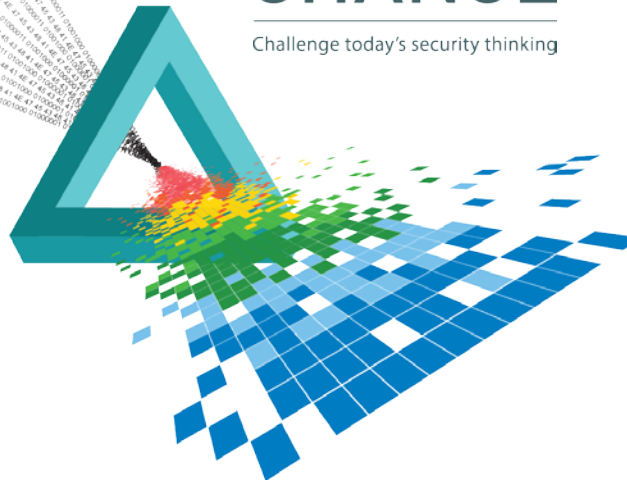
RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking



SESSION ID: CDS-R01

Validating the Security of the Borderless Infrastructure

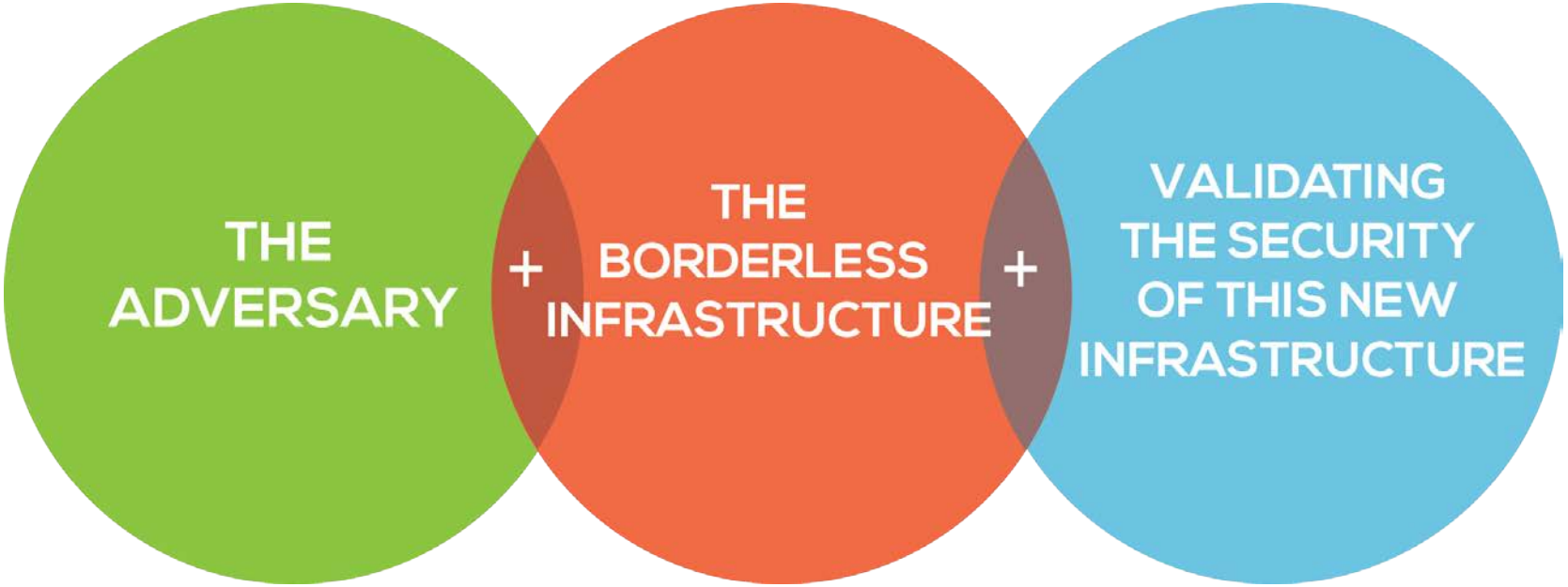
David DeSanto

Director, Product Management
Spirent Communications, Inc.
@david_desanto

SPIRENT

#RSAC

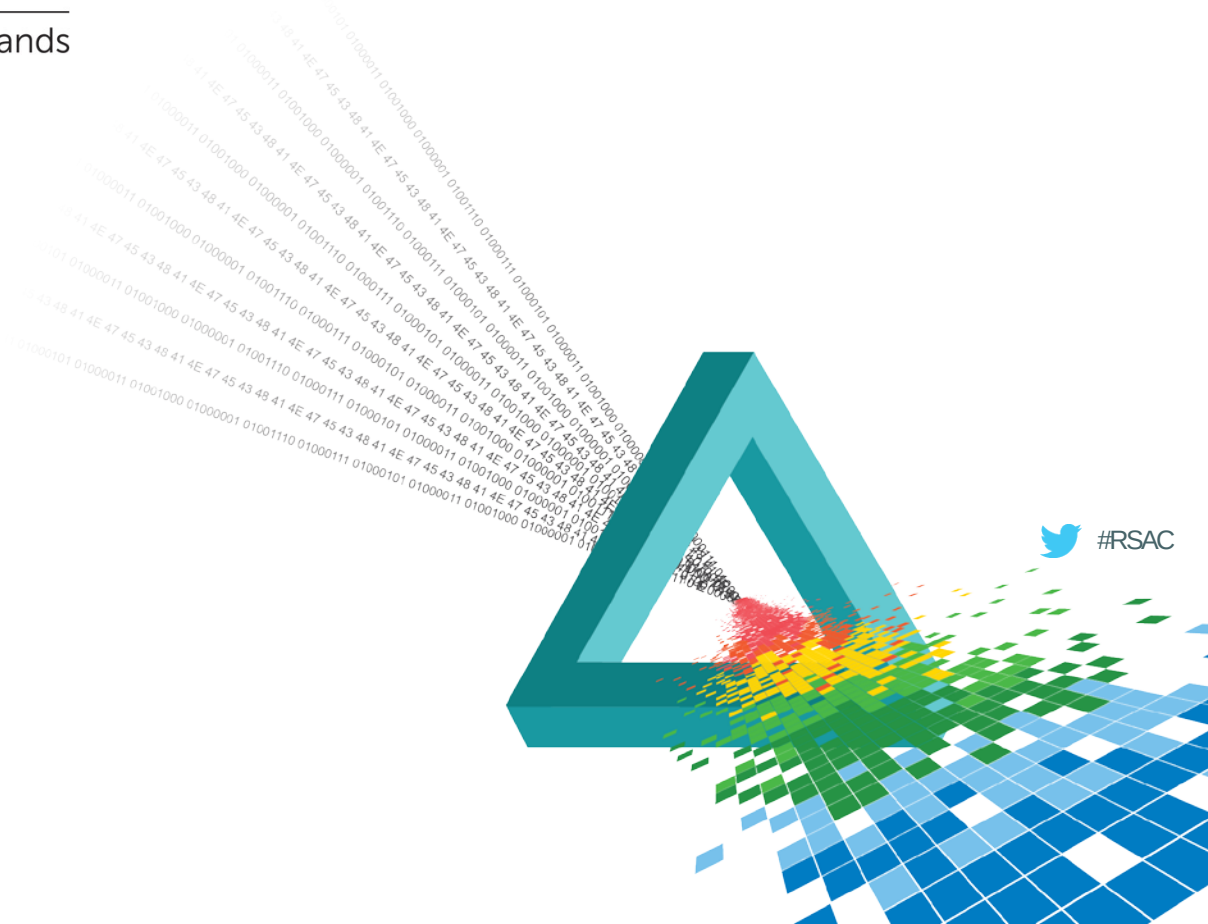
Agenda



SPIRENT

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

The Adversary

SPIRENT

The Adversary

Three Main Types of Attacks

- DDoS Attacks
  - Volumetric – Consume all bandwidth
  - Protocol – Consume all state (i.e., TCP state table)
  - Application – Consume or exploit application layer

- Exploits
  - Targeting public facing services for vulnerabilities
  - Used as the delivery mechanism for command and control channels (data exfiltration)
- Malware
  - Advanced Persistent Threats / Targeted Persistent Threats
  - Mobile malware for gaining traction for accessing sensitive data

