Network Virtualization

To Enhance Visibility and Containment

Bruno Germain ccie,cissp
Staff Engineer
Network Virtualization and Security

vmware

Agenda

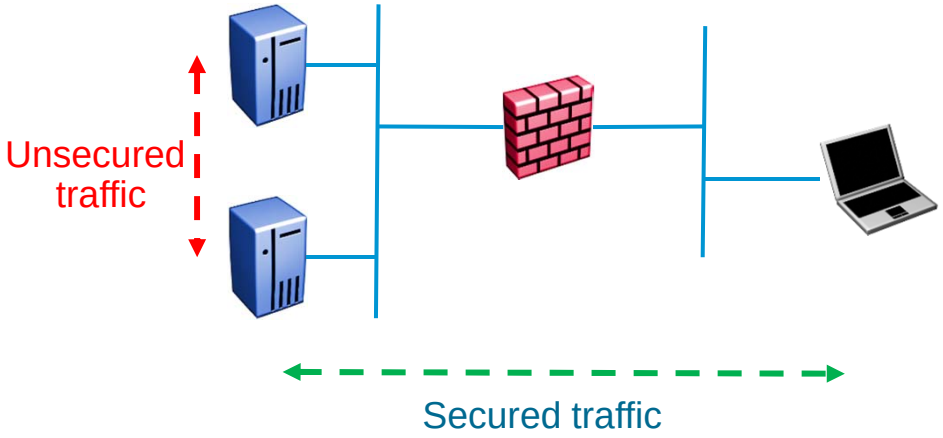
- Objectives:
  - Provide feedback from designing and implementing SDN in the field – DC Centric
    - Hint: it's not about Openflow, OpenDaylight, ACI, NSX, etc.
  - Have an architecture talk around network security and how SDN and virtualization provides new opportunities

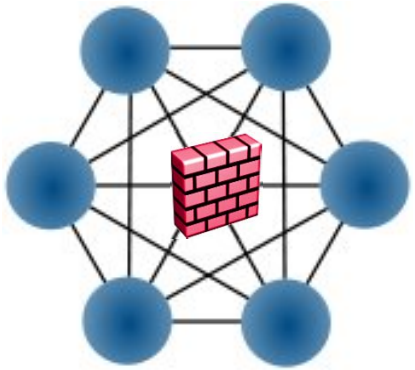
- Broad problem statement: why is network security moving into the virtual realm ?
- Narrowing it down: Threat Analysis for better security… not really a technology problem
- An example
- On the horizon

- Disclaimer: I work for Nicira / VMware. References to products are to illustrate the concepts

A fundamental truth

- **If you do not inspect your traffic, it is not secured**
  - You are ”blind” and have no way of detecting malicious activity
  - You defined an “attack surface” for attackers to take advantage of
  - You are accountable… even if you have no idea what is happening

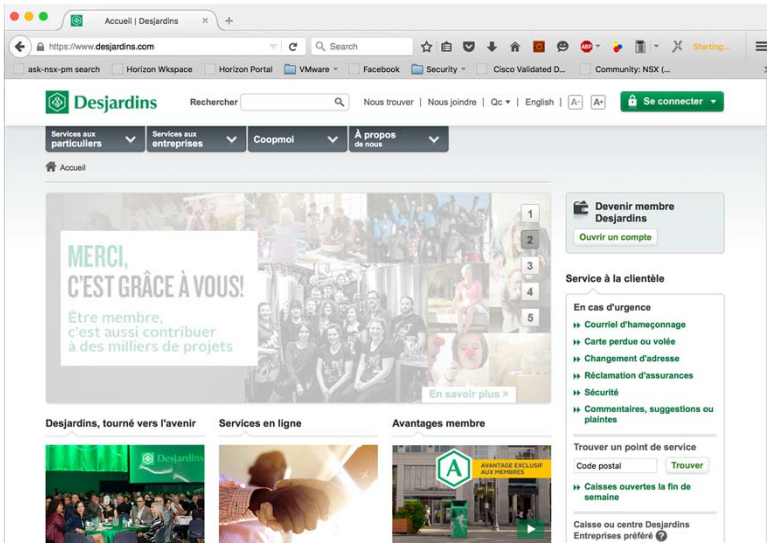




vmware

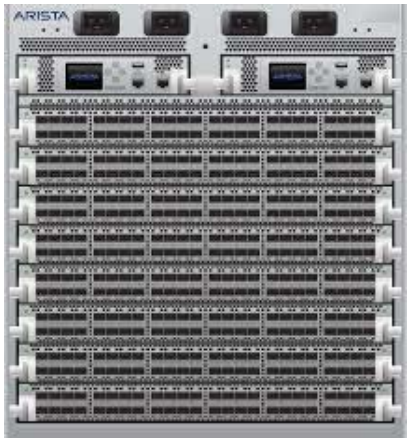
Game 1: Defining the new attack surfaces

- Where is my applications? :
  a. In my local data center
  b. In my alternate data center
  c. In a cloud provider infrastructure
  d. Partially here, at a partner, in the cloud
  e. All of the above
- The notion of trust based on a location, a device or a network loses all meaning
- Static perimeters where we are mapping VMs are breaking in the face of virtualization
  - Security must follow the application not the other way around
  - Impossible to use an IP address or a Vlan to represent an application anymore



Attack surface = the diameter of uninspected traffic… smaller is better !
Q: Where do you put your security controls ?

Game 2: Building a DC with the idea of inspecting all traffic
(the basis of micro-segmentation)

