

## Inflection: Security's Next Ten Years

SESSION ID: STR-T09

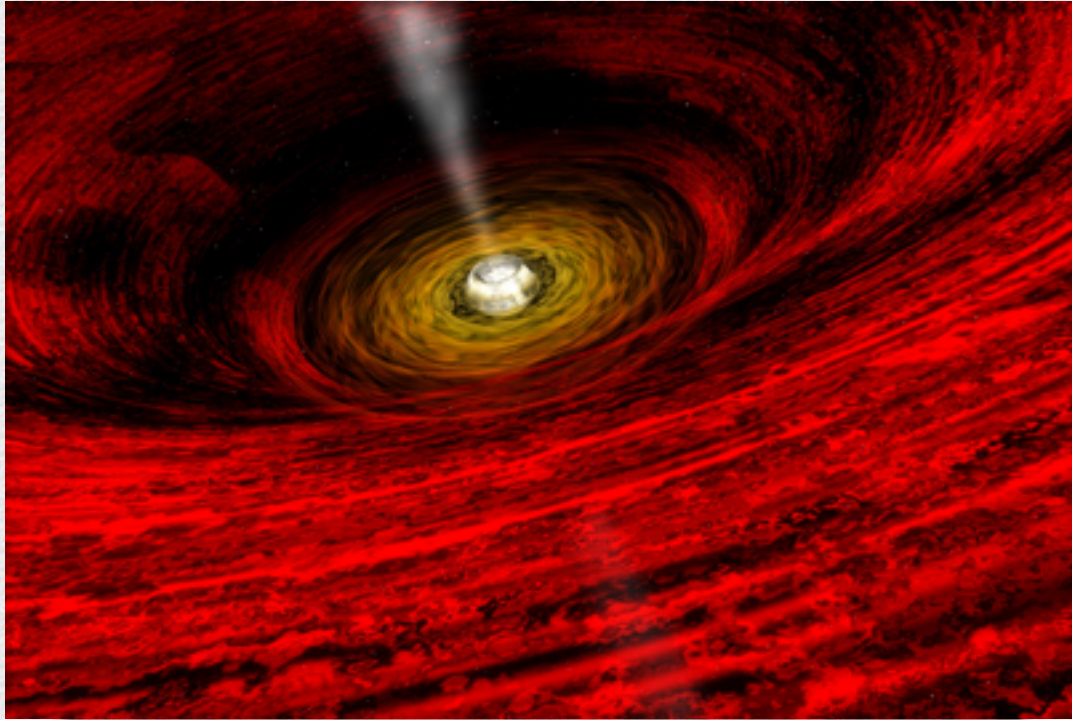
Rich Mogull

Analyst, CEO  
Securosis  
@rmogull





# Our Next Ten Years

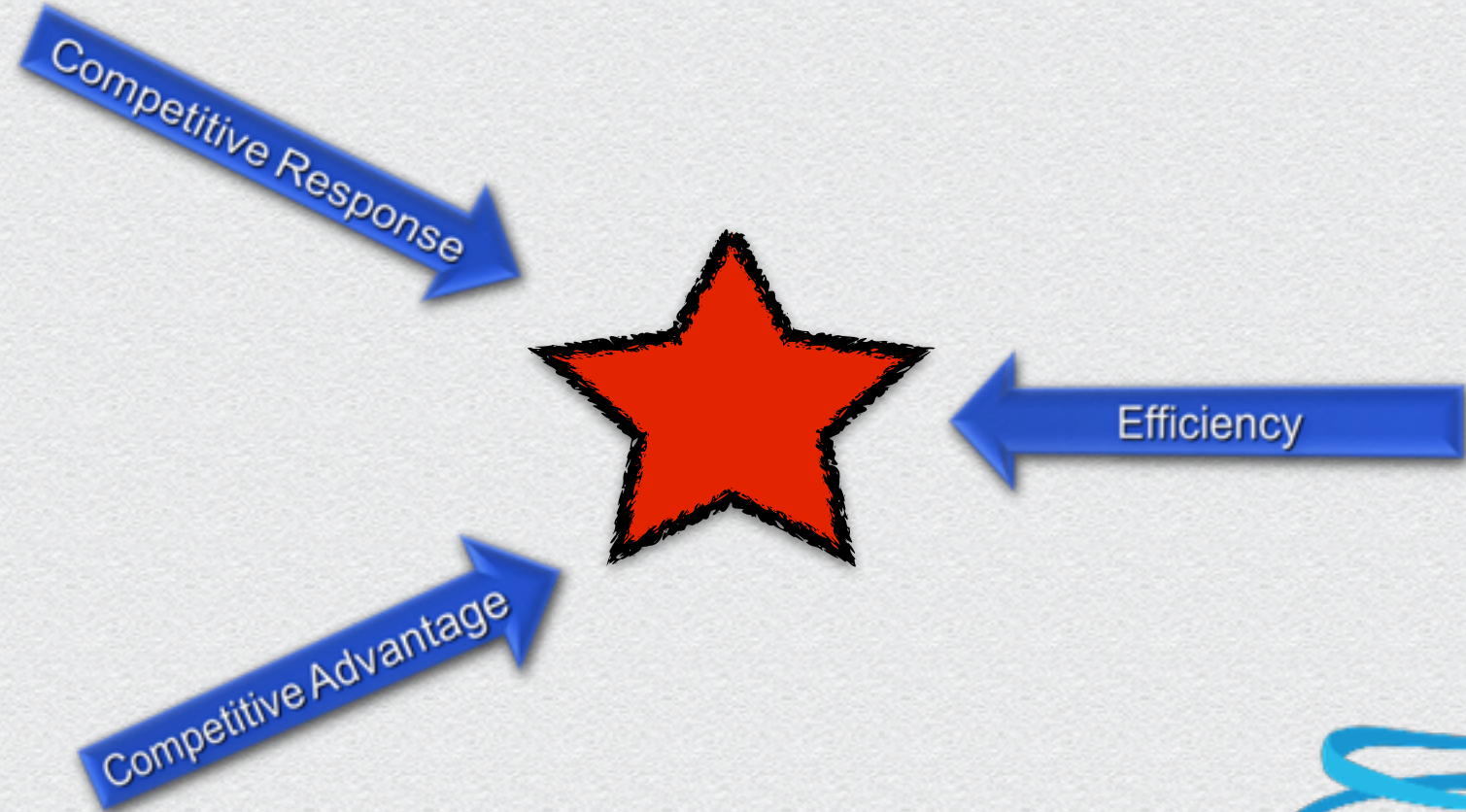




Let's talk about innovation...

