
- Trends in Flaw Research
  - KVM (qemu/PIIX exploit by Nelson Elhage)
  - Cloudburst video driver hack on VMware variants
  - Xen hack via virtual video framebuffer

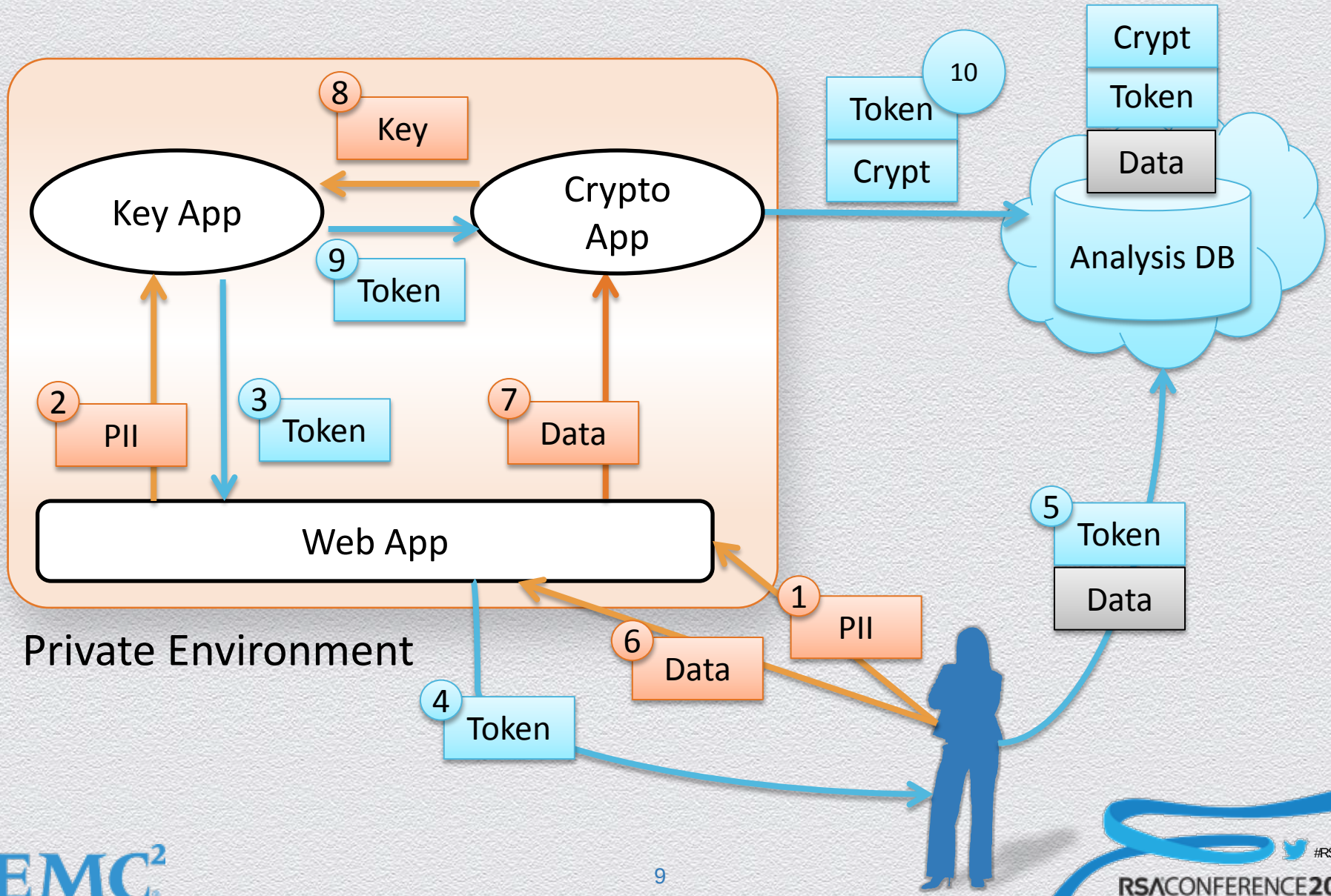
…All Virtualized ***Devices***



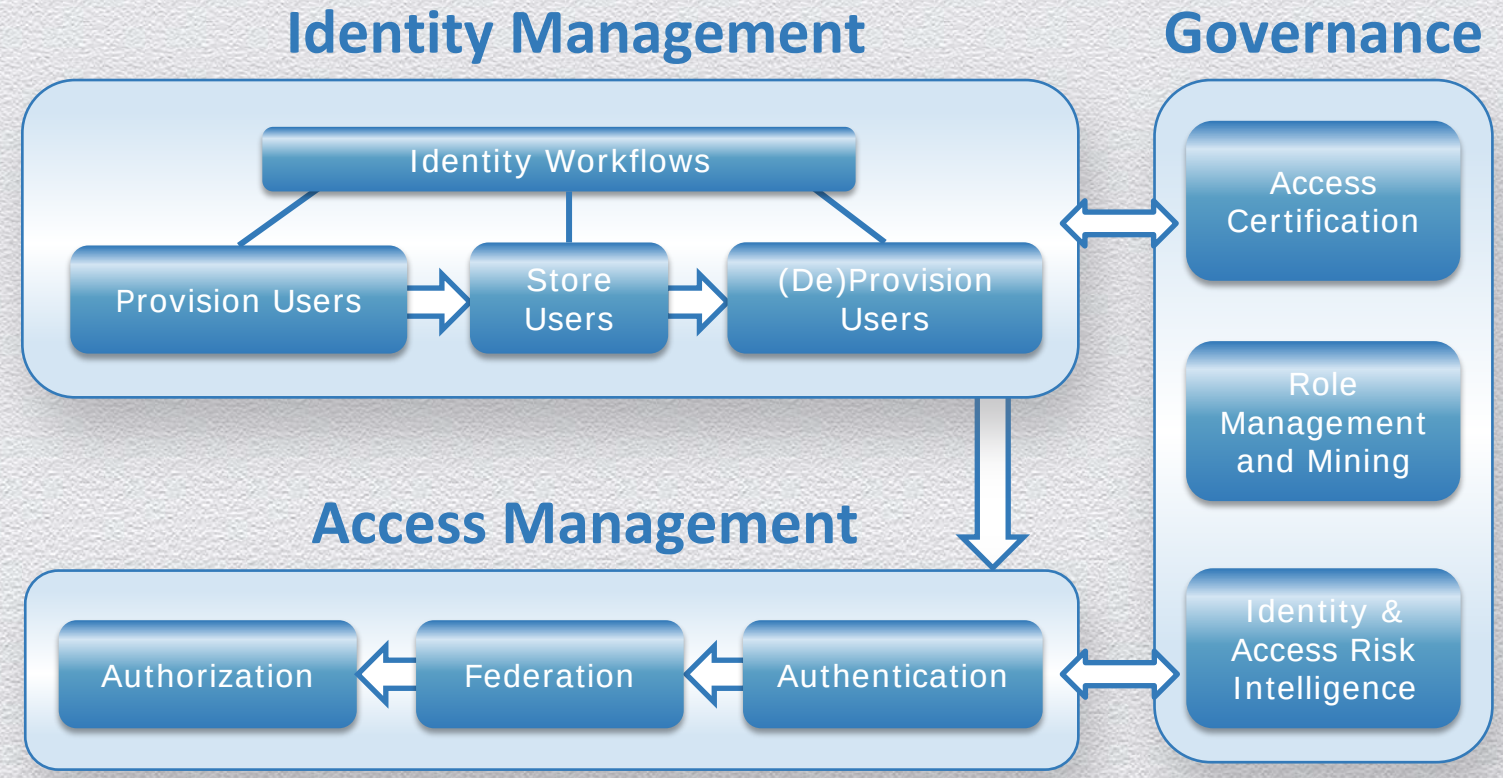
1. Reduce Target Area - Tokenize