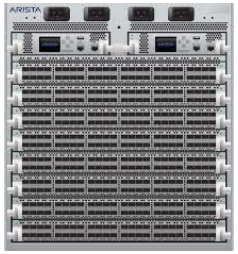


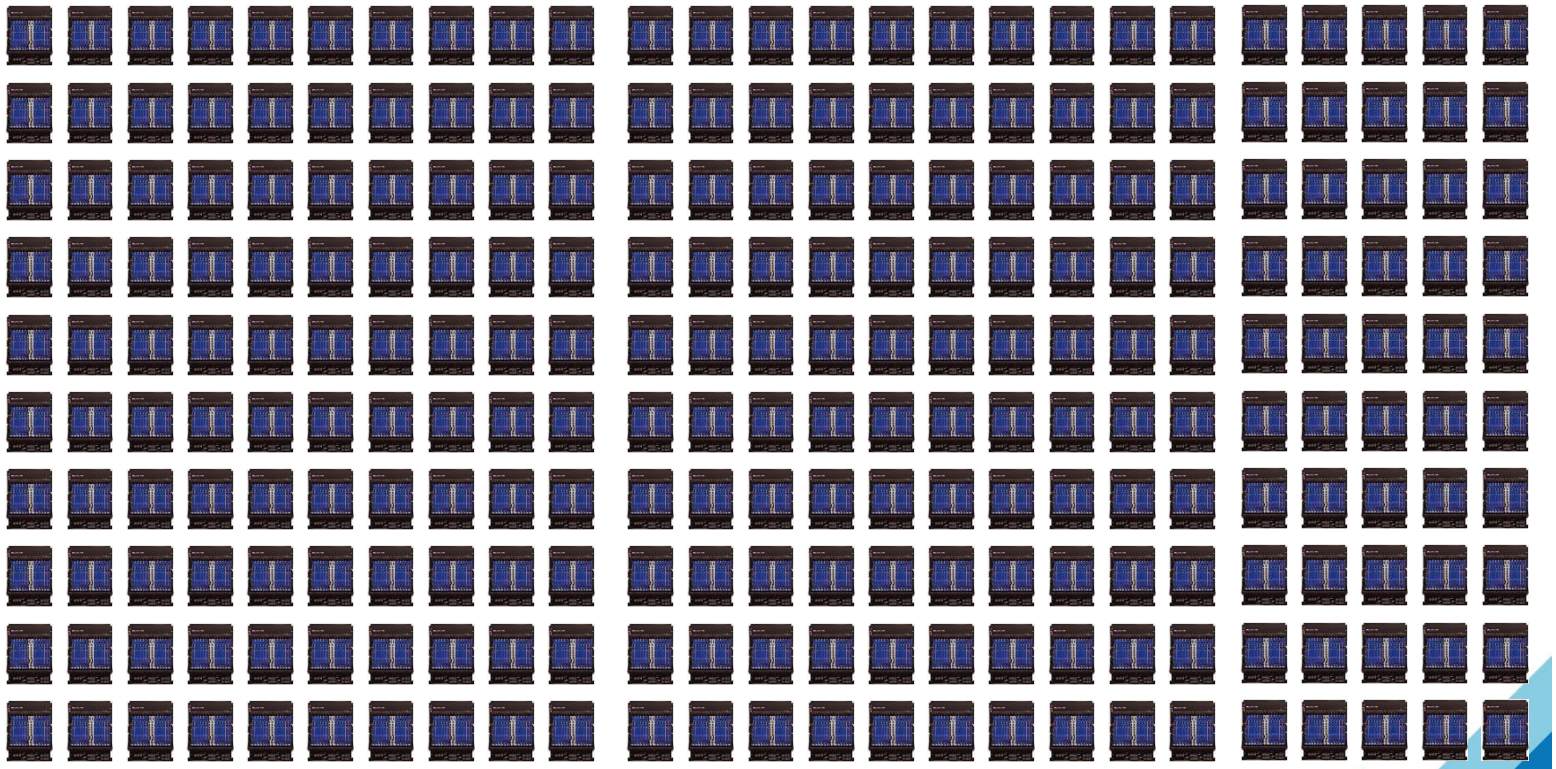
Arista 7508
- 1152 ports 10GE
- 288 ports 40GE
- 30 Tbps total

CheckPoint 61000
- Up to 60 ports 10GE
- Up to 8 ports 40GE
- Up to 120 Gbps production traffic

Q: How many 6100 do I need to inspect all the traffic from a single 7508 ?

Reaching the limits of physical centralized / inline solutions





Solving the Complexity In Data Center Networks

- End-To-End Principle (Saltzer, Reed & Clark – 1981, MIT)
  - The end-to-end principle states that application-specific functions ought to reside in the *end hosts* of a network rather than in *intermediary nodes*

- Q1: where do we put Firewalls in the Internet ?

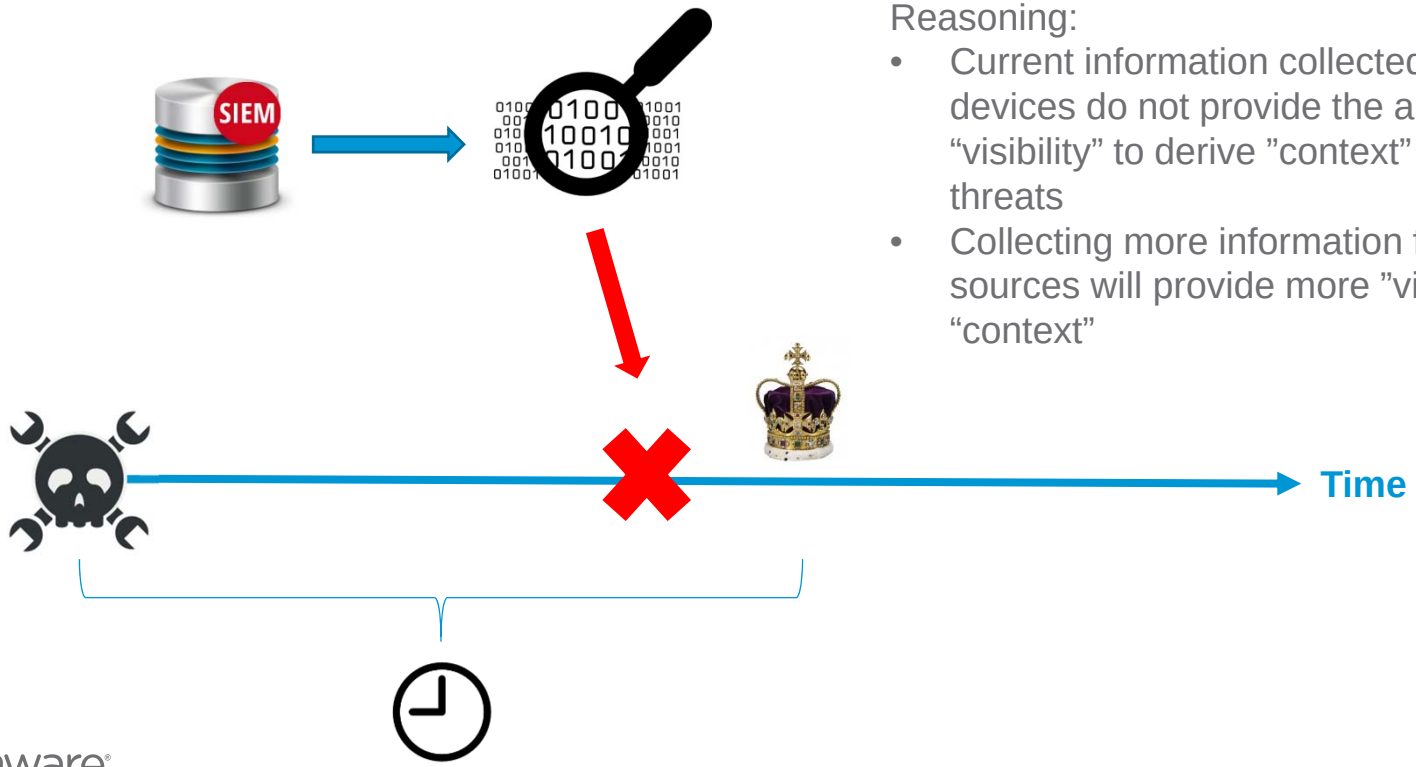
- Q2: which elements during a file transfer or while browsing a web site controls the amount of data being sent, notices errors and corrects them by re-transmitting the data, etc ?

- Q3:what is the role of the Internet in the delivery of the services you get ?