The Adversary

- DDoS Attack Statistics

90% of service providers **experienced an application-layer attack**

47% of service providers saw **application-layer attacks targeting HTTPS**

400 Gbps
Largest attack recorded in 2014

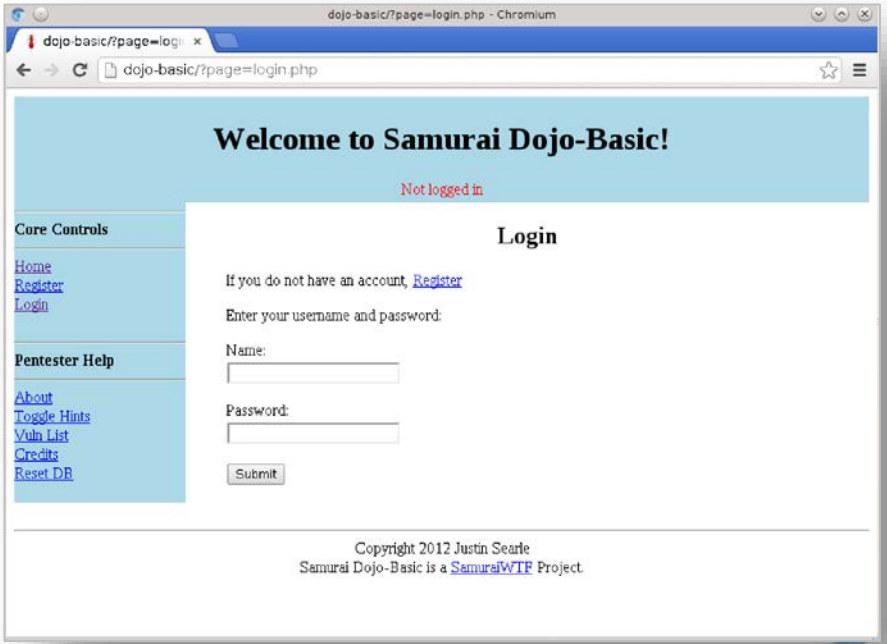
75% of service providers saw **application-layer attacks targeting HTTP and DNS**

- SOURCE: Arbor Networks Tenth Annual Worldwide Infrastructure Security Report

SPIRENT

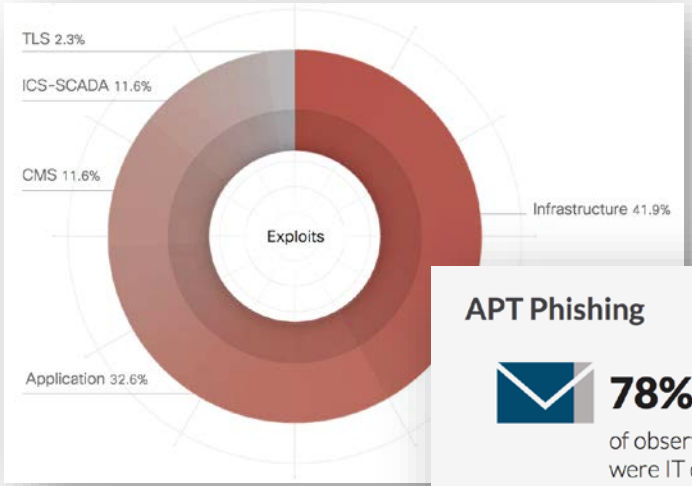
The Adversary

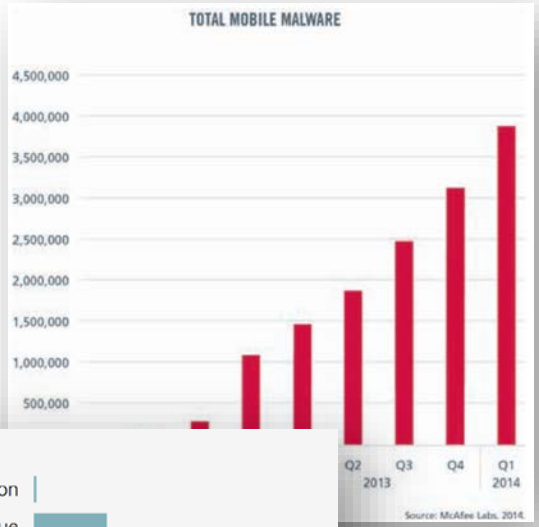
- Application DDoS Attack Example
  - R.U.D.Y. (R-U-Dead-Yet)
    - HTTP Slow POST DoS attack
    - Targets web forms with never ending POST values
    - Easily scalable into an application DDoS attack
    - With little effort, website becomes unavailable



The Adversary

- Exploit and Malware Statistics





- SOURCE: Cisco 2015 Annual Security Report, Mandiant M-Trends 2015: A view from the front lines, McAfee Labs Threats Report June 2014

The Adversary

- Malware Example
  - Duqu 2.0 - Cyberespionage Advanced Persistent Threat (APT)
    - Known to have exploited three different zero-day vulnerabilities
    - Highly sophisticated anti-detection techniques
    - Command-and-control (C&C) mechanisms masked within image files
    - Known targets
      - Kaspersky Lab
      - Iranian Nuclear Talks (P5+1 events)
      - European Telecoms Operator