1. Reduce Target Area - Encrypt



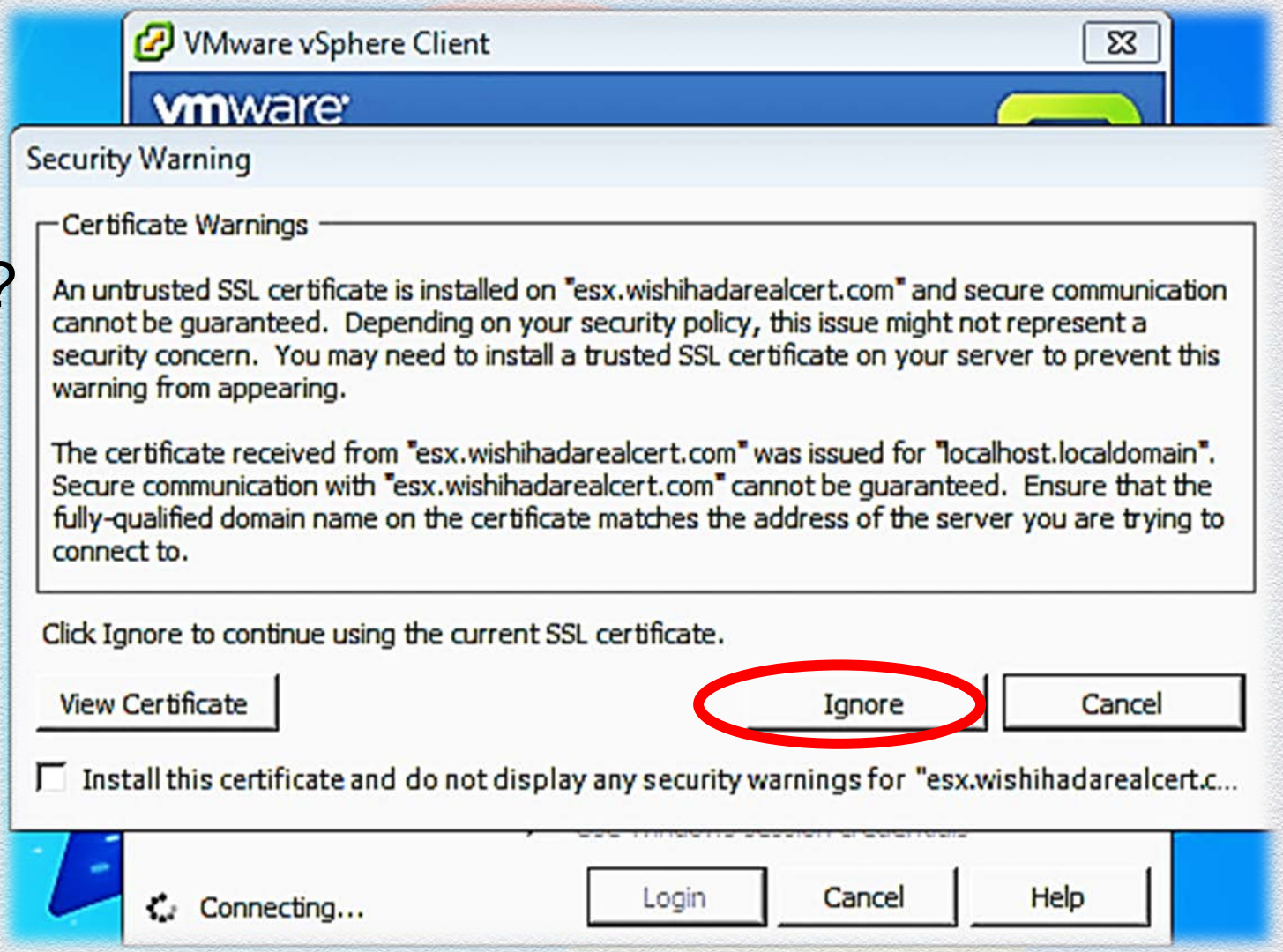
2. Manage Identity and Access (IAM)



- Do Not Use Shared Accounts
- Use Groups (Roles) to Grant Permissions
- Require Multi-Factor With Strong Passwords

2. IAM

Do You Ignore Warnings?



Do You Classify Data?

Have Choke Points?