DC networks do not respect the end-to-end principle thus driving complexity in the network
To solve the complexity problem, we need to push the network services to the edge

Need to solve the operational problems of a distributed system

Threats Analysis Assumptions



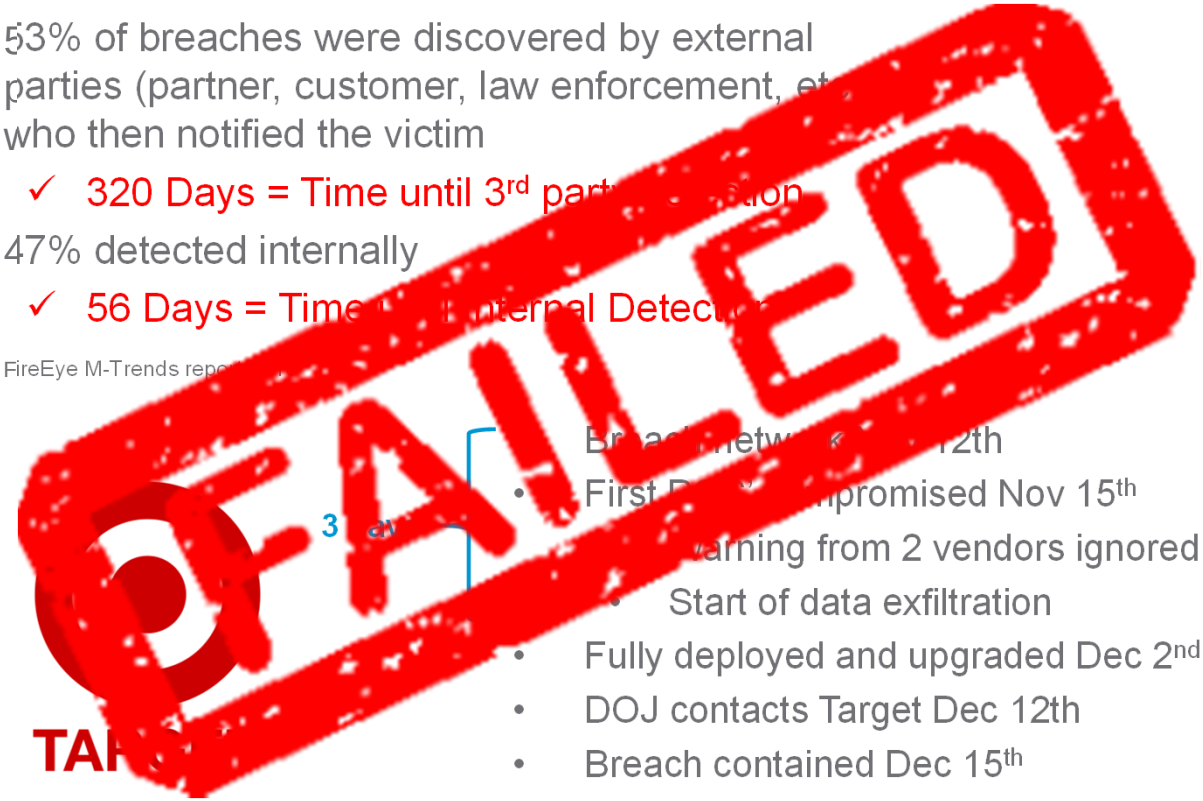
Reasoning:

- Current information collected by security devices do not provide the appropriate “visibility” to derive ”context” and identify threats
- Collecting more information from diversified sources will provide more ”visibility” and “context”

A Reality Check

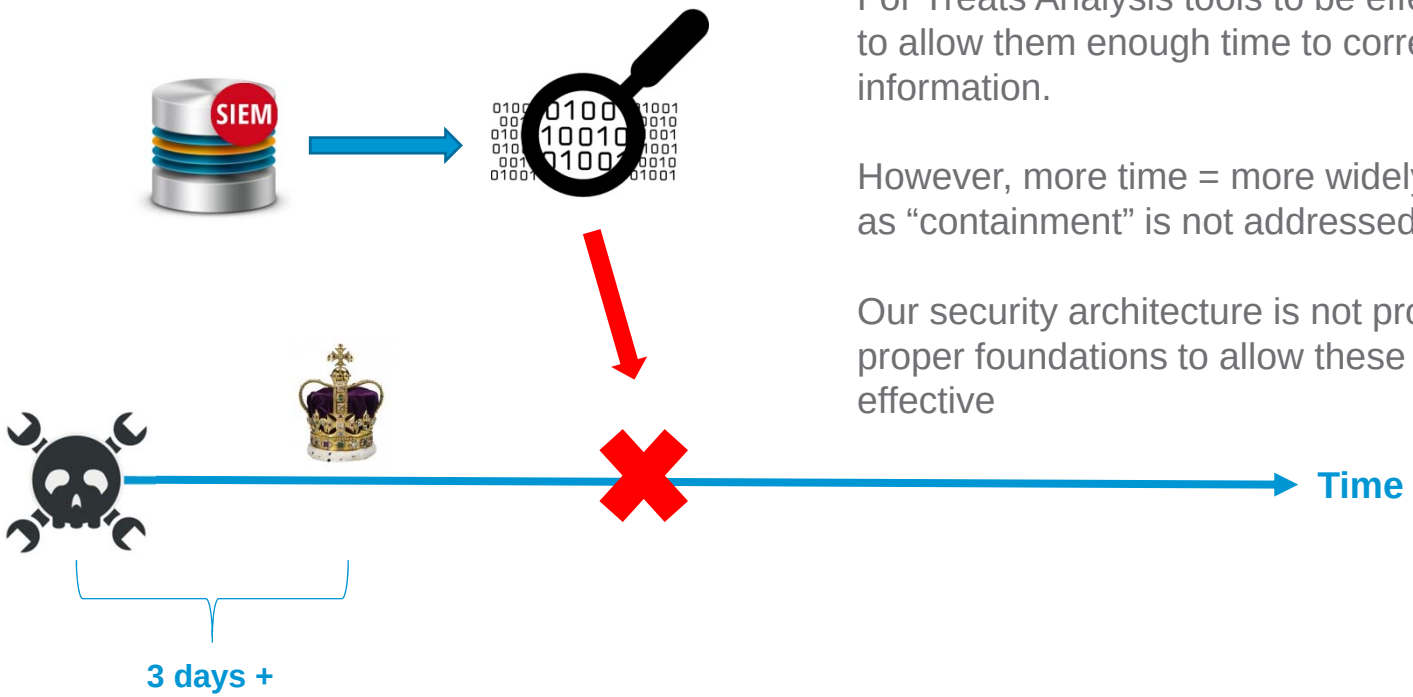
- 53% of breaches were discovered by external parties (partner, customer, law enforcement, et… who then notified the victim
  - ✓ 320 Days = Time until 3rd part… tion
- 47% detected internally
  - ✓ 56 Days = Time … nternal Detec…

Source: FireEye M-Trends repo…



- Br… netw… 12th
- First … mpromised Nov 15th
  - …arning from 2 vendors ignored
  - Start of data exfiltration
- Fully deployed and upgraded Dec 2nd
- DOJ contacts Target Dec 12th
- Breach contained Dec 15th
- 40M credit cards & 70M client records

