Life in the Cloud

A Service Provider's View

Michael Smith mismith@akamai.com
Security Evangelist

Agenda

- ✓ Cloud is Secure, Right?
- ✓ Building a Cloud Security Program
- ✓ Security Program Case Study
- ✓ Features, Products, and Configurations
- ✓ What I Want You to Know
- ✓ Summary

Because this is a Cloud Security Talk

Cloud is:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

--CSA Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

What the Cloud Security Alliance Says

"Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties."

--CSA Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

What the Cloud Security Alliance Says

"Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties."

--CSA Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

But...

CSA Guidance is customer-centric and cloud is, by nature, provider-centric.

What the Cloud Providers Say*

- We have a SAS-70 *(but we won't let you see the results or the assertions)*
- We have a ton of big customers, so you can trust us *(and maybe you can talk to them)*
- *The cloud is more secure!*

*Self Excluded

What the Cloud Providers Say*

- We have a SAS-70 *(but we won't let you see the results or the assertions)*
- We have a ton of big customers, so you can trust us *(and maybe you can talk to them)*
- *The cloud is more secure!*

Source:cornify.com

*Self Excluded

So Really....

- What drives a cloud provider's security program?
- How does a good cloud security program look?
- What does a cloud tenant need security-wise to build inside of a particular cloud?
- How does the cloud provider protect themselves from customer security problems?

The “Proper Landing Attitude”

Security of the cloud solution is a joint responsibility between the customer and the service provider.

Please act accordingly.

Agenda

- ✓ Cloud is Secure, Right?
- ✓ Building a Cloud Security Program
- ✓ Security Program Case Study
- ✓ Features, Products, and Configurations
- ✓ What I Want You to Know
- ✓ Summary

Security Program Considerations

- Avoid DNS--”Does Not Scale”
- Build secure infrastructure
- Automate, automate, automate
- Provide self-service capabilities wherever possible
- Meet 75% of customers’ requirements with organic platform features
- Meet 25% of customers’ requirements with add-on modules

Security Program Considerations

- Avoid DNS--"Does Not Scale"
- Build secure infrastructure
- Automate, automate, automate
- Provide self-service capabilities wherever possible
- Meet 75% of customers' requirements with organic platform features
- Meet 25% of customers' requirements with add-on modules

= "Reduce the one-off costs per customer while building a security program that scales."