SPIRENT

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

#RSAC

The Borderless Infrastructure

SPIRENT

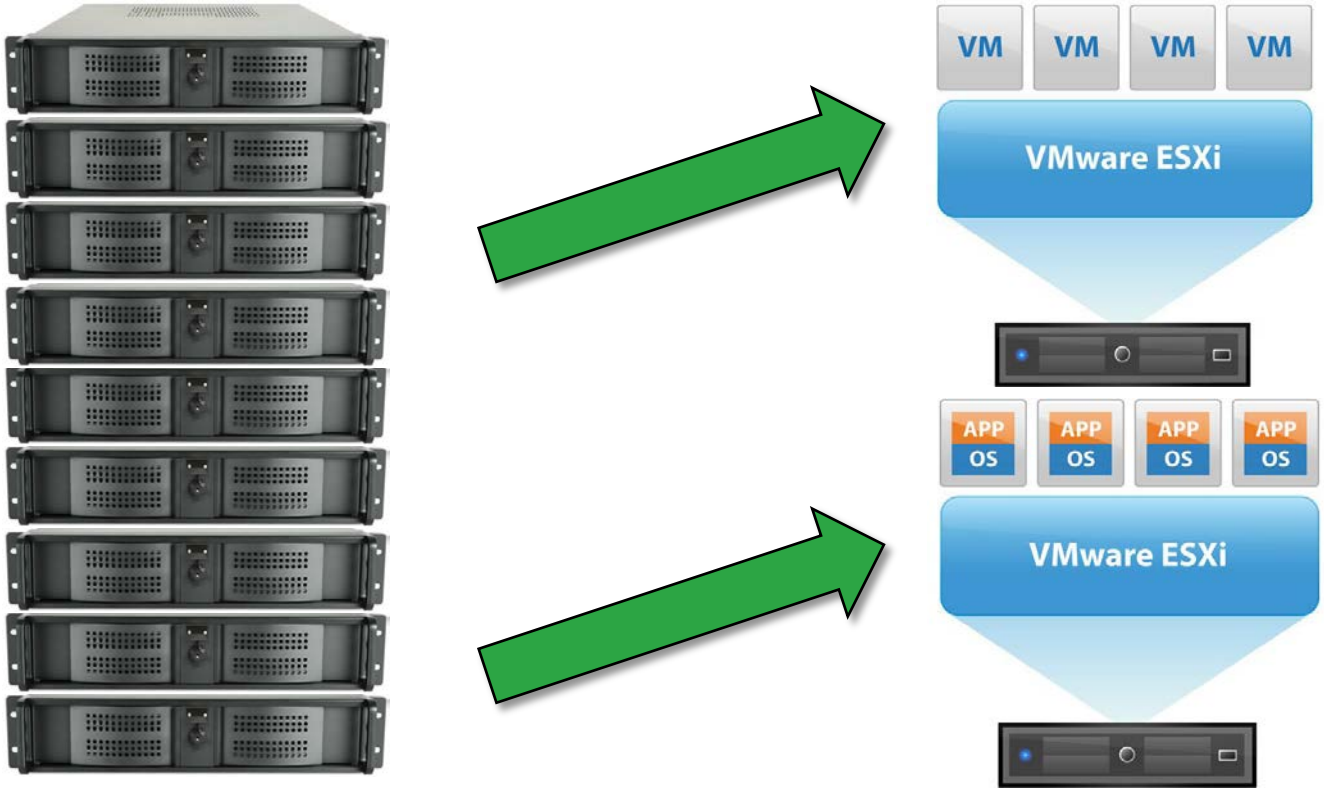
The Borderless Infrastructure

“In the early years of this market, most data virtualization was focused primarily on the financial services, telecom and government sectors. In the past three years, however, Forrester has seen significantly increased adoption in other verticals, such as insurance, retail, health care, manufacturing and e-commerce.”