Threats Analysis Trend In Reality

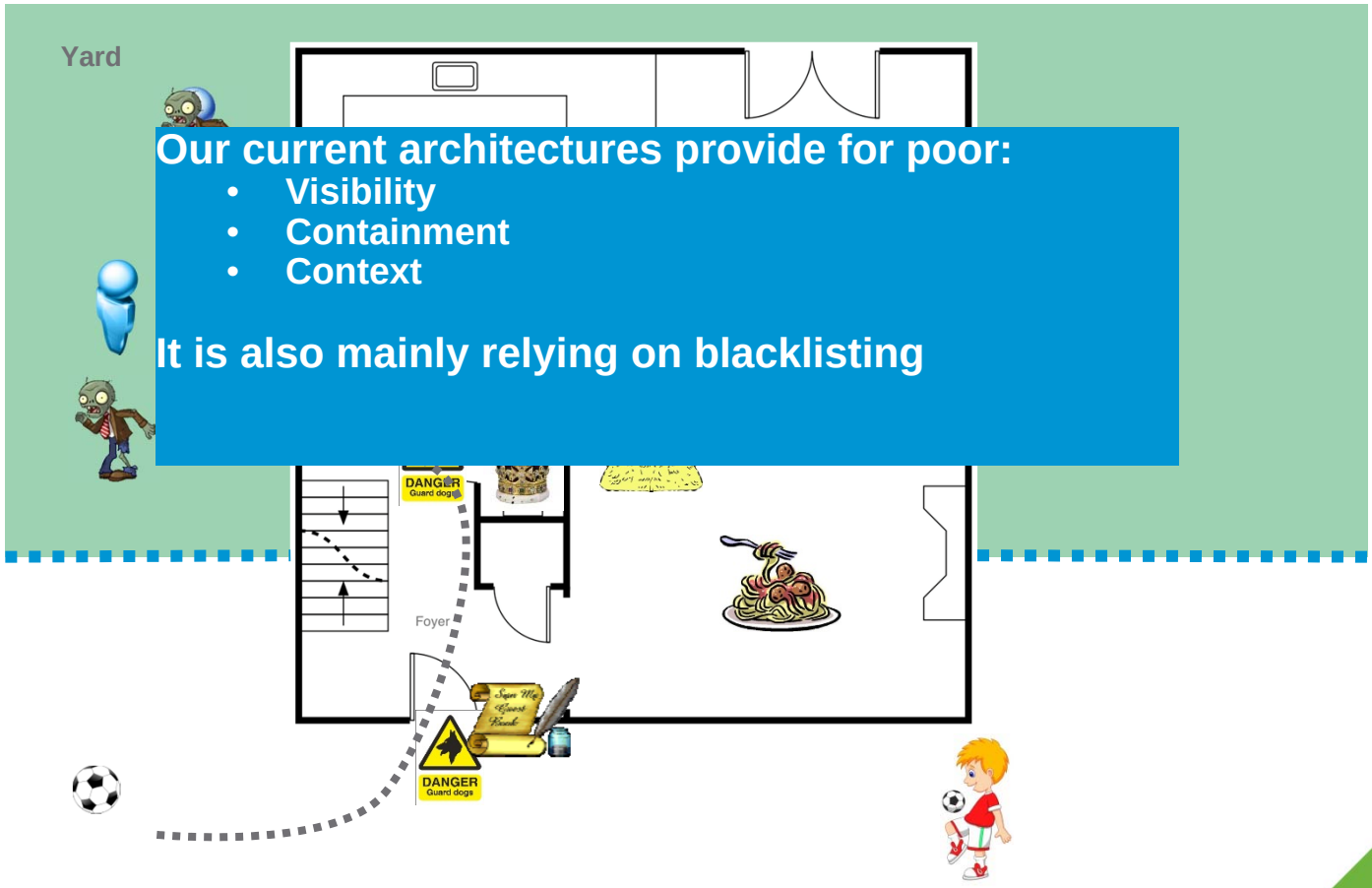


For Treats Analysis tools to be effective we need to allow them enough time to correlate the information.

However, more time = more widely compromised as “containment” is not addressed

Our security architecture is not providing the proper foundations to allow these tools to be effective

Anatomy Of An Attack

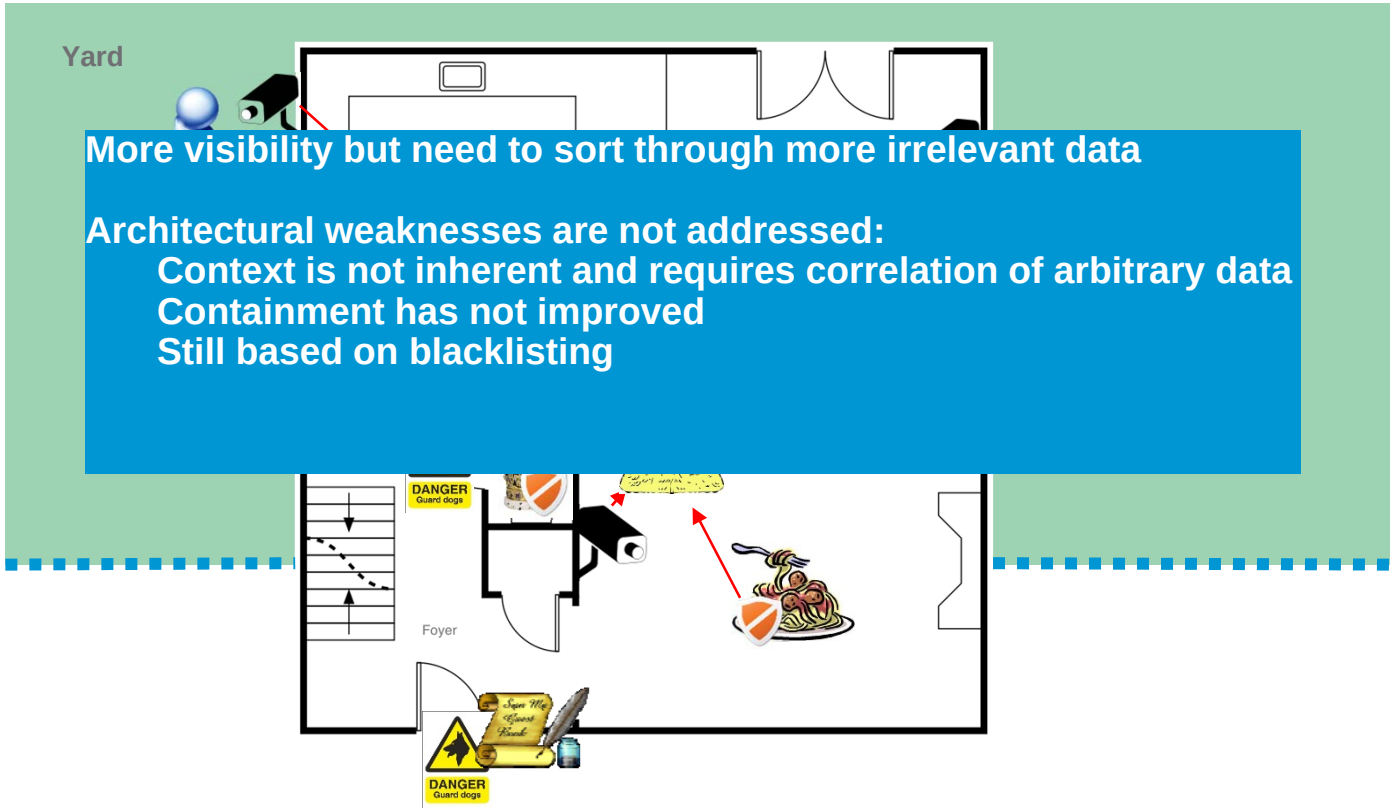


Our current architectures provide for poor:

- **Visibility**
- **Containment**
- **Context**

It is also mainly relying on blacklisting

Our Current Response



IEEE COMMUNICATIONS SOCIETY

Context

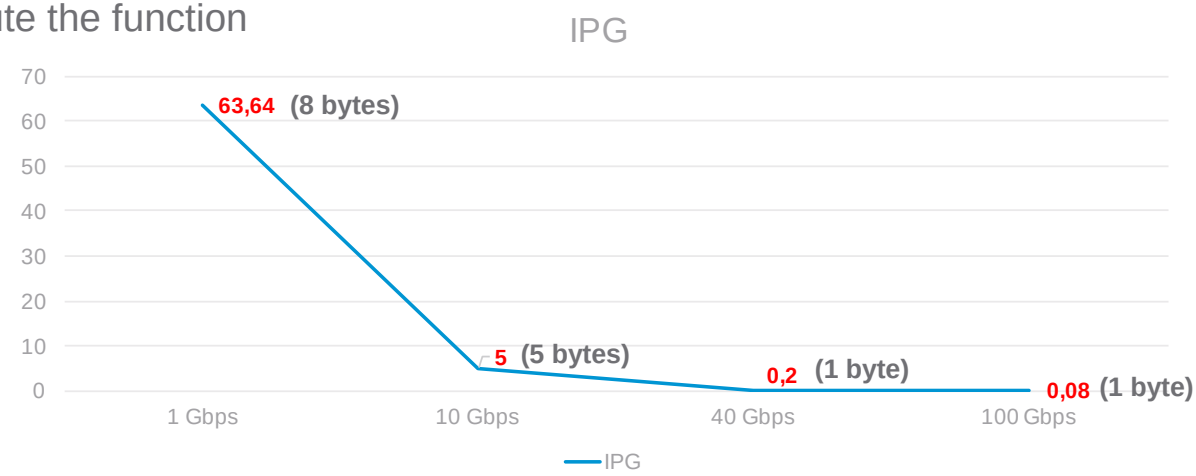
- Meaningful information related to the state of the application or its communications
- Naturally achieved by grouping element with similar attributes
  - Member of a particular application, a compliance zone, administrative domain, same function, etc.
- Traditionally achieved through segmentation
  - DMZ, DB segment, VoIP, common, etc.

- Issues & limitations
  - Tied to physical infrastructure and cannot extend easily to different physical environments
  - The “reason” for segmenting does not propagate as information in events
  - Events cannot be ascertained positively as threats, more data is required
  - Multifaceted context cannot be build: How do you segment for ”a public web server part of Application-A and administered by Admins-Z” ?

vmware

Visibility

- You cannot “see” what you do not capture or inspect
  - Inline inspection of the aggregate DC traffic in hardware devices is unfeasible
  - Need to distribute the function



- Sending more ”hay”, ie irrelevant events to the SIEM, requires more efforts and time
  - ***A whitelisting / least privilege model would generate significantly less events and eliminate false positive***

IEEE COMMUNICATIONS SOCIETY

Containment

- The ideal situation
  - A system gets breached
  - The attack is contained in the compromised system until the threat analysis tools figure out something is wrong
- The reality
  - Lateral movement is relatively easy as the infrastructure is exposed in the system
  - Endpoint protection is really good with known attacks, not so good with new ones
  - Very few know and lock down the processes required on a system
  - Treat analysis is done off board on groups of system or requires trending over time to be analyzed mostly by humans
- An attacker has a good window of opportunity and a large attack surface by design

vmware

IEEE COMMUNICATIONS SOCIETY

Whitelisting / Least Privilege

- Do you know what is running in your Data Center ?
- Do you know which system should talk to which other system over which channel ?
- Do you know who should be accessing these systems ?
- Do you understand how information flow across particular applications ?
- Do you know what should exit your company, by who, to who ?
- Etc.

- For most organizations, the answer to these questions is no.
- Therefore we fall back on a blacklisting model
  - Block known threat and assume the rest is ok… log and hope for the best.
  - No easy way to implement whitelisting until now

vmware

Whitelisting / Least Privilege

IEEE COMMUNICATIONS SOCIETY

vmware

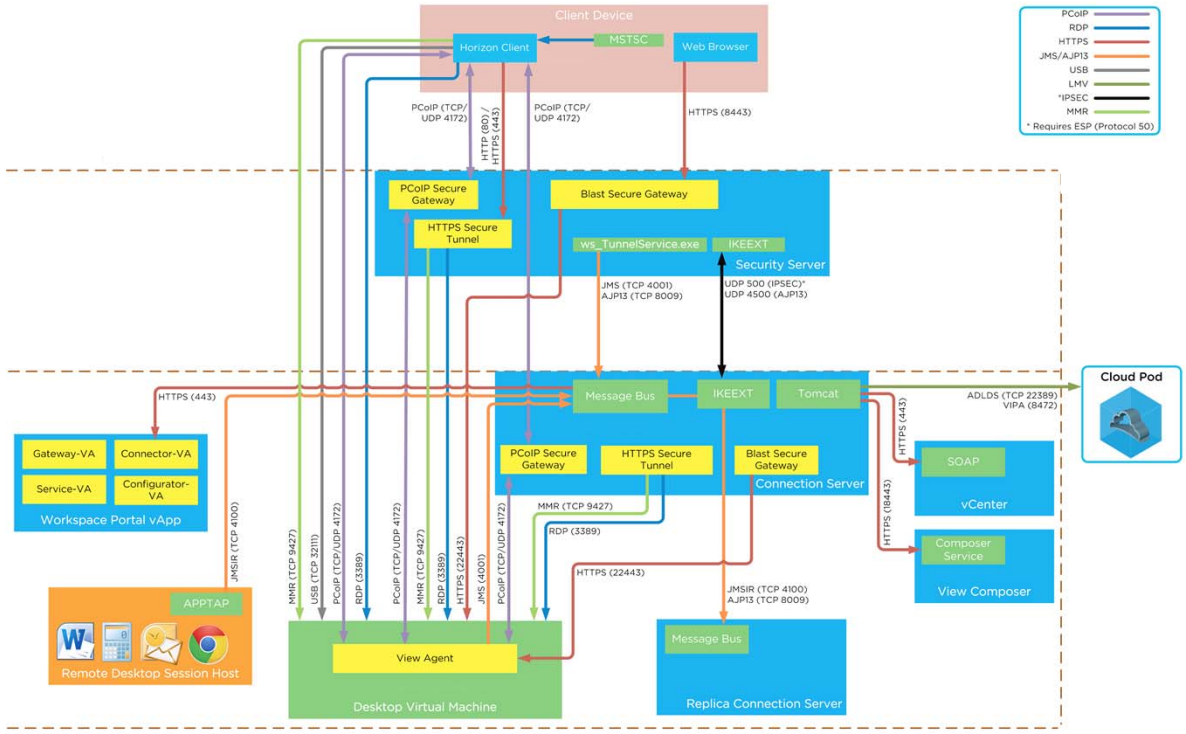
What Does Software Defined Networks Bring ?