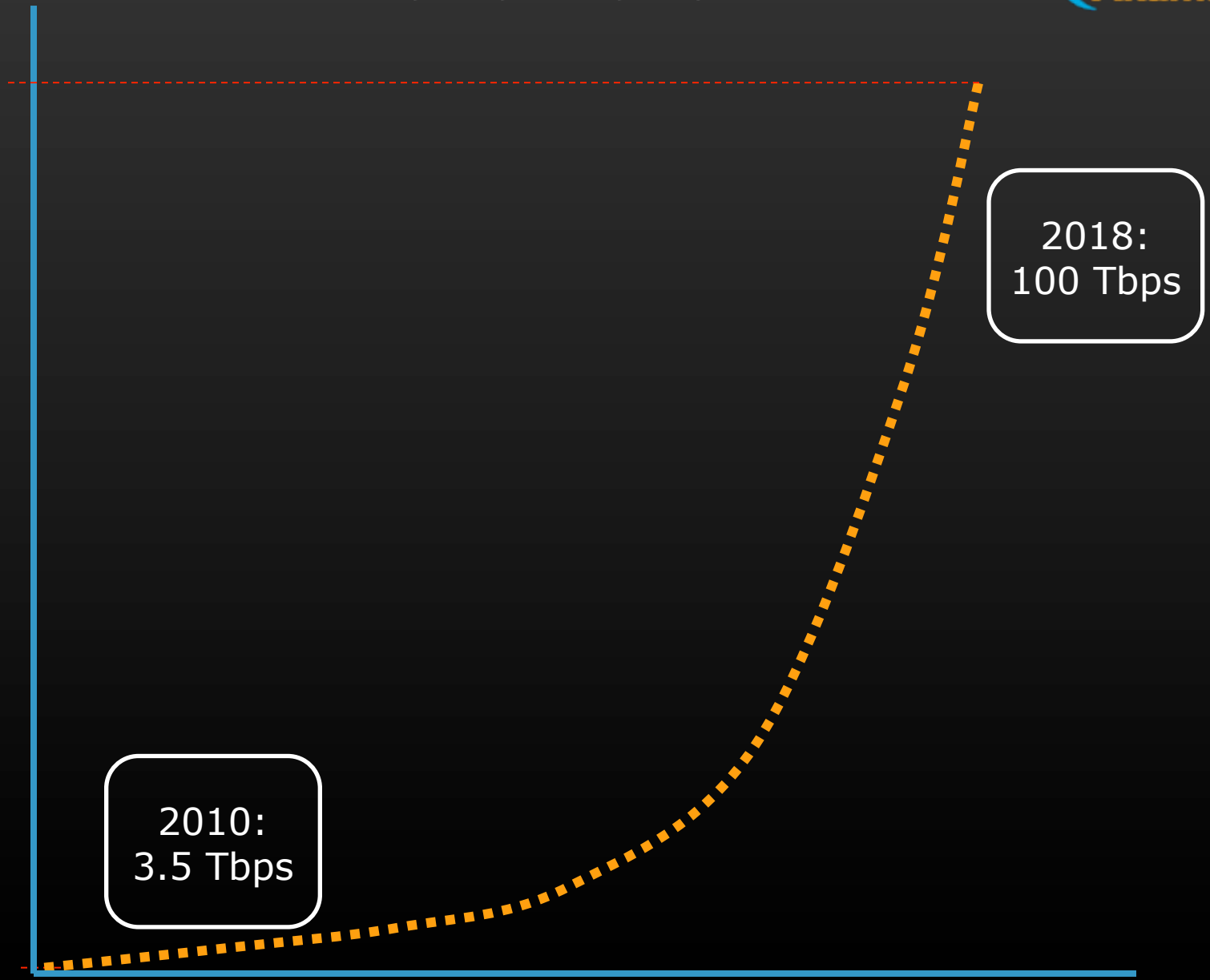
The Akamai Cloud: Largest Distributed Computing Platform in the World

- 73,000+ Servers
- 1,600+ Locations
- 70 Countries

- All branches of the US Military
- 85 of the top 100 online retailers
- 9 of the top 10 anti-virus companies
- 29 of the top 30 M&E companies

- 4.5+ Tbps, 15-25% of web traffic
- 10+ Million transactions per second

What Drives the Akamai Platform?



Agenda

- ✓ Cloud is Secure, Right?
- ✓ Building a Cloud Security Program
- ✓ Security Program Case Study
- ✓ Features, Products, and Configurations
- ✓ What I Want You to Know
- ✓ Summary

Security Governance

- Policy framework established around ISO 27002 framework
- Policies established by Sr. Director of InfoSec
  - Evaluated annually by 3rd party security consulting firm
  - Executive report available upon request
- Quarterly reporting to CEO and staff on state of security

Compliance

- PCI DSS certified Level 1 merchant service provider
  - Annual 3rd party audit
  - Annual penetration testing
  - Quarterly vulnerability assessments
- Annual ISO27002 gap analysis (Foundstone)
  - 2009 rating: 92% compliance against the standard
- US Government
  - DHS Authorization to Operate (NIST SP 800-37)
  - USAF Assessment