The Forrester Wave™: Enterprise Data Virtualization, Q1 2015

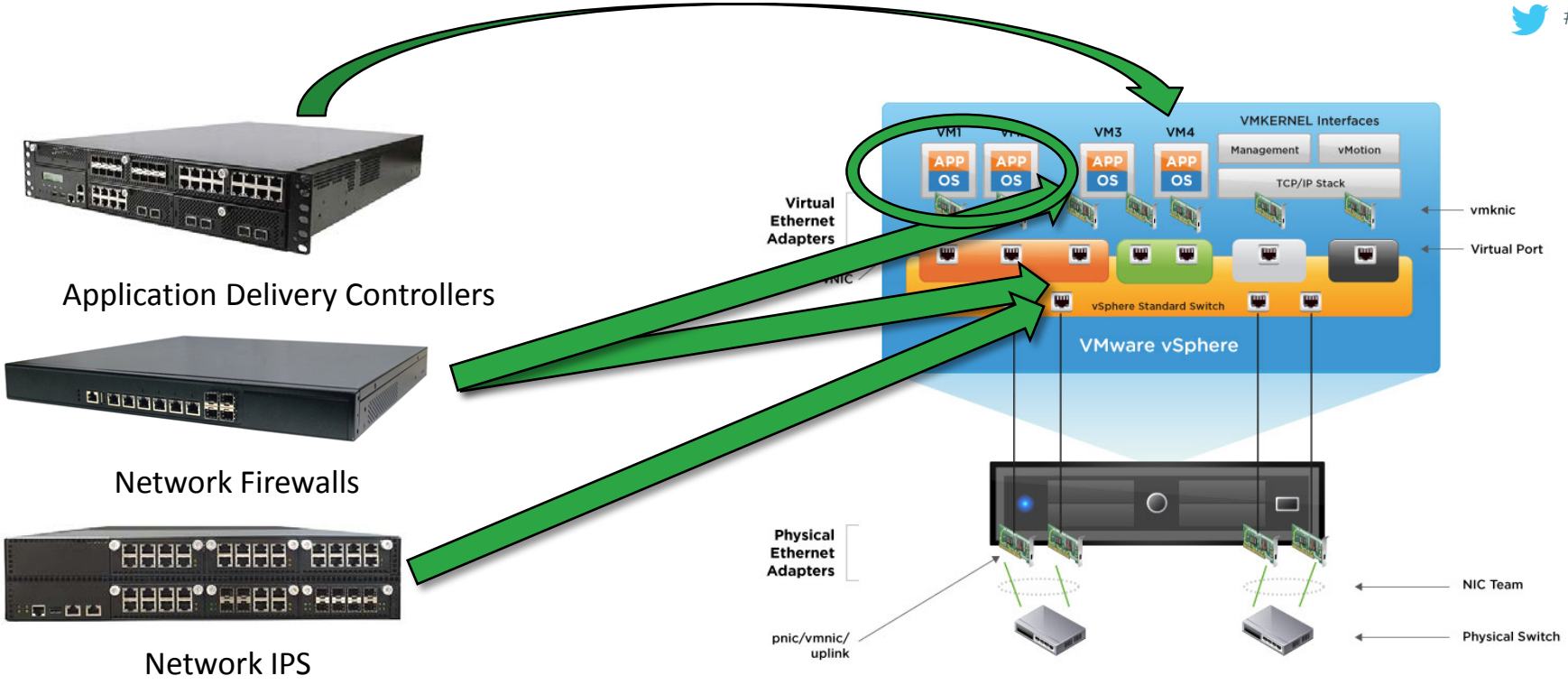
Forrester Research, Inc.

SPIRENT



Server and Application to Virtual Deployments

Deployments within data centers as well as migration to the cloud



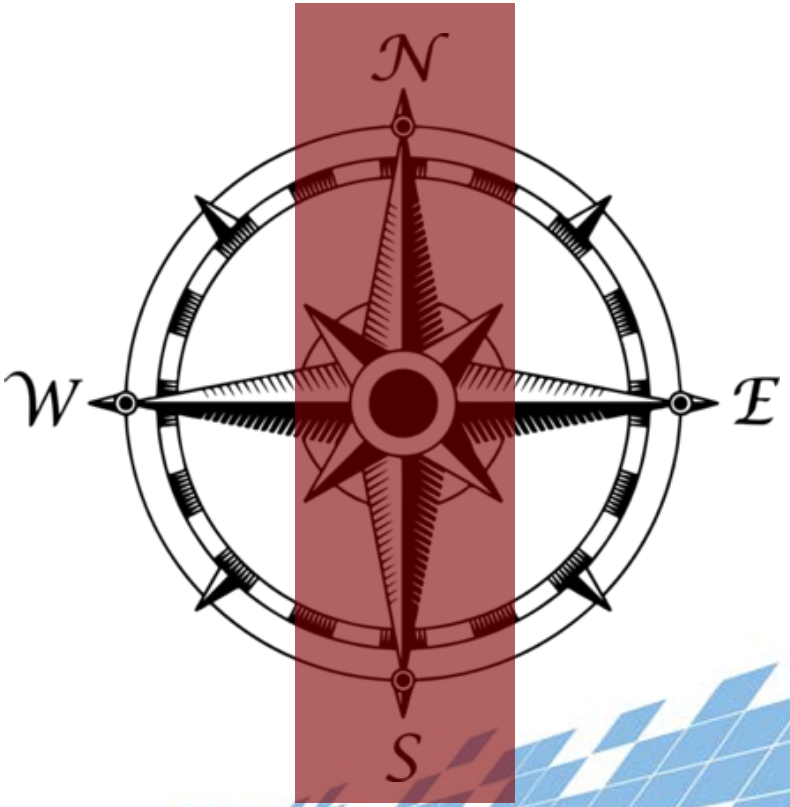
Virtual Security and Content Delivery Deployments