- It dissociates the infrastructure from the services it delivers
  - If this would be a privacy talk, we would say that we have dissociated your identity from your home address, phone number, etc.
  - Extensible to clouds / multi-site scenarios and third party integration
- Segmentation boundaries are what you want them to be
  - An admin group, a compliance scope, a security zone, etc or all of the above
  - ***This brings context***
- It removes the services from the core of the network to ”split and smear” them granularly at each VM, container, etc
  - ***This brings visibility and enables whitelisting***
  - ***Network speed becomes irrelevant***
- Creates a “security control plane”
  - ***Enables declarative policies***
  - Enables new security model such as Zero Trust

Requirements For An Improved Security Architecture

- Adopt a whitelisting / Least Privilege model
  - Server virtualization and containers makes it feasible
  - Applies also to hypervisors that can be locked down and baselined for least privileges operation
  - Have tools that can create an application baseline
  - Simplified logic: Allow & monitor whitelisted traffic / drop & alert for anything else
    - All drop events are now 100% pertinent and threat analysis tools can concentrate on valid traffic being abused
  - Provides better containment by default
- Embrace network virtualization
  - Dissociate infrastructure from security requirements, ie don't base your security on IP addresses, subnets, Vlans, etc
  - Establish a central policy / security management plane
  - Distribution of security functions at every system providing true micro-segmentation

Horizon View Networking – flows and protocols



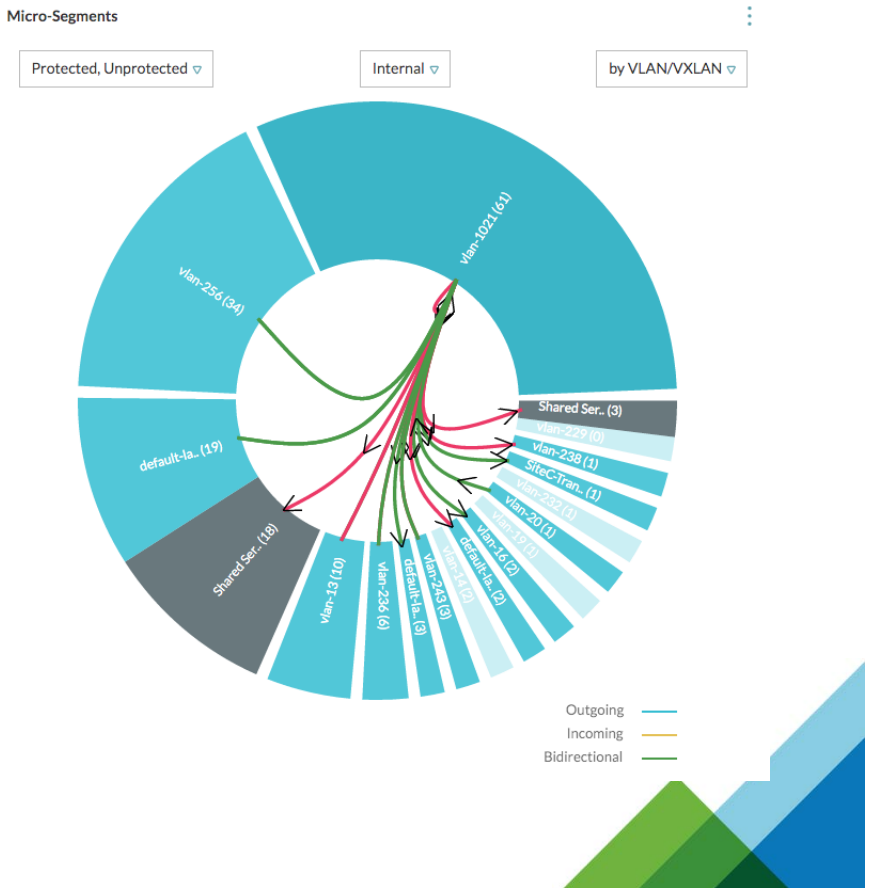
Source Ray Heffer
http://blogs.vmware.com/consulting/2014/06/vmware-horizon-6-view-firewall-network-ports-visualized.html

Horizon 6 Services (partial)

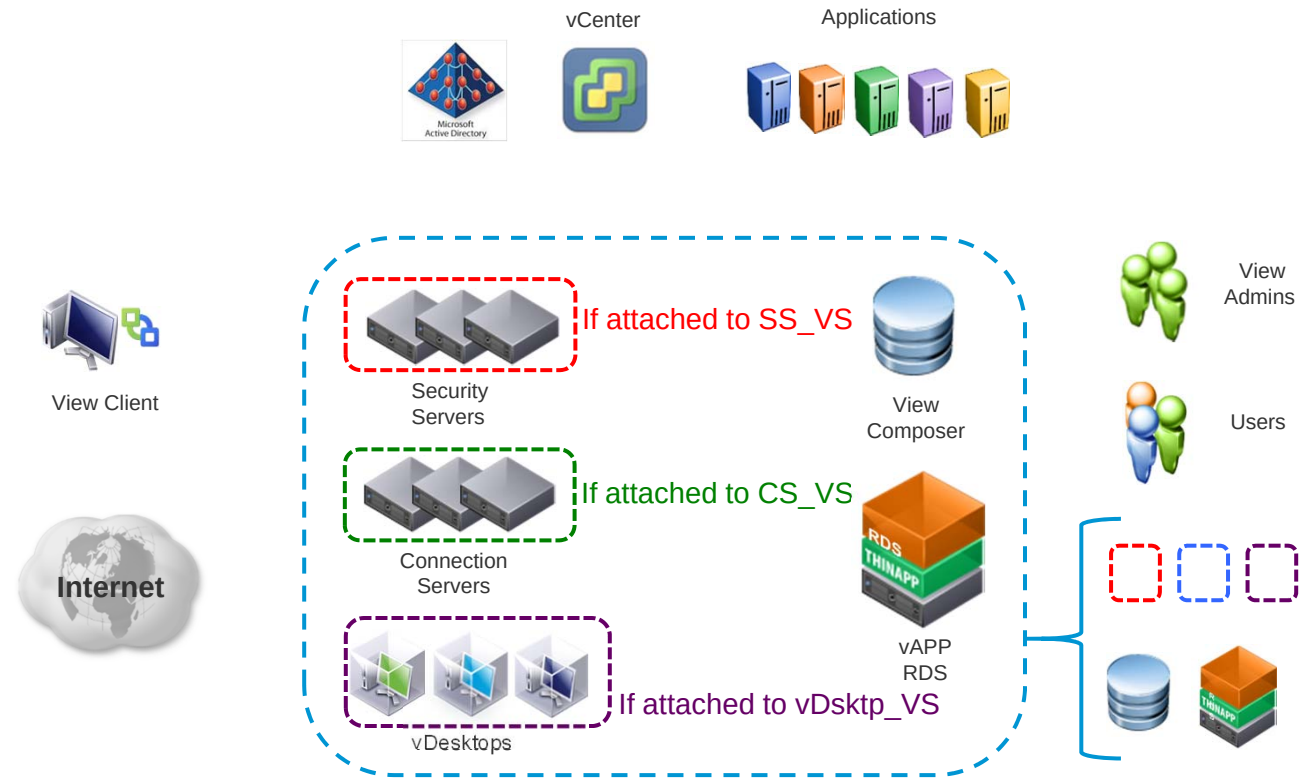
Horizon Service	Protocol	Destination ports	Source	Description
Horizon6-Agent	TCP	4172,3389,9427,32111,22443	any	PCoIP,RDP,MMR,USB redirection
Horizon6-ComposerService	TCP	80,443,18443	any	Secure connection between composer service and connection servers
Horizon6-CS_inbound_client	TCP	4172	any	Client connections to internal connection server
Horizon6-CS_inbound_client2	UDP	4172	any	If PCoIP secure gateway is used
Horizon6_interCS	TCP	4001,4100,8009	any	CS to CS traffic
Horizon6_SS_to_CS_1	TCP	4001, 8009	any	SS to CS traffic
Horizon6_SS_to_CS_2	UDP	5,004,500	any	SS to CS traffic
Horizon6_SS_to_Agent_1	TCP	4172, 9427, 3389, 22443, 4001	any	SS to agent
Horizon6_SS_to_Agent_2	UDP	4172	any	SS to agent