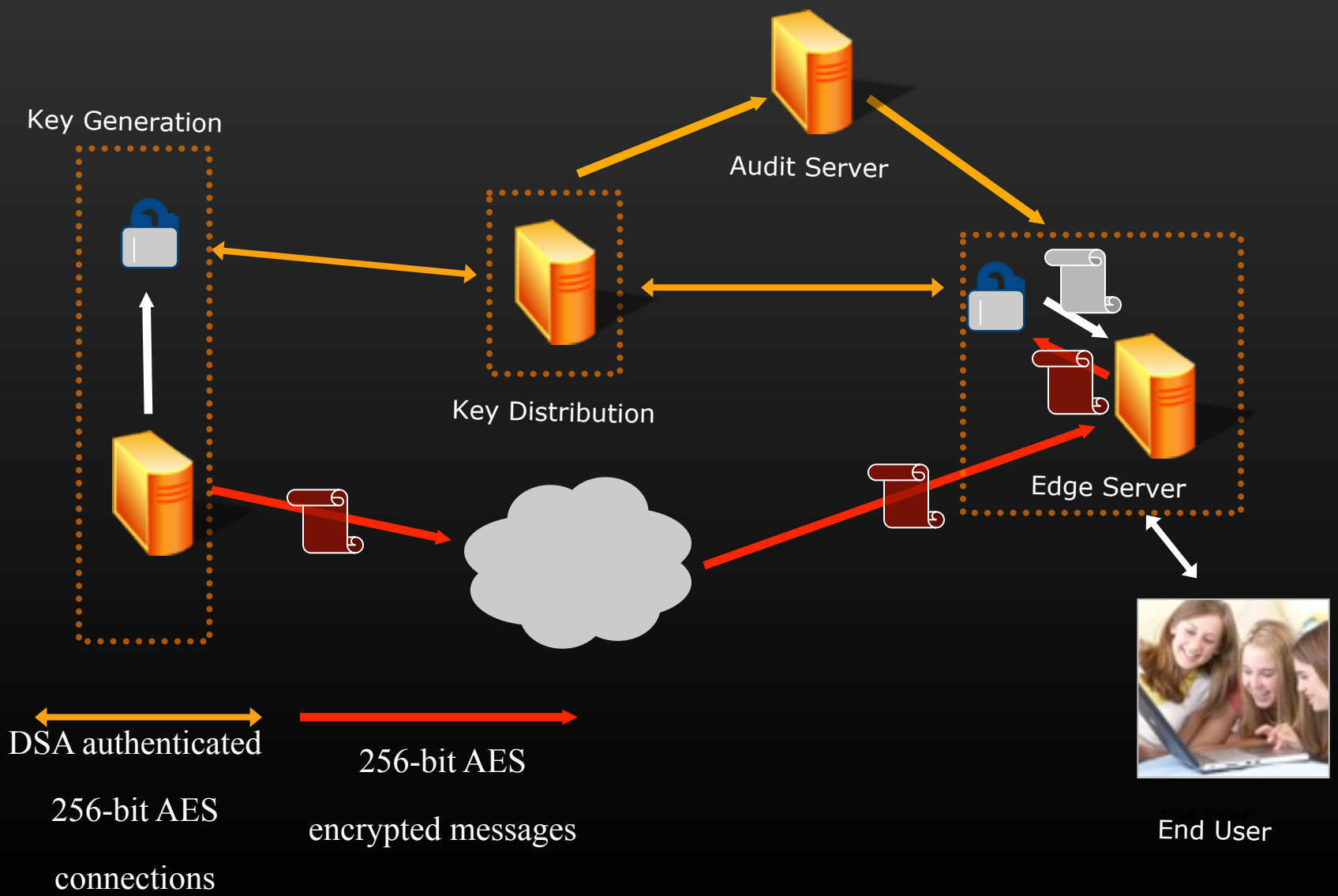
Risk Management

- Risk management activities conducted throughout the product lifecycle
- Vulnerabilities evaluated in two models
  - Probability (Common Vulnerability Scoring System)
  - Damage (Severity/Actor evaluation)
- Risks categorized by area of influence
  - Security (Threats)
  - Scaling (Growth)
  - Bulletproofing (Human error)

Physical/Environmental Security

- SSL network:
  - Safe combo locks on racks
  - In-rack cameras reporting intrusion events directly to Akamai NOCC
- Network deployed in professional colocation facilities with industry standard environmental controls
- Software controls for key management to minimize physical attack surface