Deployments within data centers as well as migration to the cloud

SPIRENT

The Borderless Infrastructure

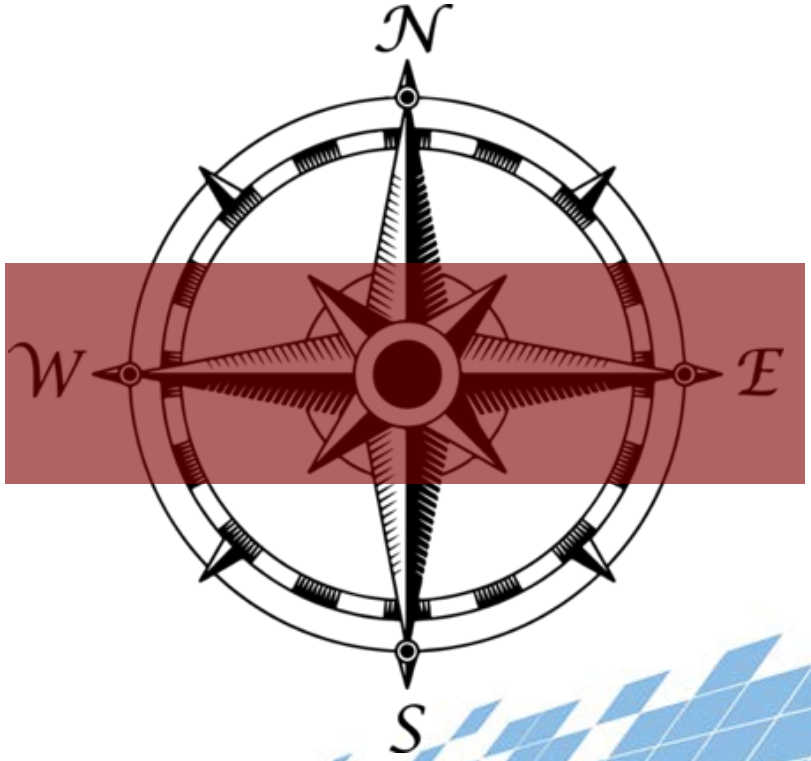
- North / South Traffic
  - Traffic entering from an external source into the virtual environment
  - This traffic may or may not go through other physical security equipment
  - Limit access to public facing applications and services
  - Only allow access on the protocols / ports needed
  - Inspect incoming requests for security risks and block any malicious traffic
  - Alert on malicious traffic



SPIRENT

The Borderless Infrastructure

- East / West Traffic
  - Communications between virtual machines in different port groups or security zones
  - Virtual machines can reside on the same virtual host or different virtual hosts
  - Limit what applications or services can communicate between security zones
  - Confirm this traffic is the actual application
  - Inspect this traffic for security risks



SPIRENT

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

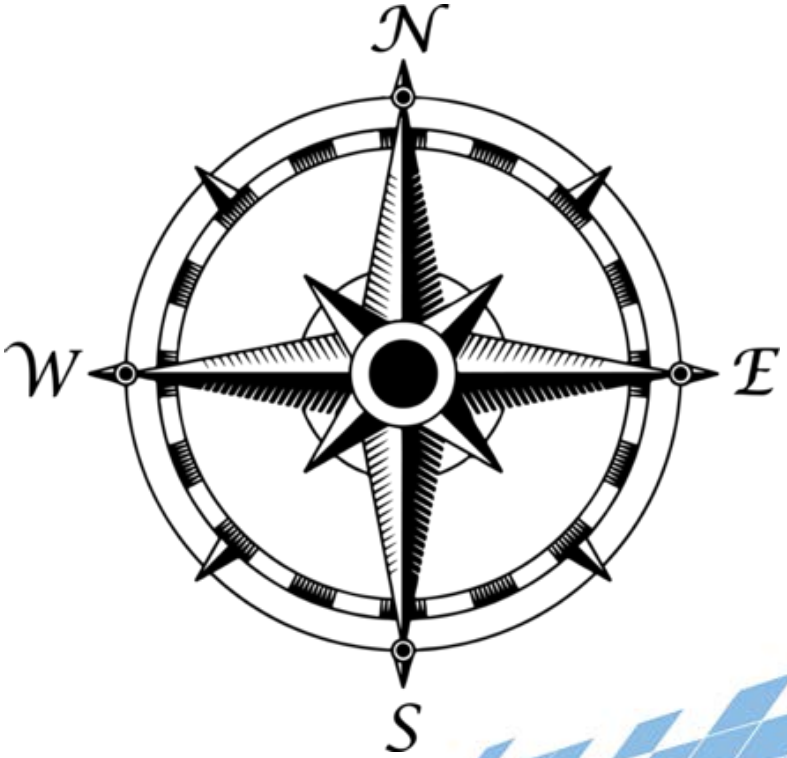
Validating the Security of This New Infrastructure