Manager

Bridge or Proxy

Directory Service

Fat

CLI

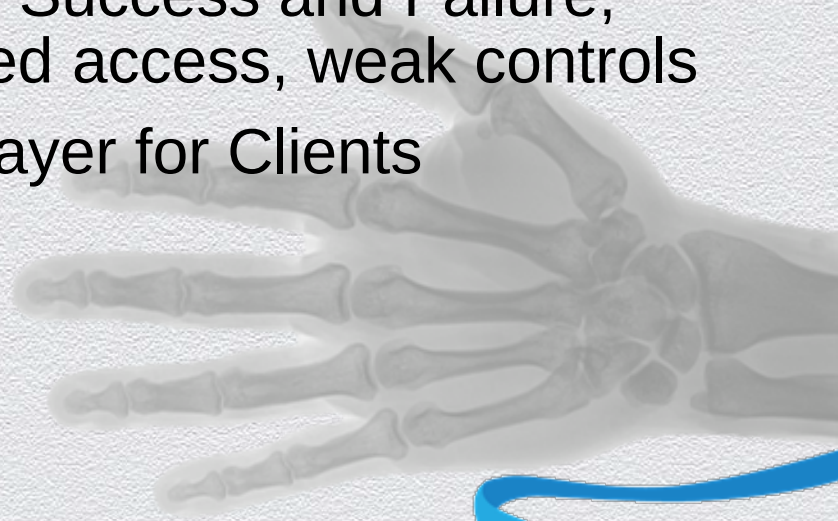
Web

API

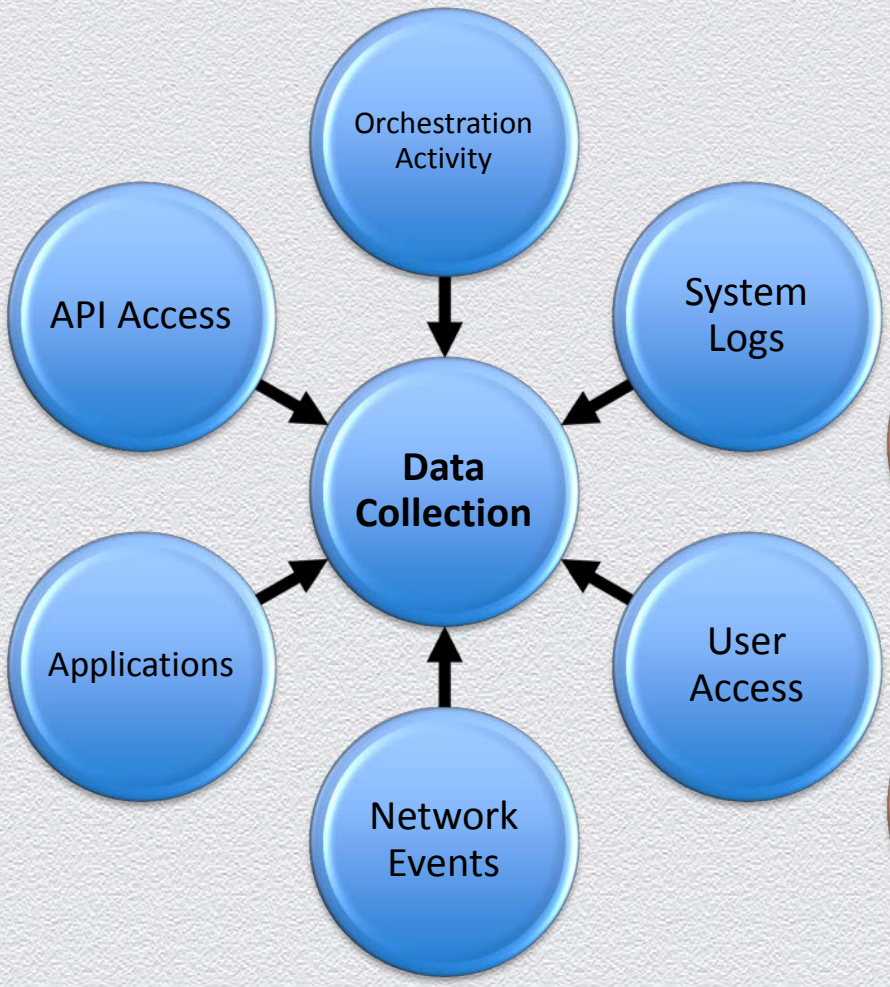
Administrative Interfaces

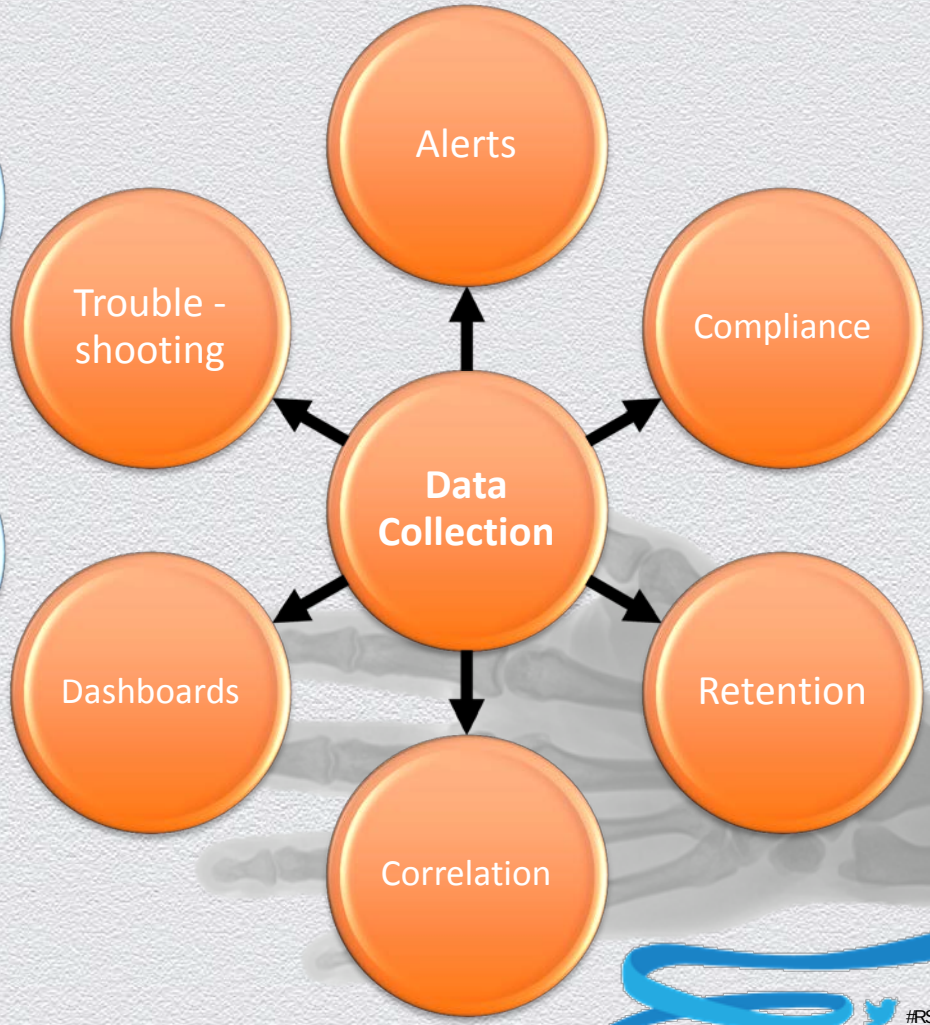
3. Monitor and Alert

- Read-Only Users/Roles
- Log as Much as Possible (Don’t DoS Yourself)
- Consider WORM
- Log Shells (especially ESXi when shell logins enabled)
- Consider sshd ForceCommand in Unix (stop unauthorized tunnels and stop unlogged commands)
- Log All Firewall and VPN Traffic, Success and Failure; Typical end-user VPN = privileged access, weak controls
- Virtualization Log = Protection Layer for Clients