A Whitelisting Approach

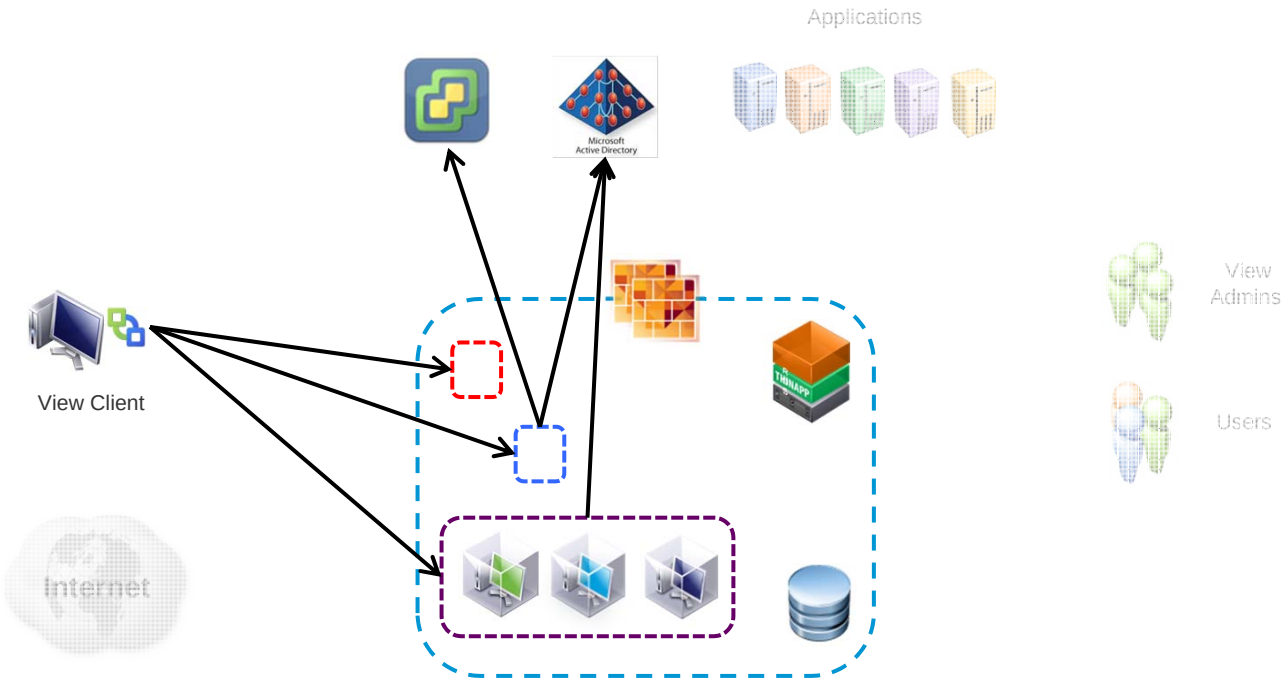
- Take your application one at the time and get a fingerprint of its communications:
  - The internal flows between the components of the application
  - The external flows to other systems in the data center
  - Who the users are and where they come from
- Establish how to group the components for the application
- Create your whitelist ruleset



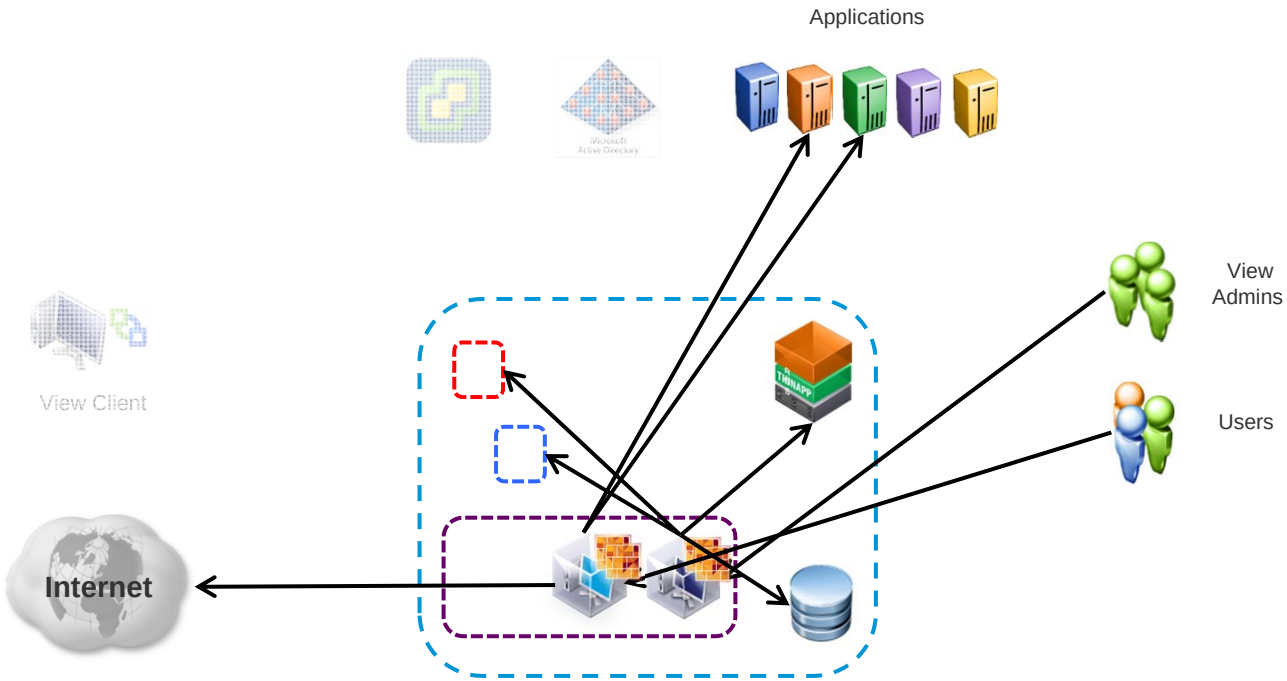
A Whitelisting Approach
The Horizon View "bubble" – Grouping by functions