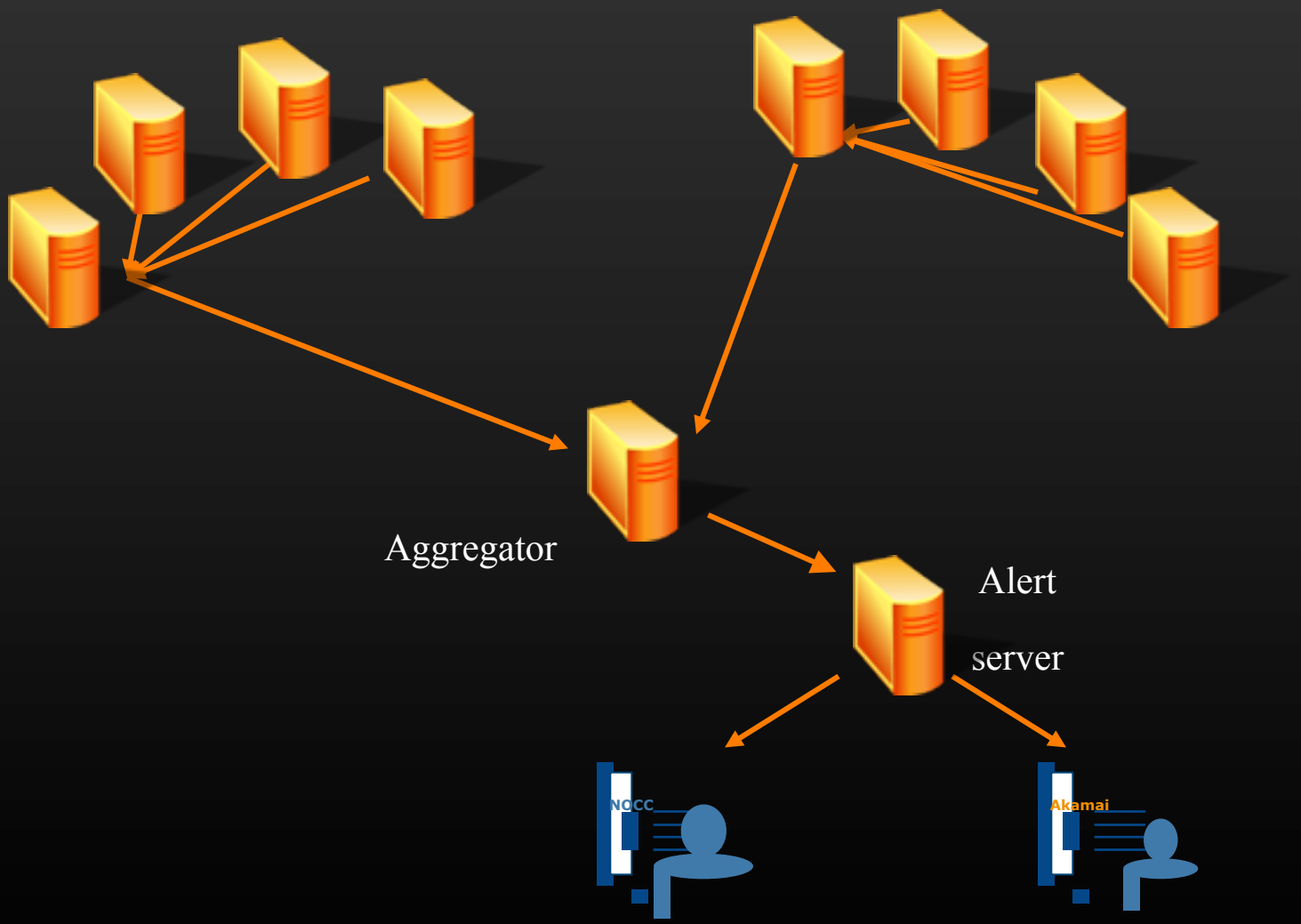
Secure Key Management: "KMI"