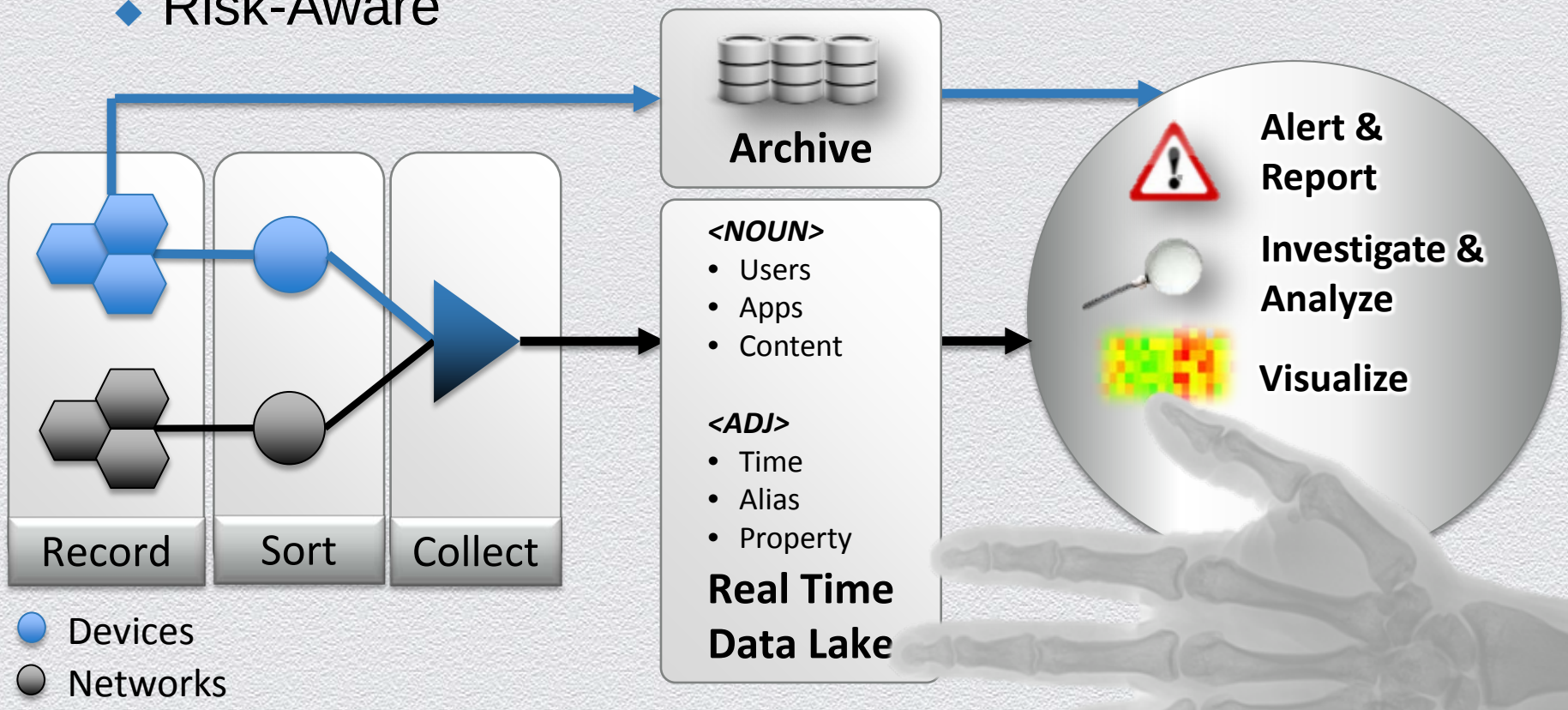
3. Monitor and Alert



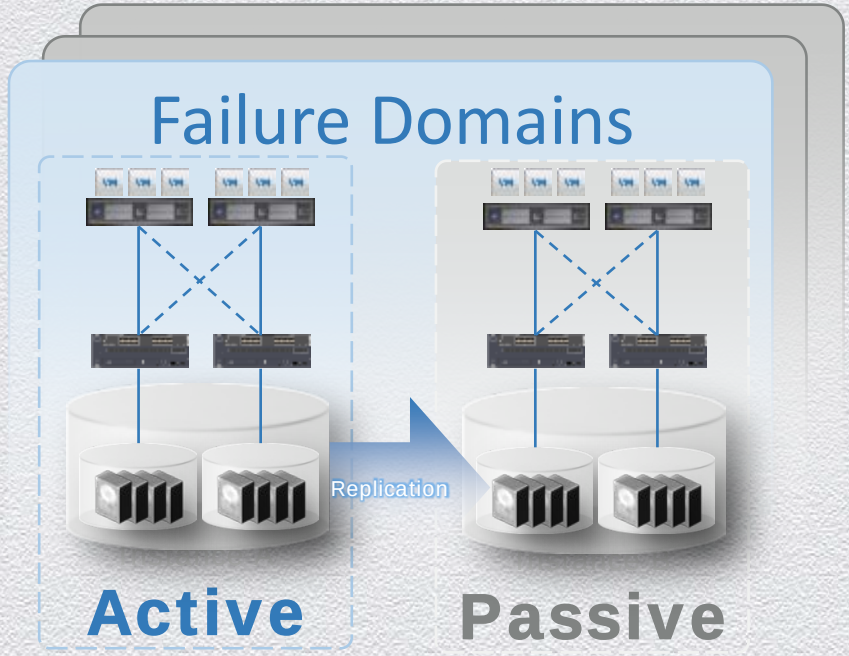


3. Monitor and Alert

- Intelligence-Driven
- Risk-Aware

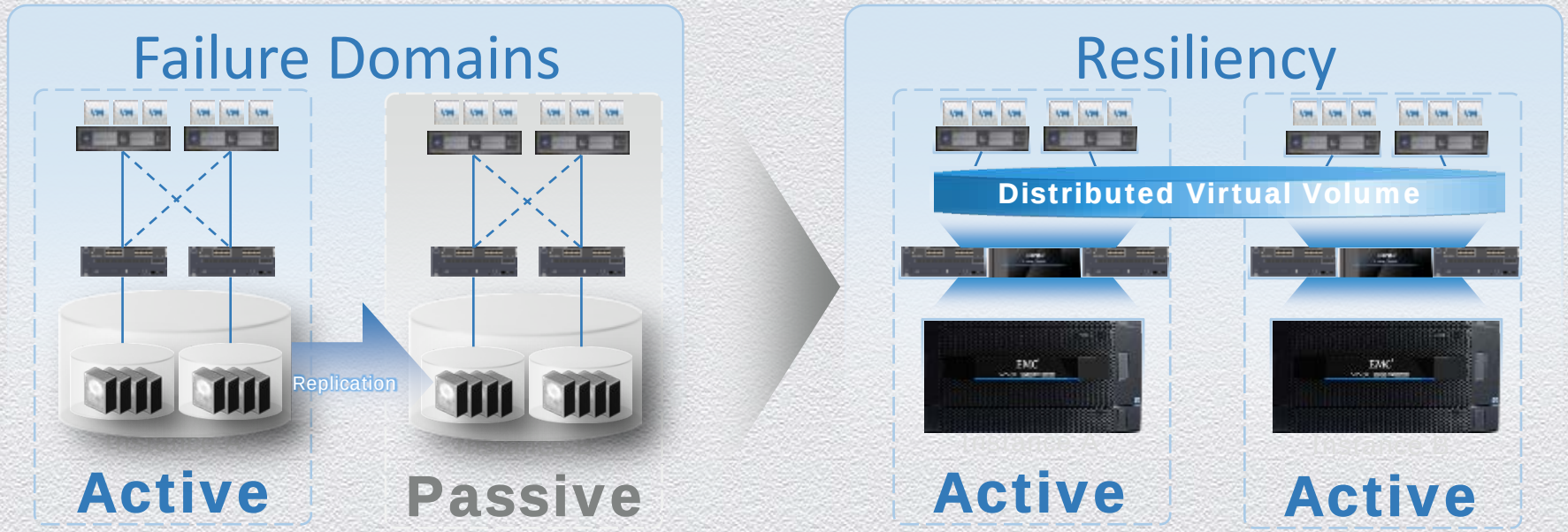


4. Maintain Availability



- Application Disruption
  - Planned
  - Unplanned
- RTO: Minutes-to-Hours
- Failover and Fail-back
- Passive, Idle Resources