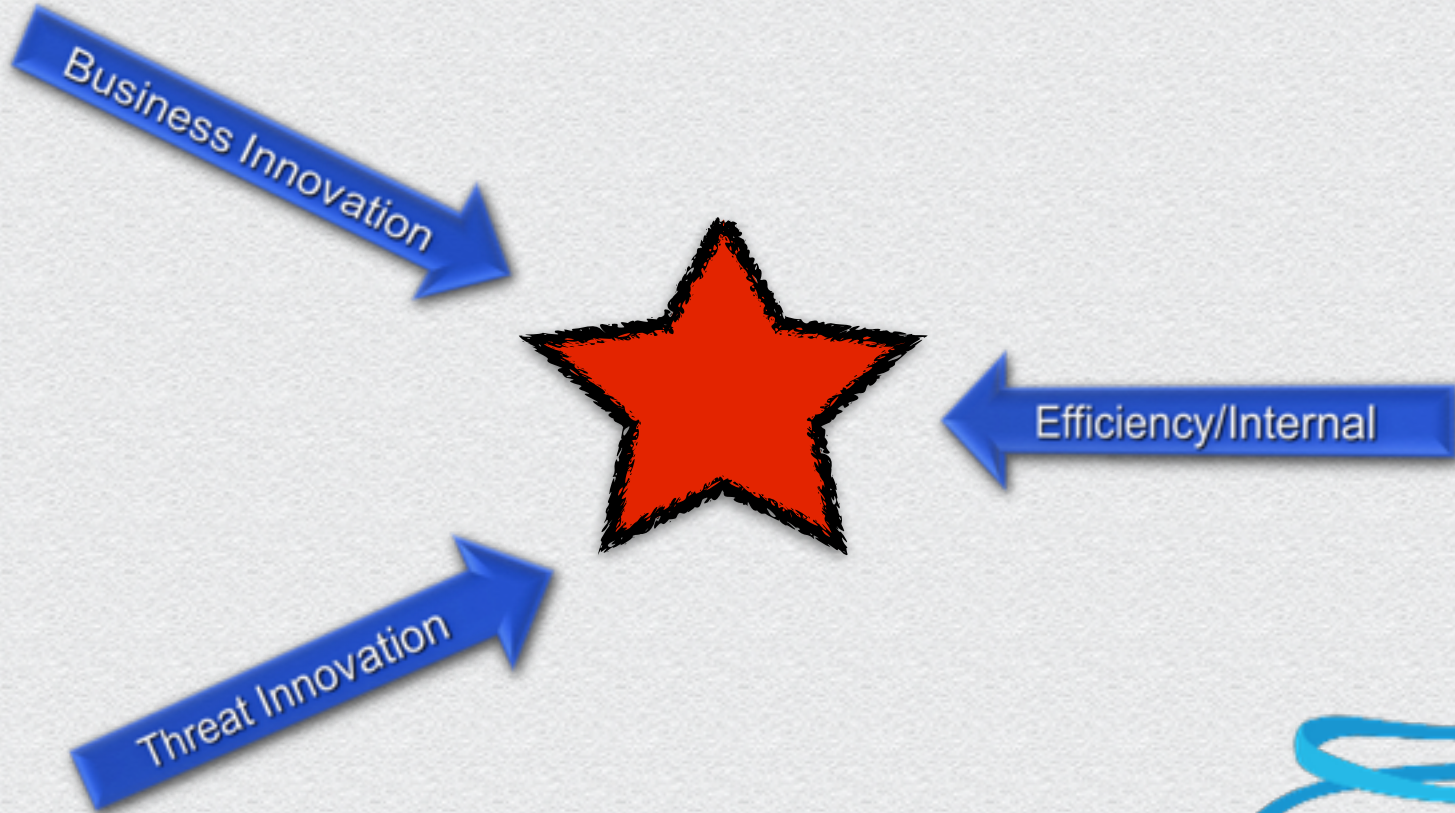


# Business Drivers





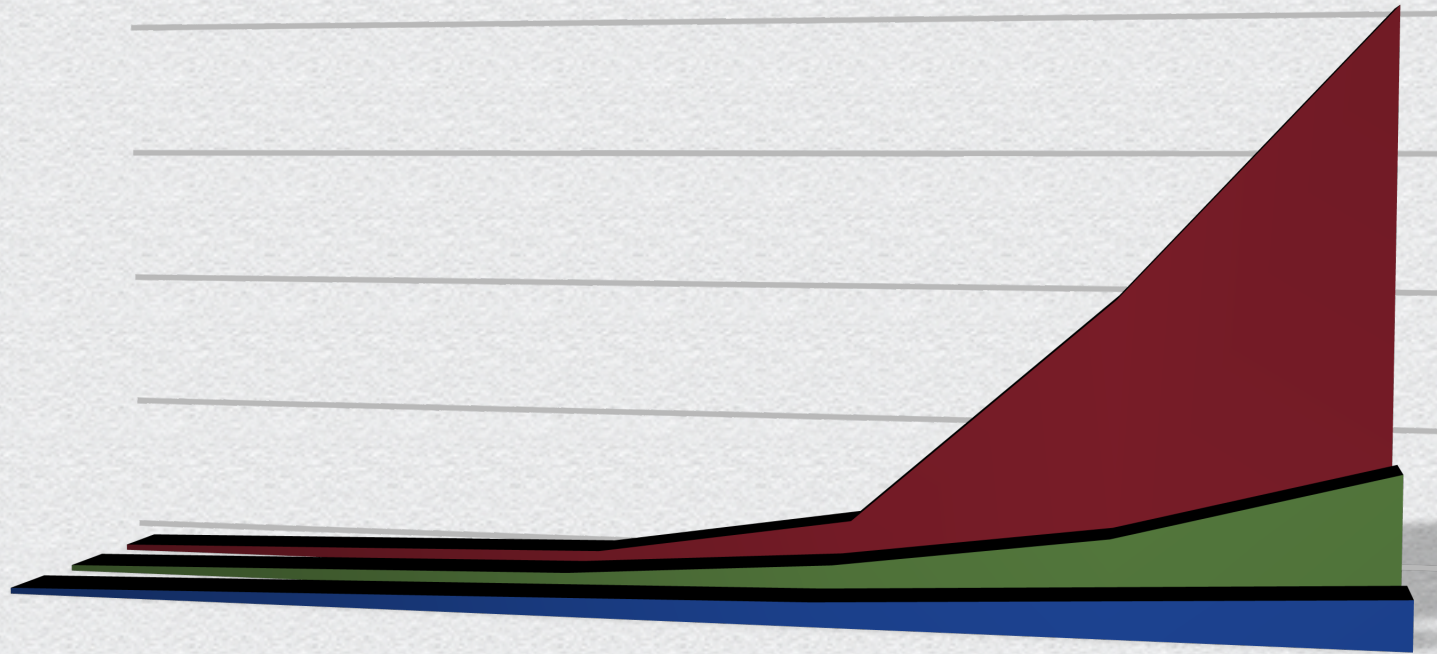
# Security Drivers





Innovation Drives Change...  