#RSAC

SPIRENT

Validating the Security of This New Infrastructure

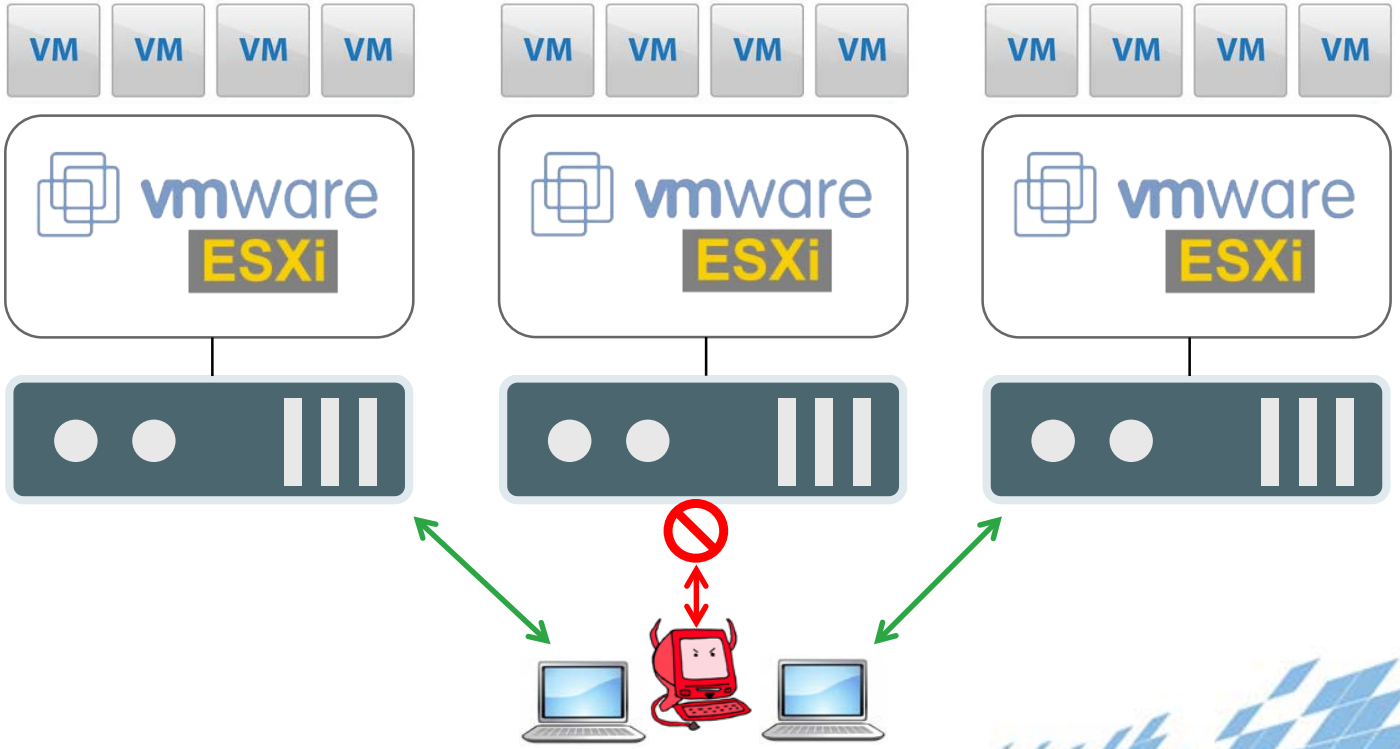
- Confirm only allowed traffic enters protected zones
- Confirm unwantedd traffic, whether by policy or malicious, is blocked from entering protected zones
- Measure impact of different types of policies
  - Time to first byte
  - QoS impacts in deployment
- Test how performance is impacted by the hypervisor deployment
  - Configuration of hypervisor
  - Different hypervisors