4. Maintain Availability

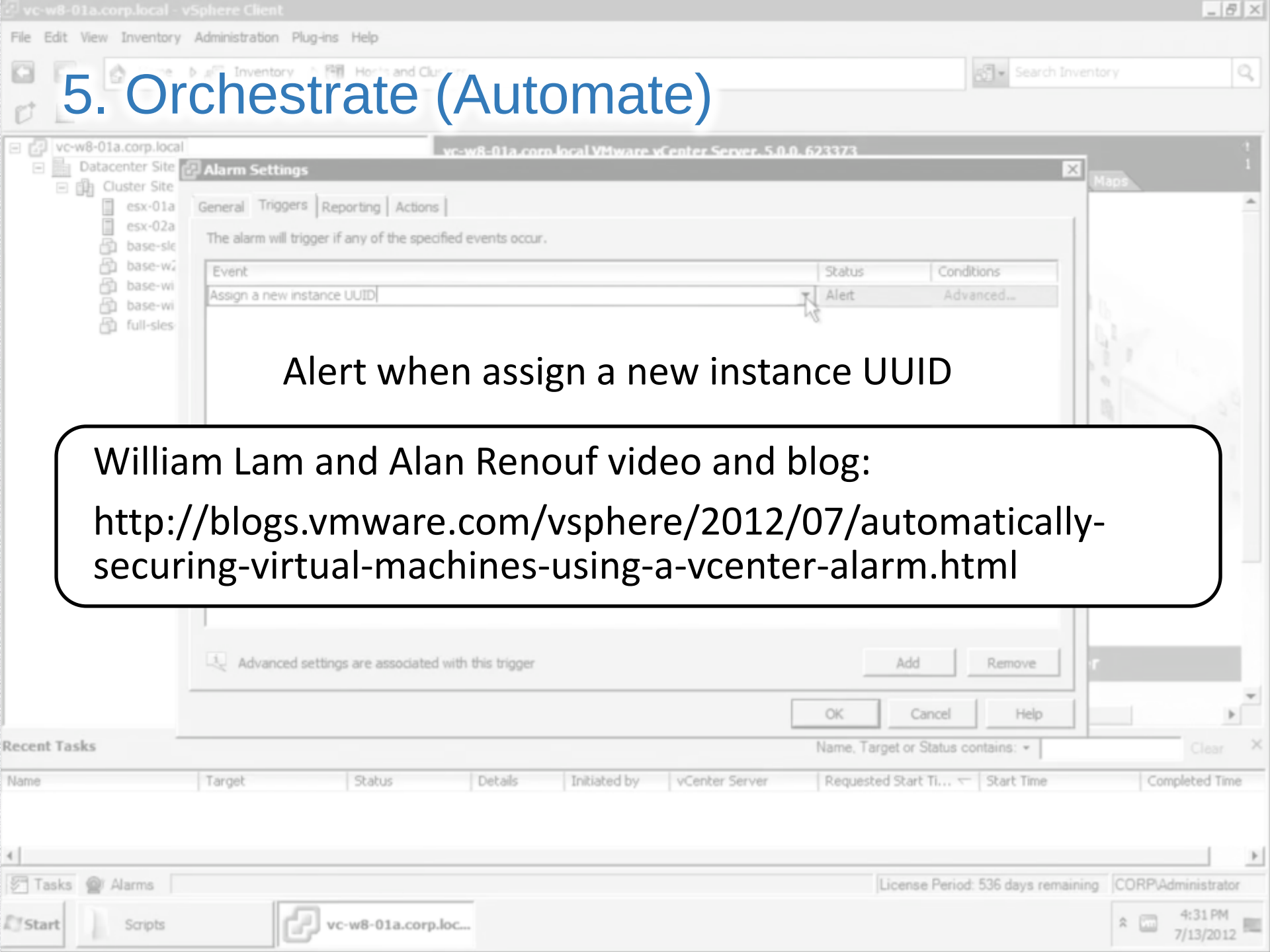


- No Disruption
- Zero RTO
- No Idle Resources

5. Orchestrate (Automate)

- Securing clouds can be hard work
- Orchestration tools should make things easier
  - Need credentials for magic
  - Adds complexity and more attack surface
  - Either reduces cost and human errors or magnifies them
- Common interface
  - Force checks
  - Verify configuration
  - Automate hardening