Disruptive Innovation requires it

# Relative Security Market Sizes



■ Internally Motivated  
■ Threat/Response

■ Compliance



Securosis



# A Disruptive Collision





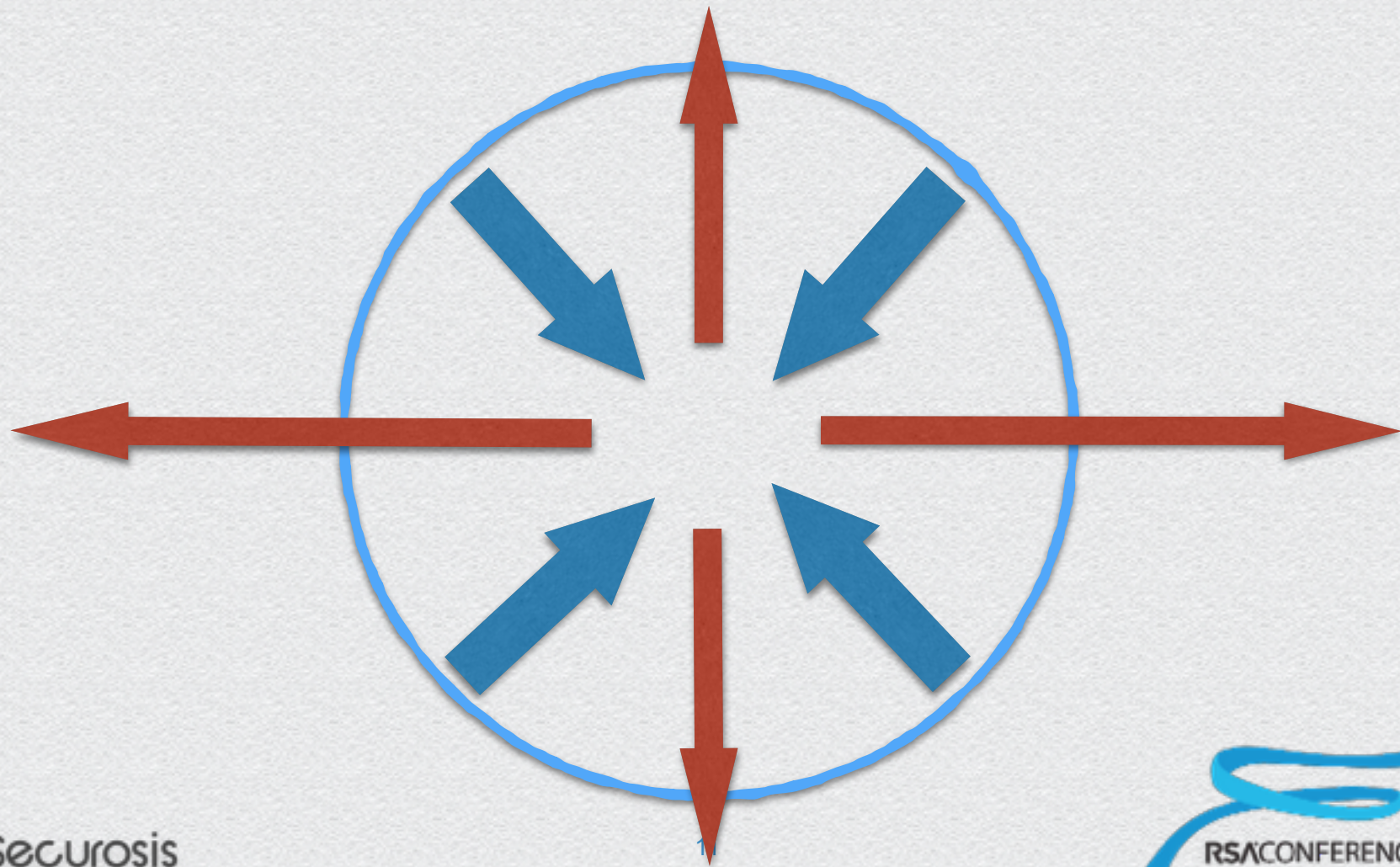
# Cloud computing disrupts security through the introduction of *abstraction* and *automation*