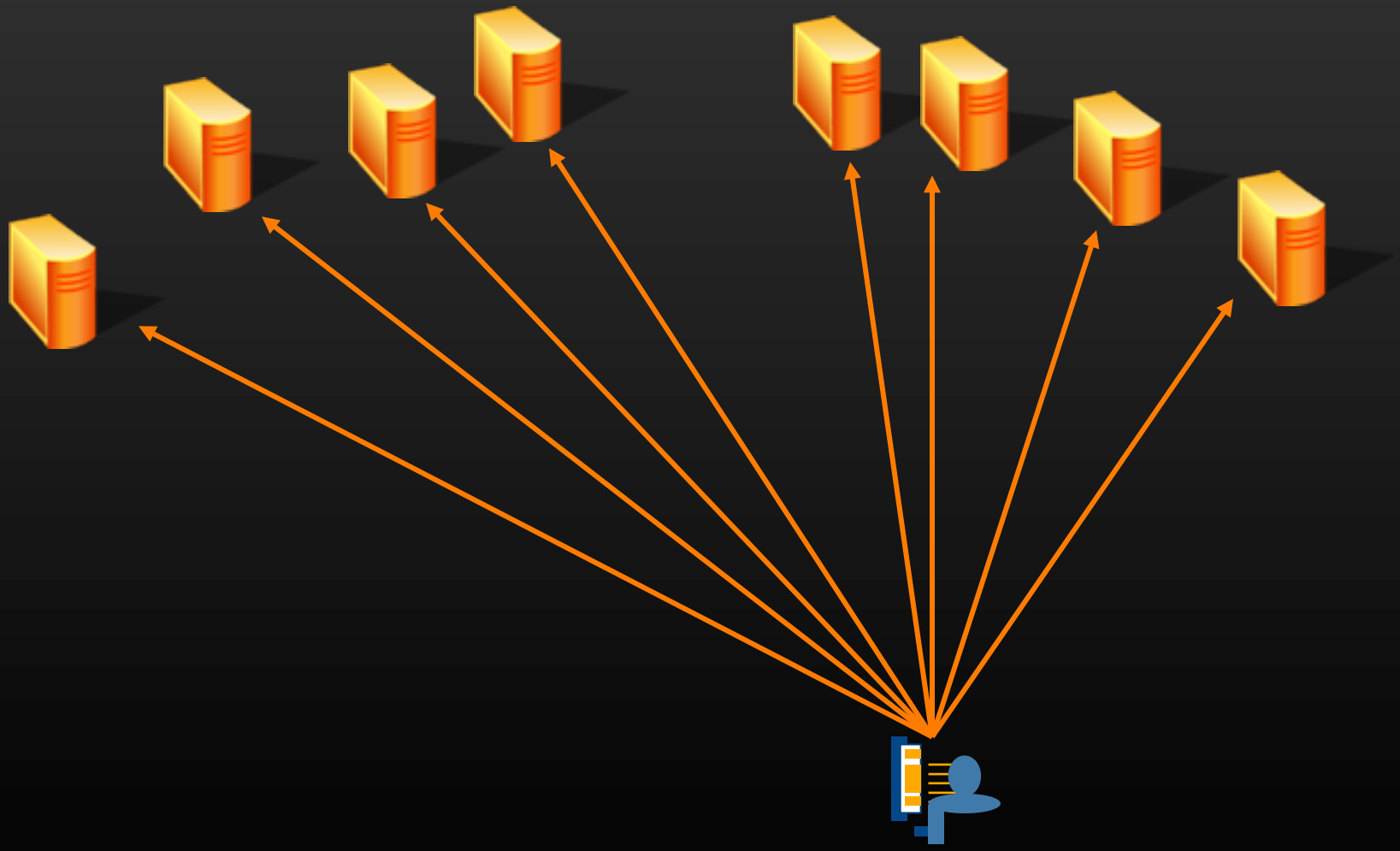
Operations Management

- Each application reports telemetry in real time into distributed reporting infrastructure
- Data aggregation feeds into autonomic management systems, alert infrastructure
  - Autonomic systems act to mitigate faults
  - Alerts trigger human actions to recover root causes
  - (e.g., system failures trigger mapping rebalancing network-wide, while alerts trigger human recovery efforts to restore a machine to service)