5. Orchestrate (Automate)



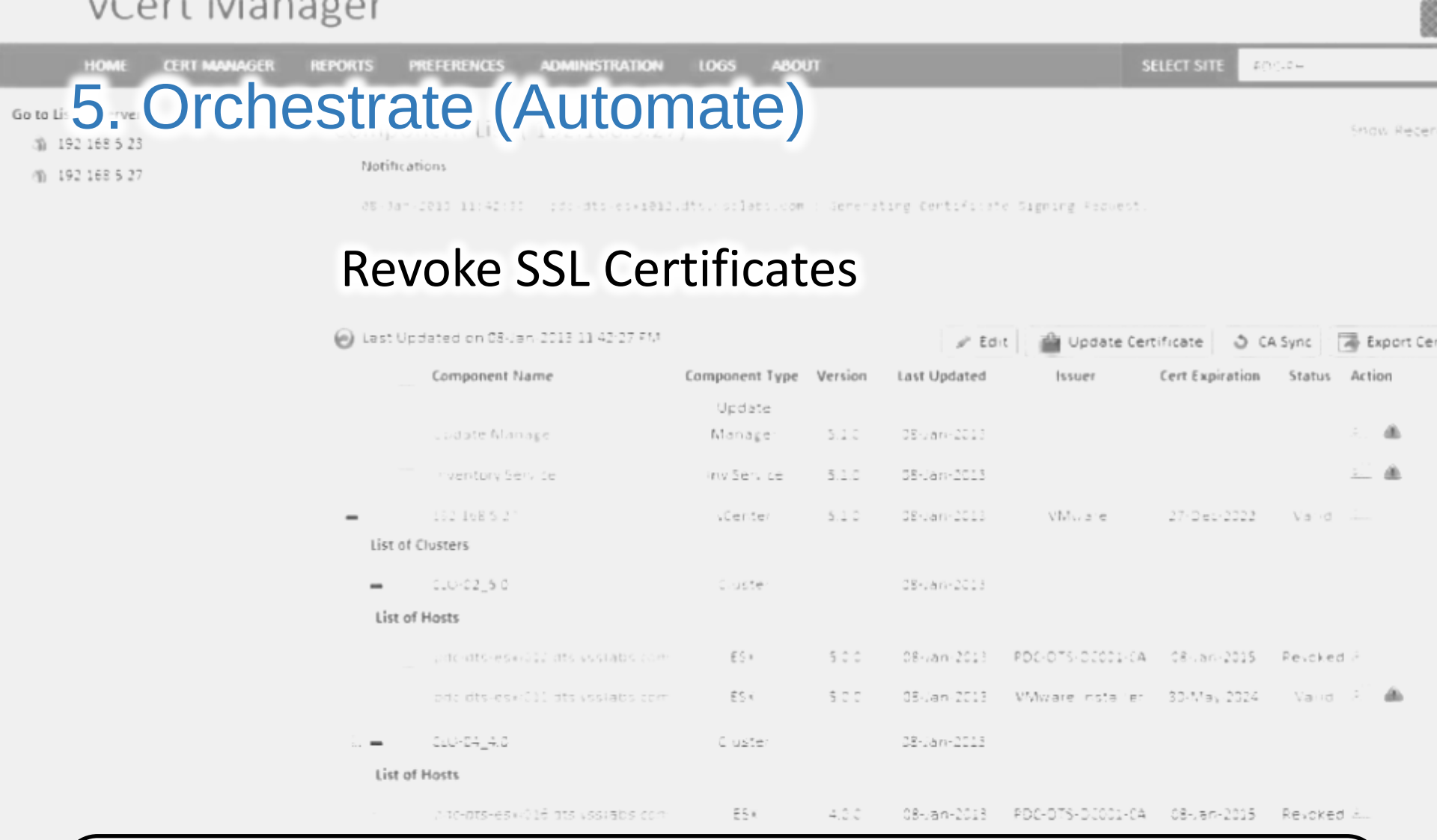
Alert when assign a new instance UUID

William Lam and Alan Renouf video and blog:

http://blogs.vmware.com/vsphere/2012/07/automatically-securing-virtual-machines-using-a-vcenter-alarm.html

5. Orchestrate (Automate)

Revoke SSL Certificates



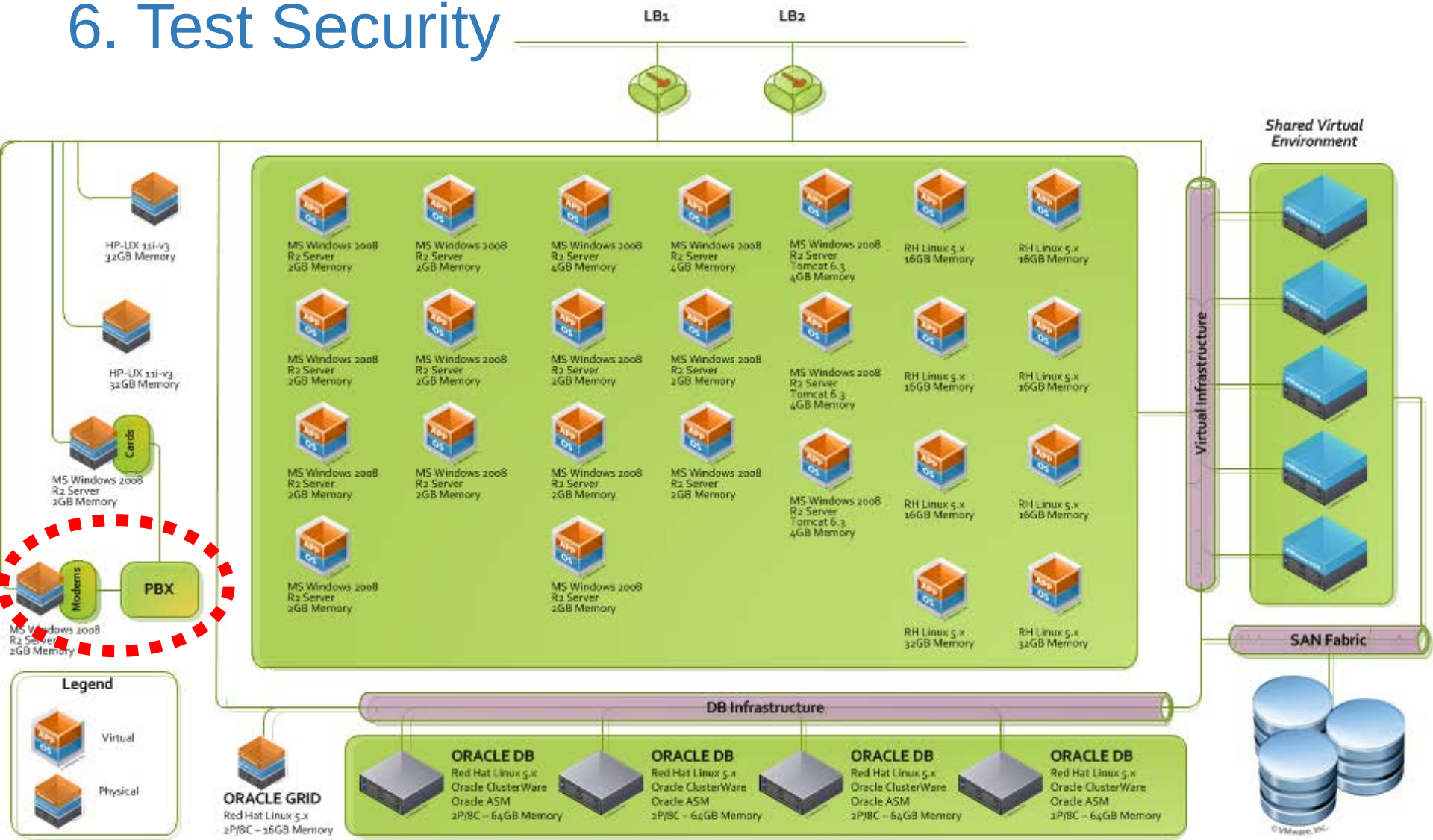
Michael Webster video and blog:

http://longwhiteclouds.com/2013/01/31/automating-vsphere-ssl-cert-management-vcert-manager-beta-demo/

6. Test Security

- Vulnerability
  - “Shouldn’t” Have Access (e.g. need CHAP secret)
  - Port-scan Yourself
  - Discovery and Inventory of Gaps
- Penetration
  - Business-Logic Assessment
  - Virtualization OPSEC (Load “tenants” and try being promiscuous)
    - Use some inside knowledge
    - Mount iSCSI targets or NFS shares
  - Application Architecture

6. Test Security



6. Test Security

- Virtualization OPSEC
  - .vxmf – teaming configuration (workstation groups)
  - .vmx – machine configurations
  - .vmsd – snapshot descriptor
  - .vmdk – disk geometry, layout, structure
  - .vmem – backup paging file
  - .vswp – swap file
  - .vmss – suspended state
  - .vmsn – snapshot of running machine state
- Suspend (Memory on Physical Disk)
  - .vmss created
  - .vswp removed

https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest

6. Test Security

- Collaborative/(C)overt
  - Credentials
  - Get-out-of-jail Card
- Debriefed or Blind
- Start the "Stopped"
- App *Includes* Data
- Exploitation = ?
  - **S** poof
  - **T** amper
  - **R** epudiate
  - **I** nformation Disclose
  - **D** *eny Service*
  - **E** levate Privileges