Mobile computing disrupts security by **distributing access** while **reducing control** over devices and networks.







# Six Trends Transforming Security

- ◆ Hypersegregation
- ◆ Operationalization of Security
- ◆ Incident Response
- ◆ Software Defined Security
- ◆ Active Defense
- ◆ Closing the Action Loop



# Hypersegregation



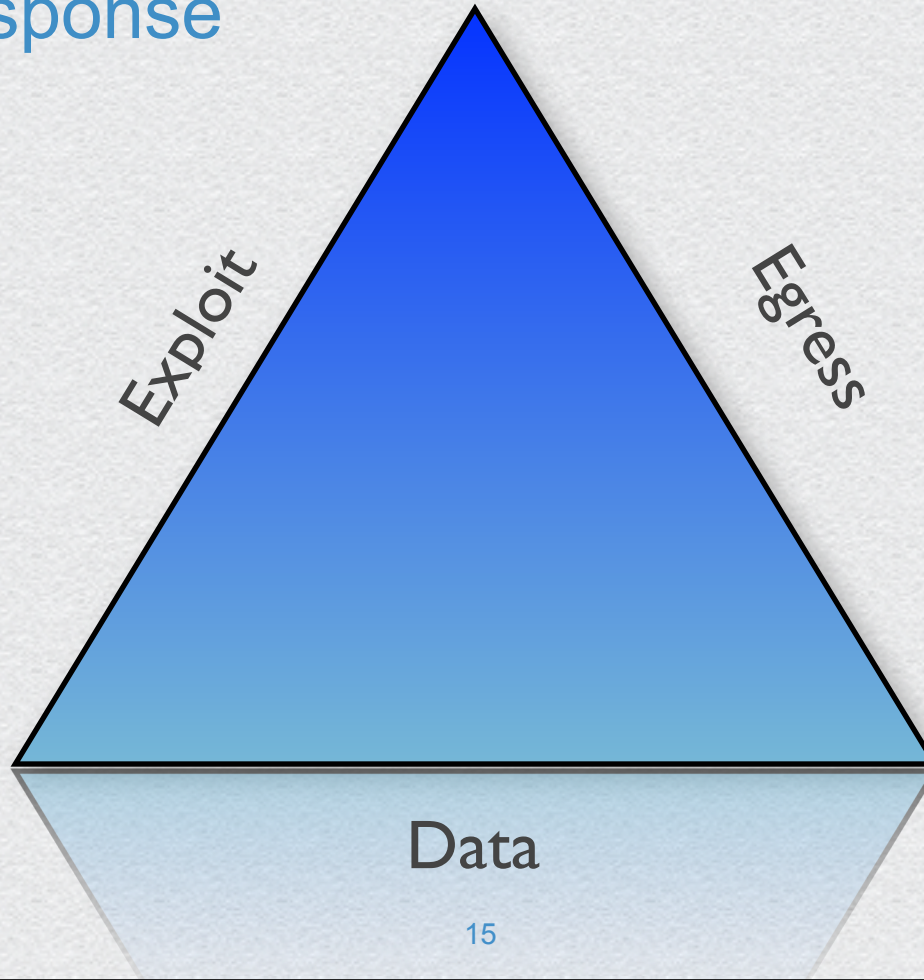
# Operationalization of Security

- Dev
- QA
- Ops
- Security

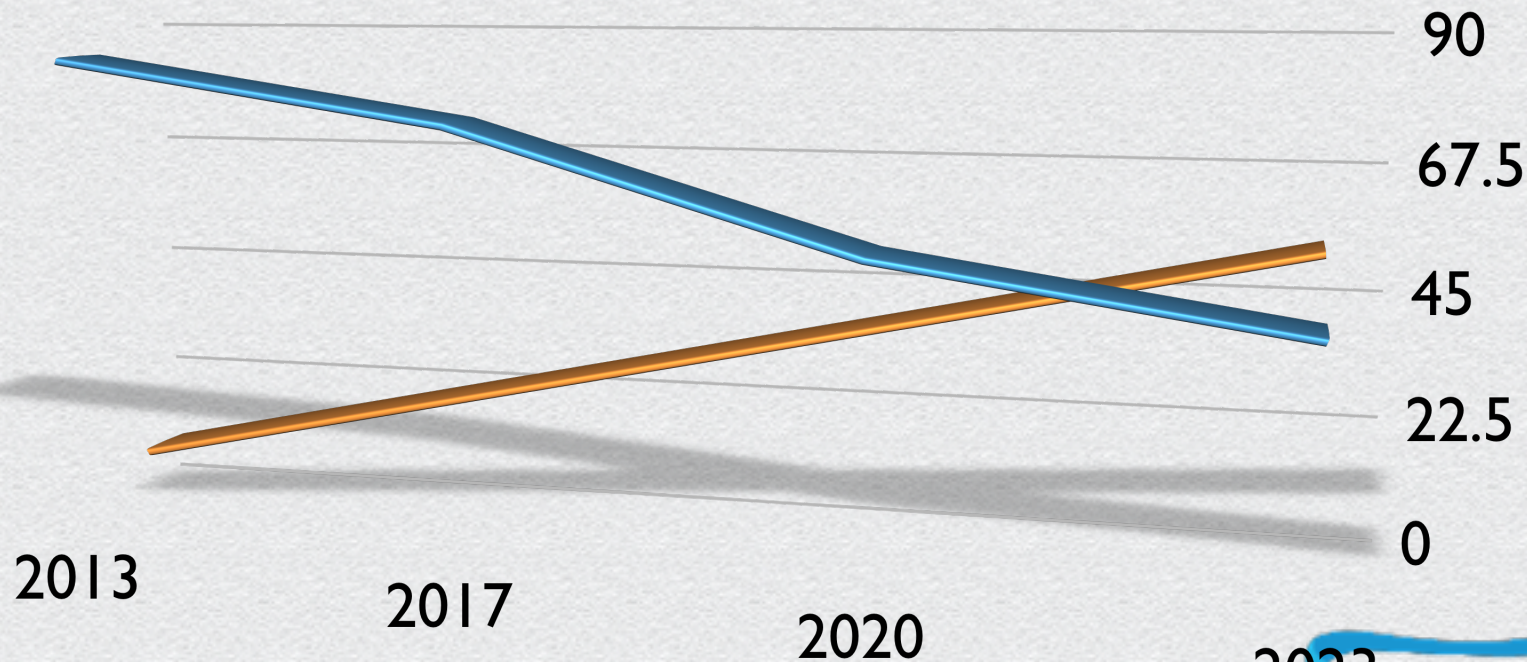




# Incident Response



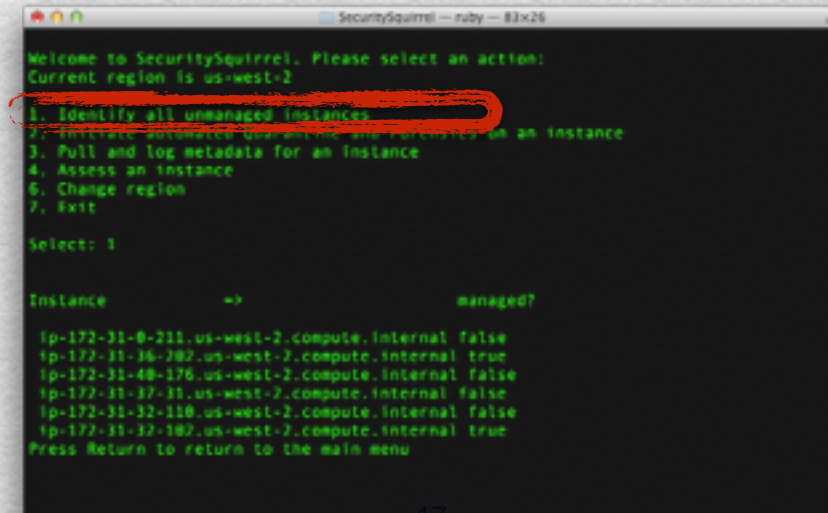
— Firewalls and AV      — Incident Response