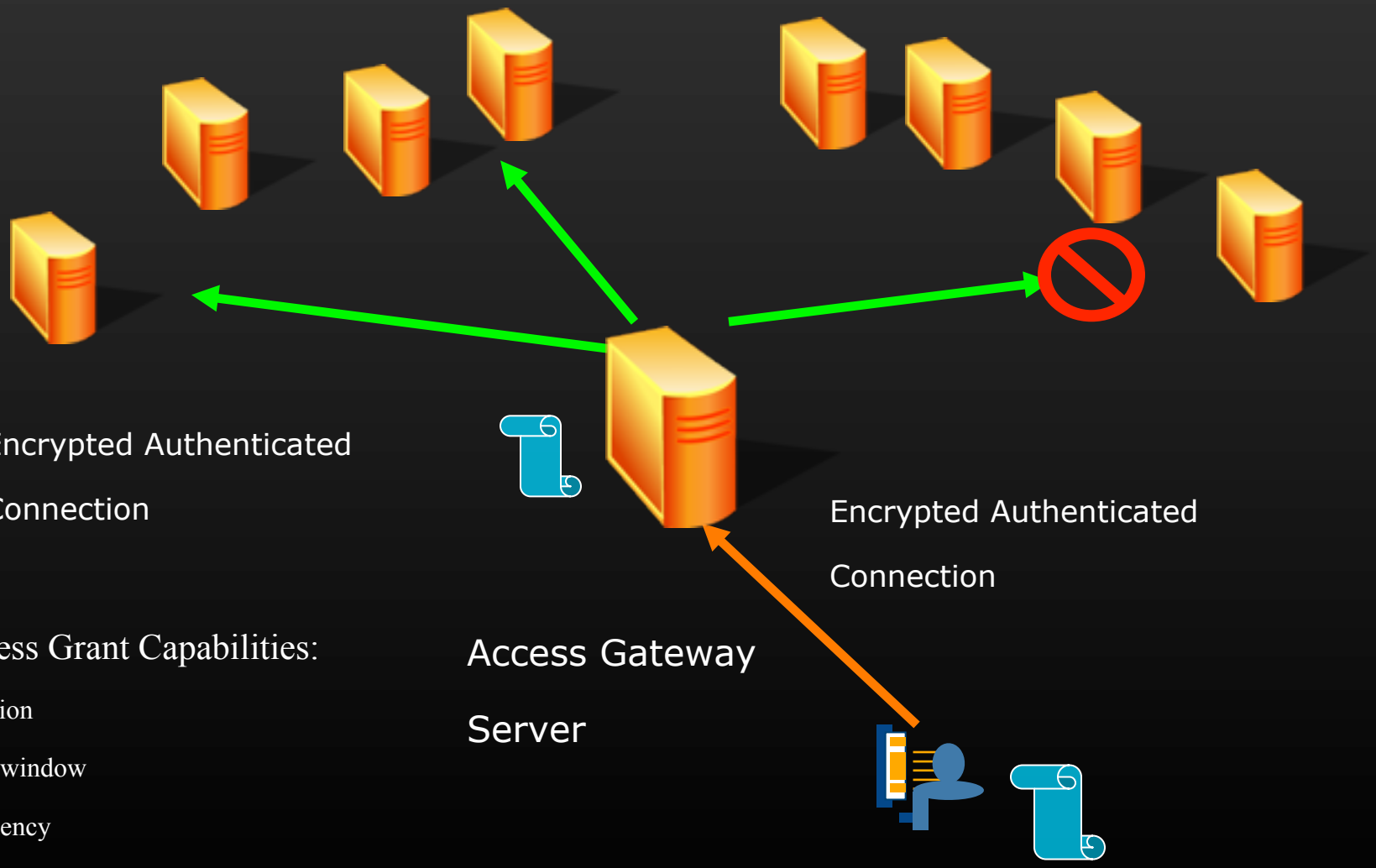
Real Time Event Management: Query



Access Control Management



Access Control Management