WARNINGS

…prevent potential adverse performance impacts on the resources you may be sharing with other customers

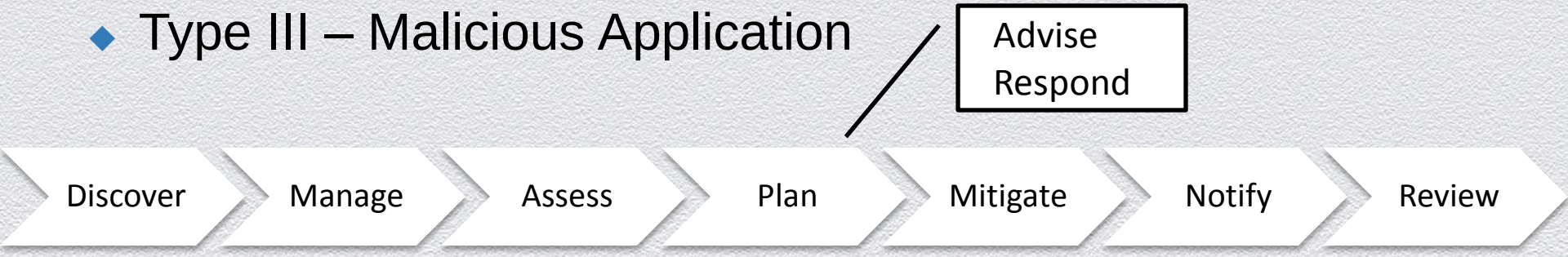
You are NOT limited in your selection of tools or services to perform a security assessment… …you ARE prohibited from utilizing any tools or services in a manner that perform Denial-of-Service (DoS) attacks or simulations of such against ANY…asset, yours or otherwise.

Prohibited activities include, but may not be limited to:

- Protocol flooding (eg. SYN flooding, ICMP flooding, UDP flooding)
- Resource request flooding (eg. HTTP request flooding, Login request flooding, API request) flooding

7. Respond to Incidents

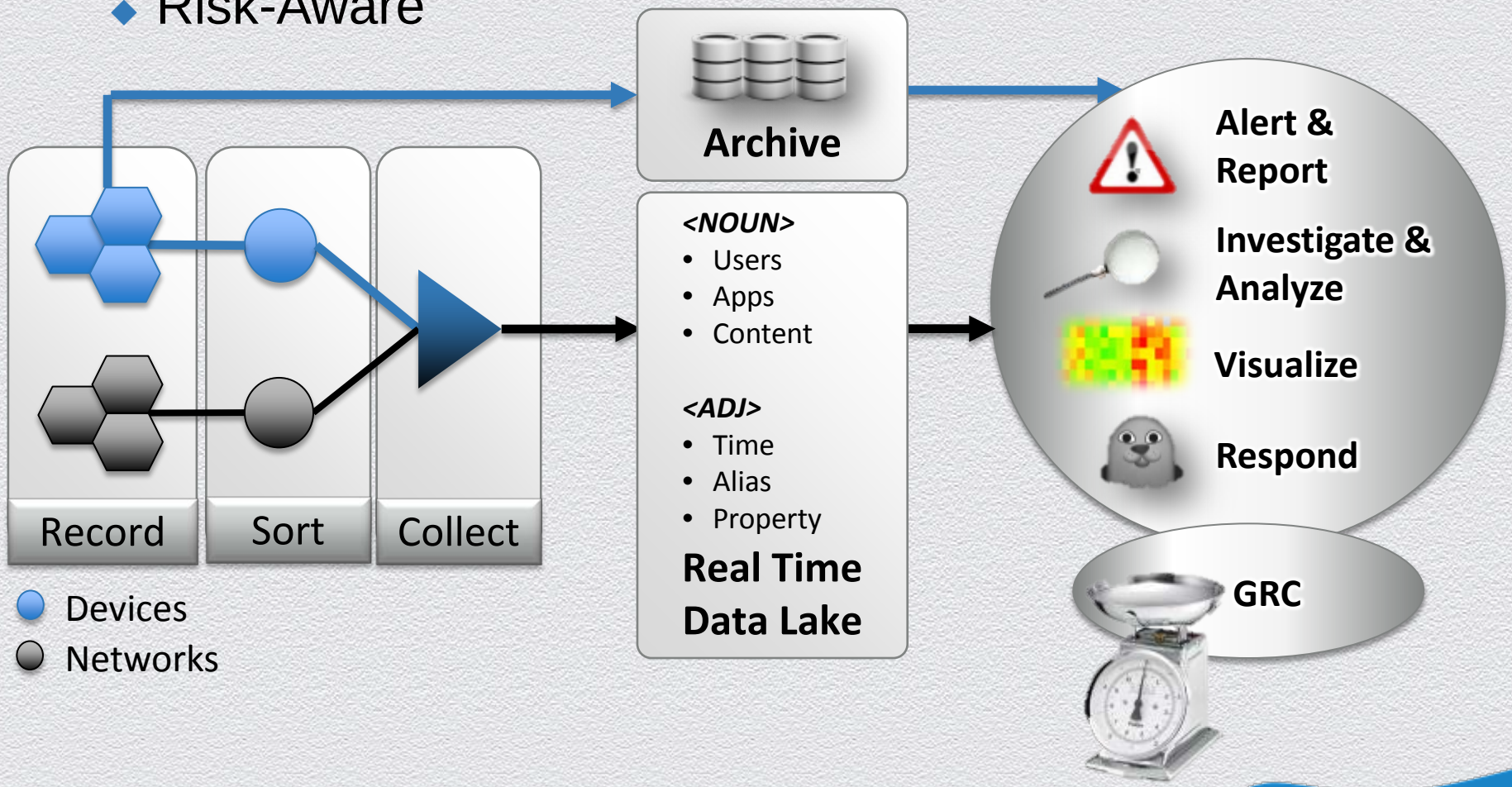
- Type I – Applications or Platform Targeted
- Type II – Infrastructure Targeted
- Type III – Malicious Application