# Software Defined Security

```
instancelist = AWS.memoize { ec2.instances.map(&:private_dns_name) }  
nodenames = nodes.map { |node| node.name }  
instancelist.each do |thisinstance|  
    managed = nodenames.include?(thisinstance)  
end
```



The screenshot shows a terminal window titled "SecuritySquirrel - ruby - 83x26". The application displays a welcome message and a list of actions. Action 1, "Identify all unmanaged instances", is highlighted with a red oval. Below the menu, the user has selected option 1. The application then displays a table of instances with columns "Instance" and "managed?". The table lists six instances with their IP addresses, private DNS names, and internal IP addresses, along with a boolean value for whether they are managed.

```
Welcome to SecuritySquirrel. Please select an action:  
Current region is us-west-2  
1. Identify all unmanaged instances  
2. Initiate automated quarantine and remediation on an instance  
3. Pull and log metadata for an instance  
4. Assess an instance  
5. Change region  
6. Exit  
Select: 1  
  
Instance      =>      managed?  
ip-172-31-8-211.us-west-2.compute.internal false  
ip-172-31-16-202.us-west-2.compute.internal true  
ip-172-31-48-176.us-west-2.compute.internal false  
ip-172-31-17-31.us-west-2.compute.internal false  
ip-172-31-32-110.us-west-2.compute.internal false  
ip-172-31-32-102.us-west-2.compute.internal true  
Press Return to return to the main menu
```

## Force Attacker Perfection



## Active Defense



# Closing the Action Loop

Today

Silos

Too many shells

Stale data

Gaps

Manual response

Tomorrow

Big Data

Visualization

Orchestration

Action



Software Defined Security



# Closing the Action Loop

Today

Silos

Too many shells

Stale data

Gaps

Manual response

Tomorrow

Big Data

Visualization

Orchestration

Action

Software Defined Security





# Implications for Security Professionals

- ▶ **Audit/assessment and penetration testing** are essential to understand the highly variable security of providers, and to assure security works as expected.
- ▶ **Incident response** is already in high demand, and must expand to cover response in the cloud-distributed enterprise.
- ▶ **Secure programming** orchestrates and automates security across cloud, mobile, and internal security tools.
- ▶ **Big data security analytics** makes sense of the vast amounts of security data we now collect, and better detect and remediate incidents involving advanced attackers.
- ▶ **Security architects** assess and design security controls — internally, across cloud providers, and for applications.



# Implications for Security Providers

- ▶ **Support APIs** so customers can directly integrate your products into infrastructure, applications, and services.
- ▶ **Lose the bump in the wire** because cloud-distributed organizations won't centralize all network traffic for you to scan or manage.
- ▶ **Provide feeds and logs** so your tool integrates with the Security Operations Center of the future; don't require customers to log into your product to access data.
- ▶ **Assume high rates of change** which exceed the scheduled periodic scans and assessments we tend to rely on.