SPIRENT

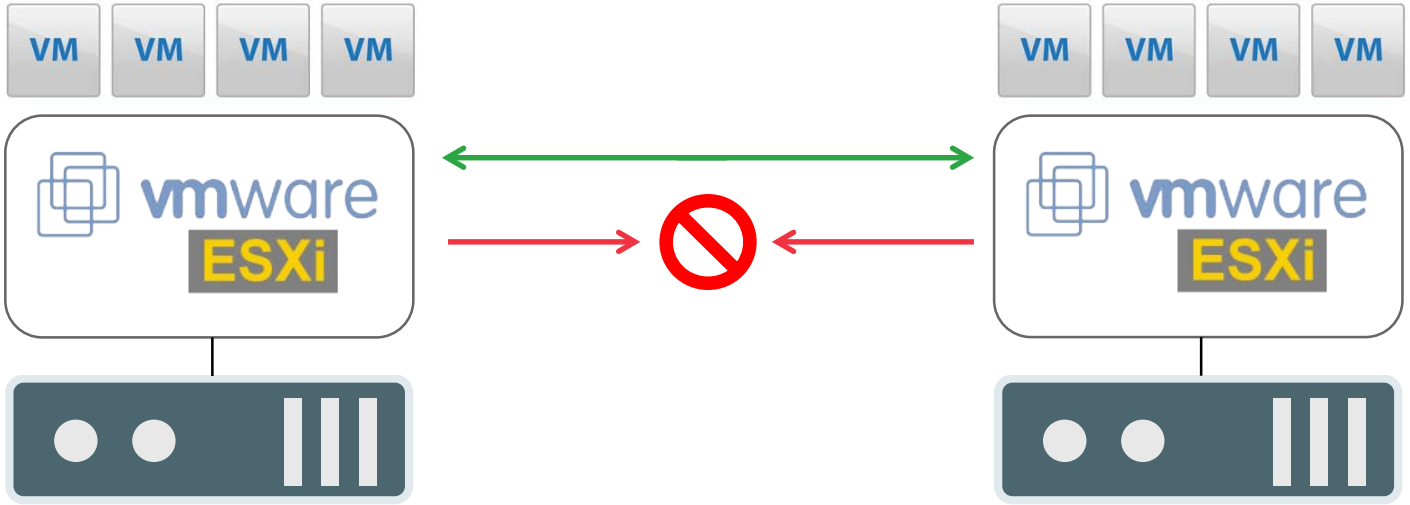
Validating the Security of This New Infrastructure

- North / South Testing



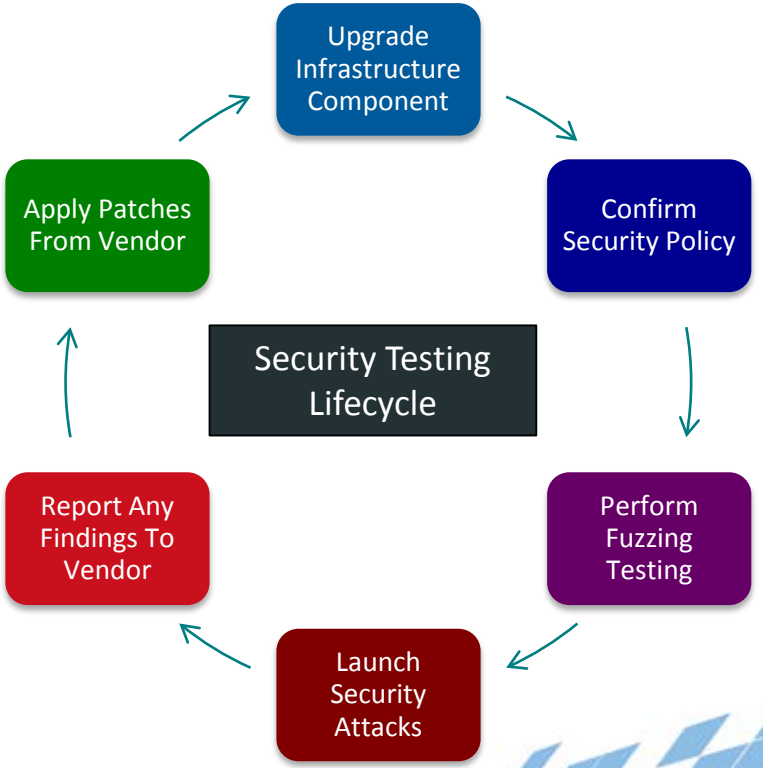
Validating the Security of This New Infrastructure

- East / West Testing



Validating the Security of This New Infrastructure

- Security Testing Lifecycle
  - Upgrade component
  - Confirm policy is still working as expected
  - Fuzz critical protocols to confirm stability
  - Launch security attacks (all directions)
  - Report found issues to product vendor
  - Apply patches provided by product vendor
  - Repeat process



SPIRENT

Key Takeaways

- The movement to virtual is increasing the threat landscape
  - DDoS
  - Malware
  - Exploits
- It is important to test all avenues for traffic
  - North / South
  - East / West
- Confirm only allowed, legitimate traffic is crossing through protected zones
- Only use testing solutions that provide a holistic view

SPIRENT

Apply What You Learned Today

- Next week you should
  - Identify the critical paths within your virtual deployments (North / South, East / West)
  - Confirm only allowed traffic traverses security policies into protected zones
- Over the next four weeks you should
  - Implement the security testing lifecycle within your organization
  - Begin collecting metrics on
    - efficacy of your security policies (i.e., are there holes you are unaware of?)
    - product updates (i.e., security efficacy, critical performance metrics)
- Over the next three months
  - Fully integrate security testing lifecycle within your organization
  - Begin reporting on how your organization is doing with its virtual security

SPIRENT

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Thank You!

#RSAC

SPIRENT

@david_desanto

https://www.linkedin.com/in/ddesanto