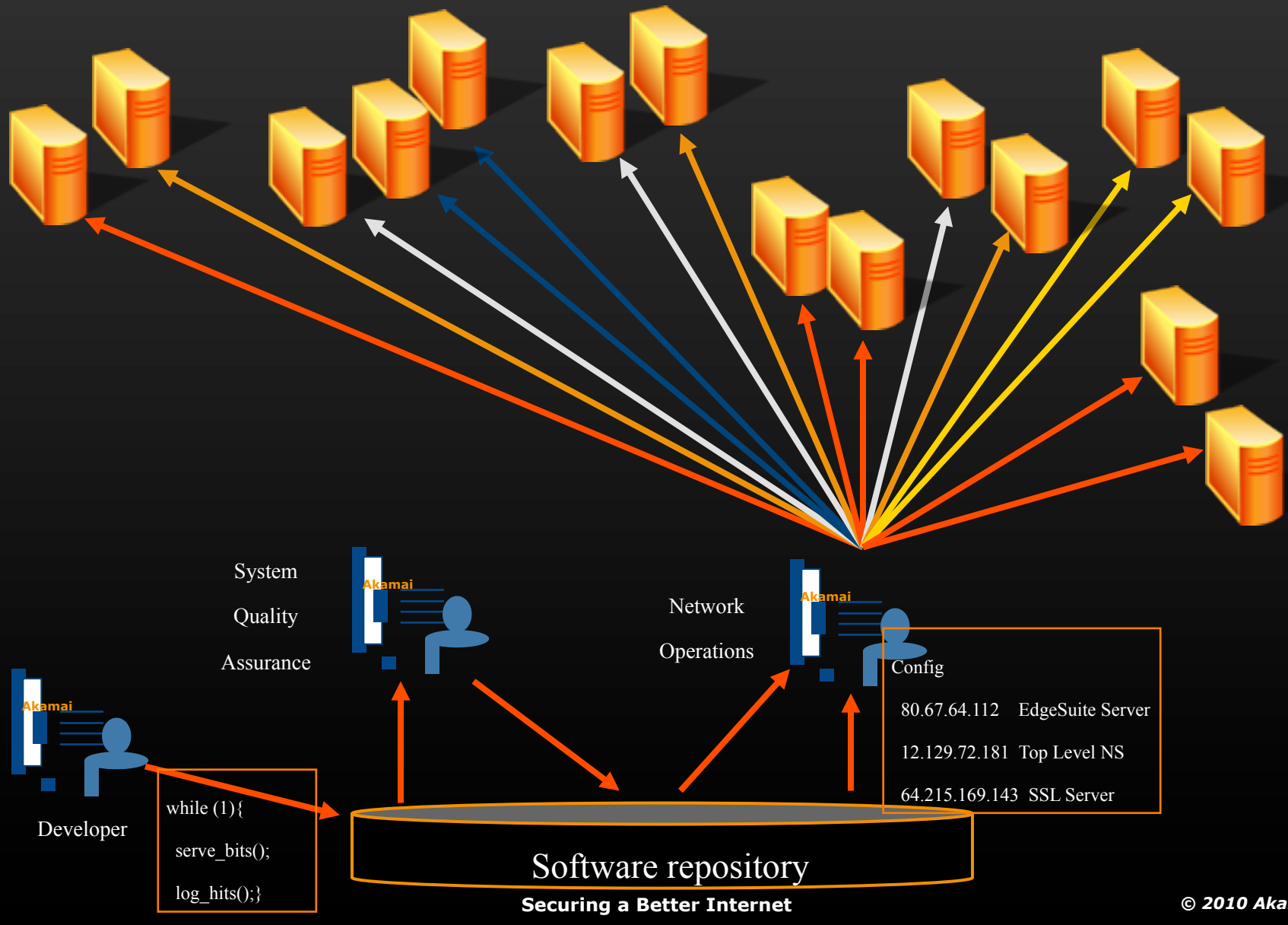
Access Grant Capabilities:

- Location
- Time window
- Frequency
- Type of target system
- 2-factor authentication