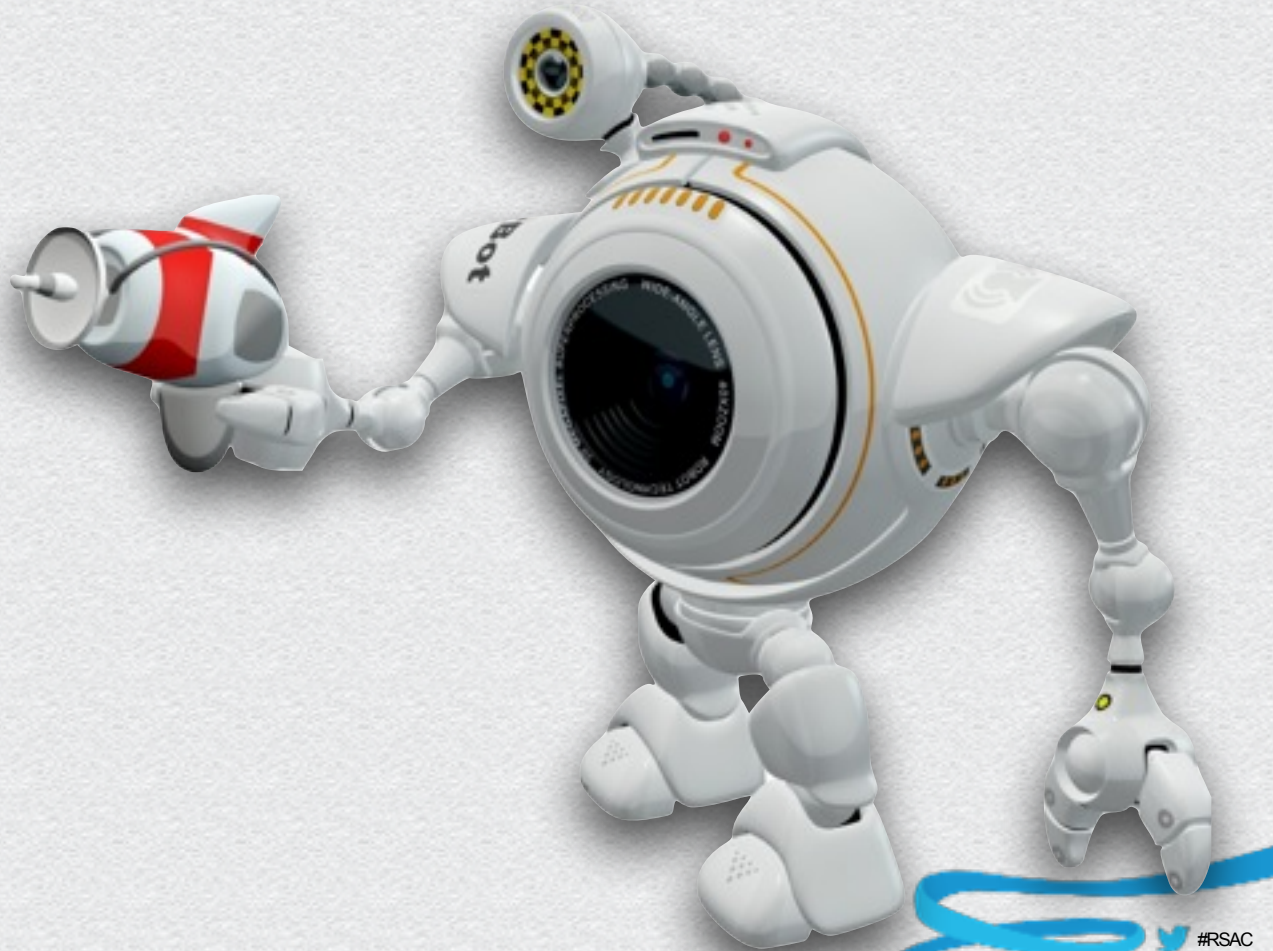
# Implications for Cloud Providers

- ▶ **Build a security baseline** that is as or more secure than an enterprise datacenter.
- ▶ **Defend against advanced attacks**. You are a bigger target than any single customer, and the rewards are higher for the bad guys.
- ▶ **Don't alter user data or workflows**. They own them, not you.
- ▶ **Protect the cloud supply chain**. A failure of one of your providers shouldn't damage your customers.
- ▶ **Support APIs for security** so customers can manage and integrate it themselves.
- ▶ **Document security** for both your internal controls and what customers can manage, so they know *how you enable their security strategy*.
- ▶ **Provide security logs and feeds** so customers always know what is happening with their data and



# Security, 2024

- ◆ Abstracted
- ◆ Automated(ish)
- ◆ Response-focused
- ◆ Orchestrated
- ◆ Hypersegregated
- ◆ Unevenly distributed





**RSA CONFERENCE 2014**

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



**Securosis**  
2000-2012

## **Inflection: Security's Next Ten Years**

**Rich Mogull**

rmogull@securosis.com  
@rmogull