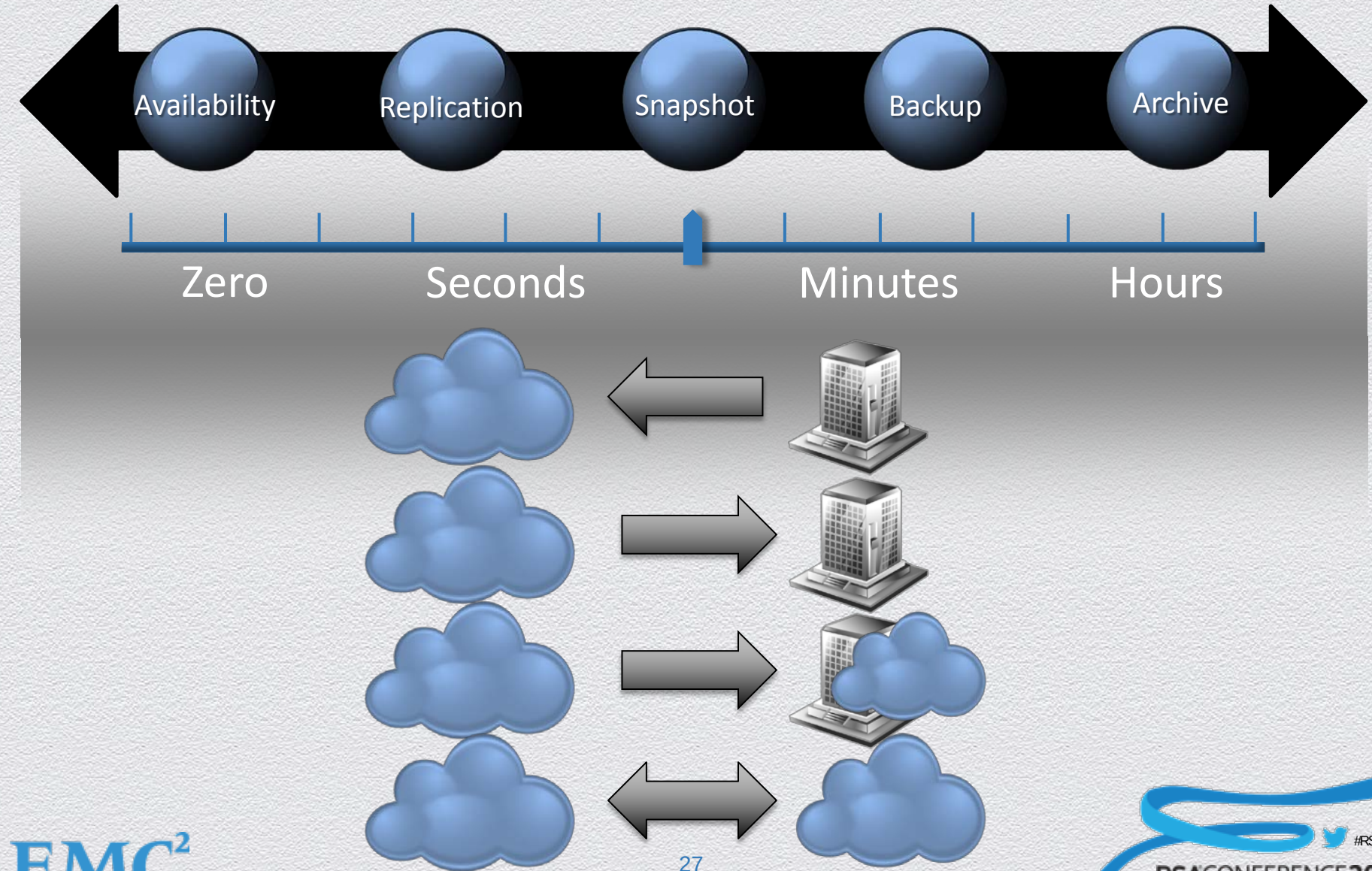
- Custody (SLA)
- Possession (Location, Single/Multi, Hybrid Clouds?)
- Controls (Hands-on Application, Network, System…)

7. Respond to Incidents

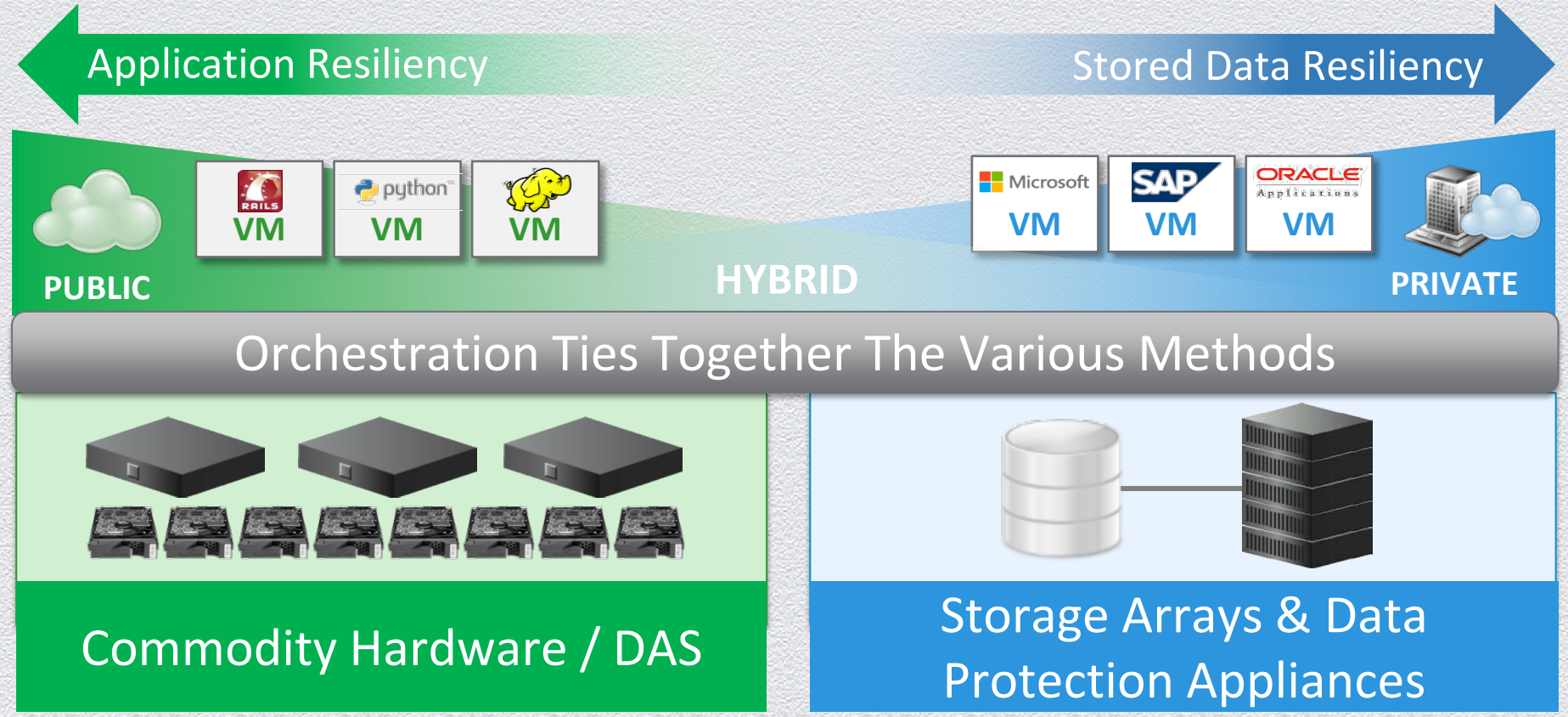
- Intelligence-Driven
- Risk-Aware



8. Backup and Restore



8. Backup and Restore



Essential Steps

1. Reduce Target Area
2. Manage I and M
3. Monitor and Alert
4. Maintain Availability

5. Orchestrate (Automate)
6. Test Security
7. Respond to Incidents
8. Backup and Restore (Exit)

Cloud Trust. Redefined

Transparency

Relevance

Resilience

Thank You!

@daviottenheimer