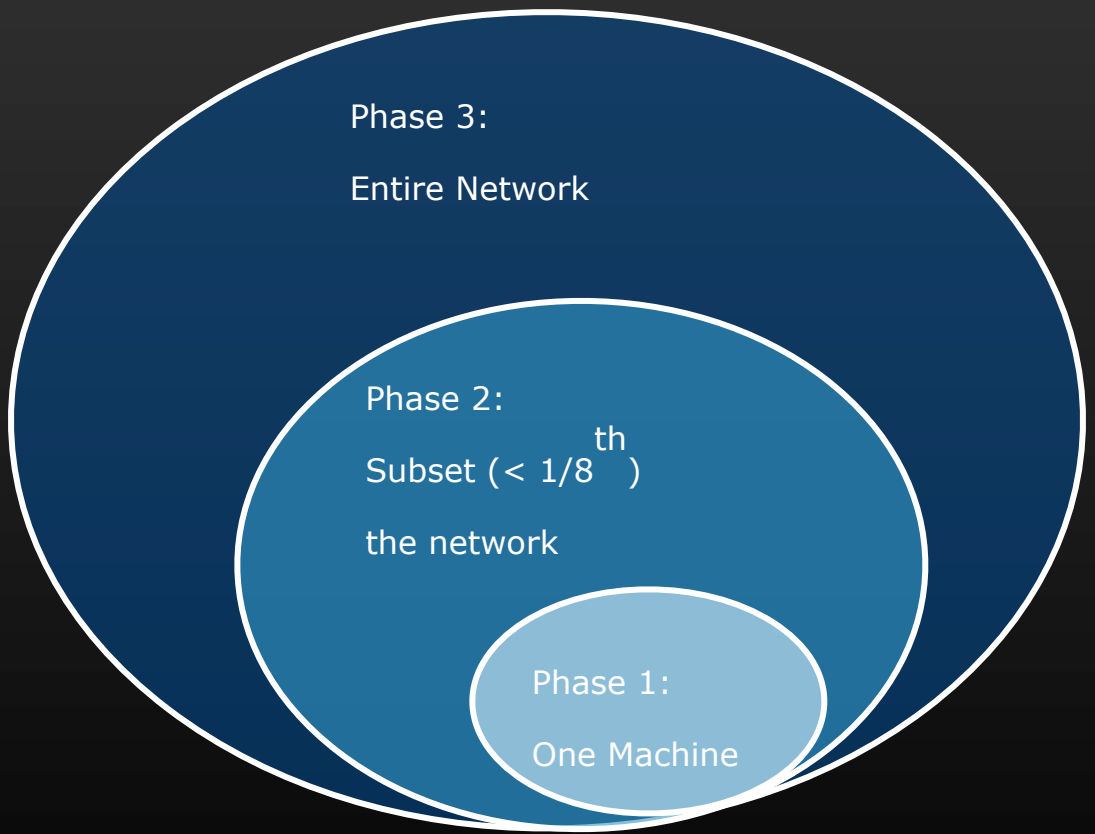
Software Development

- All system components (OS, kernel, applications), as well as configuration are treated as “software”
- Software components developed with automated configuration utilities
- Vulnerabilities and patches deployed as new software images
- “Change once, deploy often”

Software Deployment: "NetDeploy"



Zoning



Release Type	*Phase 1->2*	*Phase 2->3*
Customer Config	15 mins	20 mins
System Config	30 min	2 hours
Standard Software Release	24 hours	24 hours

Security and the Sales Lifecycle

- First Encounter:
  - Information Security Management System Focus Sheet
  - Security Capabilities Focus Sheet
  - Customer-provided questionnaire
  - Introductory security meeting
- Due Diligence Phase (requires NDA):
  - BITS SIG http://www.sharedassessments.org/
  - Executive Summary of ISO 27002 Assessment
  - More Detailed Meeting
- Audit/Assessment Phase:
  - Audit support
  - Compliance modules

Agenda

- ✓ Cloud is Secure, Right?
- ✓ Building a Cloud Security Program
- ✓ Security Program Case Study
- ✓ Features, Products, and Configurations
- ✓ What I Want You to Know
- ✓ Summary

Features, Products, and Configurations

- Controls provided to all customers
- Controls provided as an additional product
- Controls configured by customer
- Controls on roadmap
- Controls not provided

Agenda

- ✓ Cloud is Secure, Right?
- ✓ Building a Cloud Security Program
- ✓ Security Program Case Study
- ✓ Features, Products, and Configurations
- ✓ What I Want You to Know
- ✓ Summary

What I Want You to Know

I can do some things (including security) that you can't do easily or at all.

What I Want You to Know

I have tools to help you meet your security and compliance goals.

What I Want You to Know

Right-to-Audit is DNS.

What I Want You to Know

I need you to audit your portal users.

What I Want You to Know

I provide traffic logs and need you to review them.

What I Want You to Know

Your standard Terms and Conditions are DNS.

What I Want You to Know

When you set up an insecure configuration, it impacts my security.

Agenda

- ✓ Cloud is Secure, Right?
- ✓ Building a Cloud Security Program
- ✓ Security Program Case Study
- ✓ Features, Products, and Configurations
- ✓ What I Want You to Know
- ✓ Summary

Cloud Customers

- "Know Thyself" and what you can put in a cloud
  - Business processes
  - Data types
- Understand the delineation of responsibilities
  - By control
  - By component
- Get a roadmap brief
  - Changing support
  - New features, products, and capabilities
- Make decisions based on cost, benefit, and risk

Cloud Providers

- Automate, automate, automate
- Focus on your unique security capabilities
  - Availability through massive redundancy
  - Security automation
  - Security that scales with demand
- Build a standards-based security program (!=SAS-70 for most cases)
- Delineation of responsibility is how you protect yourself
- Build compliance products to meet the last 25%

"I showed you mine, you show me yours"

Agenda

- ✓ Cloud is Secure, Right?
- ✓ Building a Cloud Security Program
- ✓ Security Program Case Study
- ✓ Features, Products, and Configurations
- ✓ What I Want You to Know
- ✓ Summary