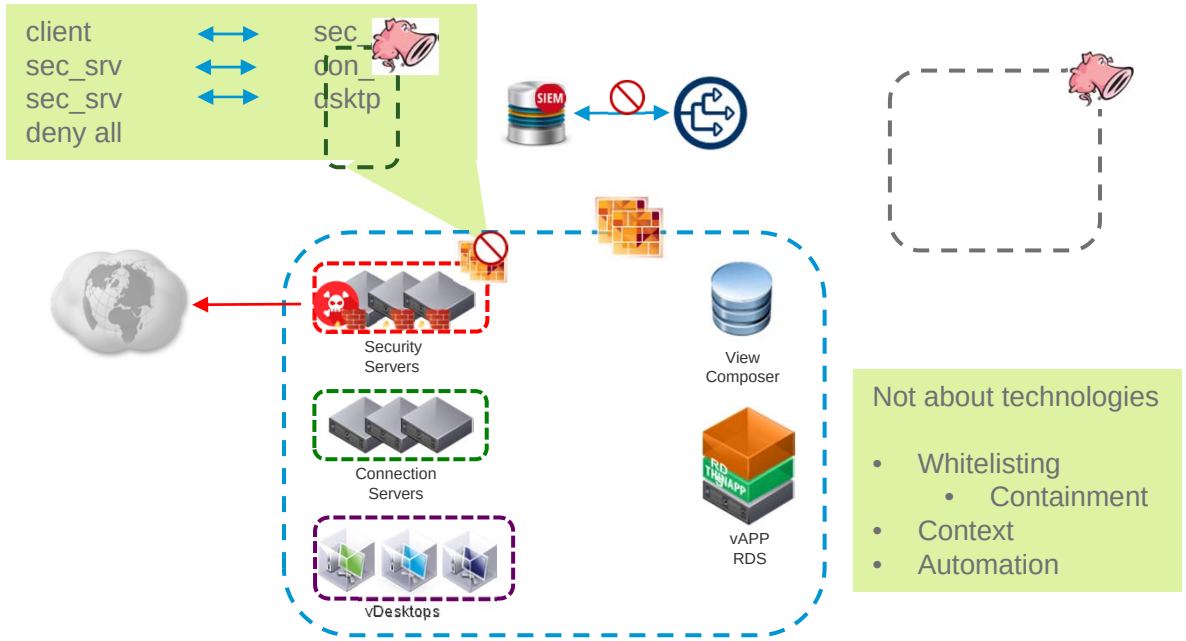
A Whitelisting Approach
Establishing the relationships - infrastructure



A Whitelisting Approach
Establishing the relationships - Applications



How Whitelisting Helps Contain Unknown Threats?

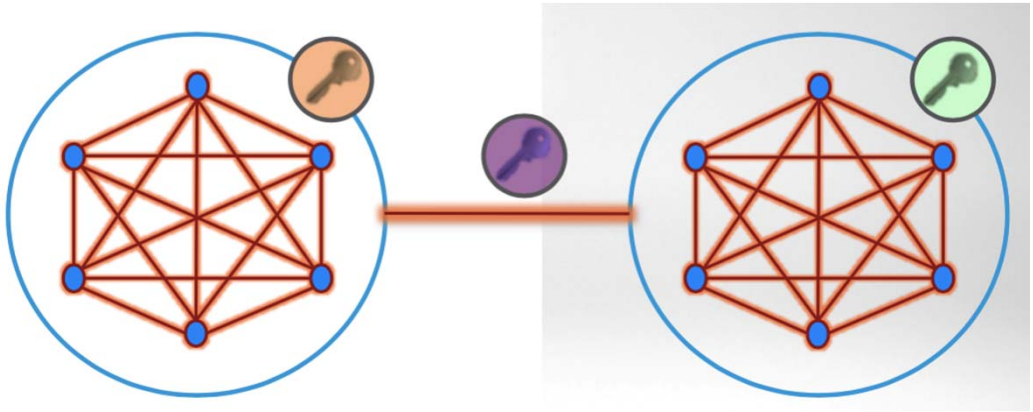


Not about technologies

- Whitelisting
  - Containment
- Context
- Automation

Extending To Communications

- Using the same grouping to ensure the proper system are the ones talking to each other
  - Encryption and / or authenticity and / or integrity
  - Protection against spoofing and eavesdropping
  - Denies any other source, any other communication channels
  - Done at the hypervisor so out of reach from the service itself
  - Key distribution, rotation and revocation managed by the same control plane



Extending To The Cloud – AWS Example

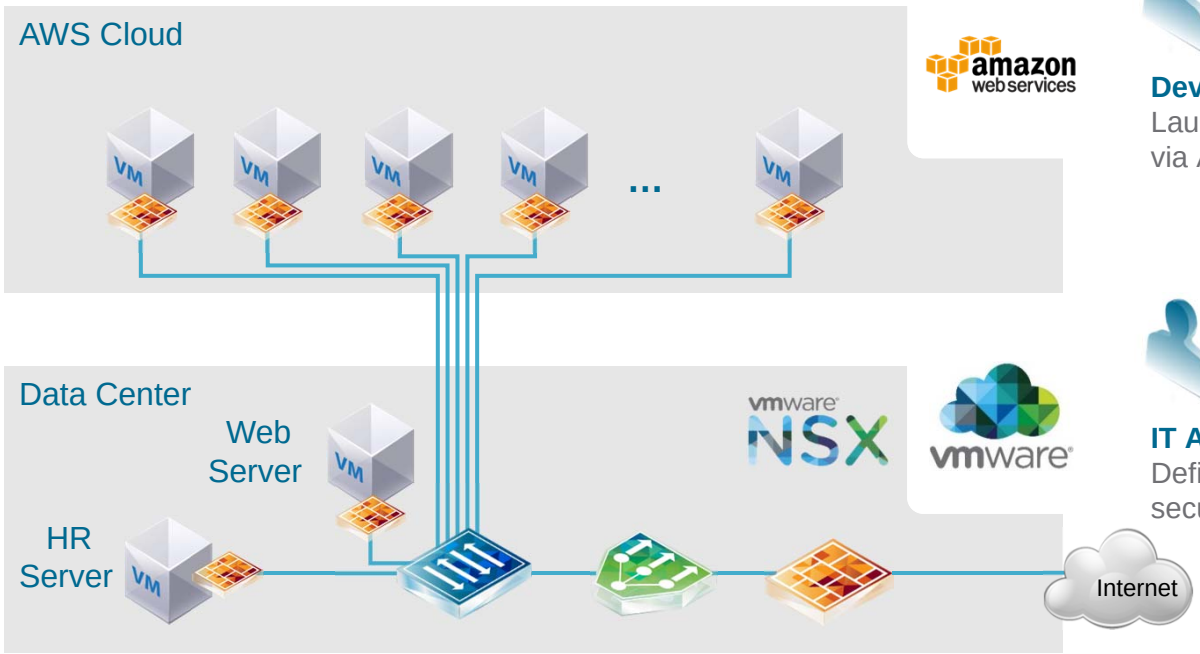
Native support for AWS instances with coherent services and security posture for on and off-premise

Amazon Web Services

- Native AWS Server instances (AMI's)
- Added to NSX virtual networks via policy

On-Premise NSX/vSphere

- AWS instances are added to logical switch
- Consistent security posture on-premise and in cloud
- AWS instances leverage services



Developer
Launches instances via Amazon console

IT Administrator
Defines network and security policy

IEEE COMMUNICATIONS SOCIETY

Summary

- Current threat analysis tools alone will not solve fundamental flaws in the way we architect our network security
- Virtualization in general and Network Virtualization specifically provides security properties that we were not able to get in the physical space
- Network Virtualization brings today
  - Better context
  - Better visibility
  - Better containment
  - Extensions to the cloud, multiple sites and to communications in general
- A security control plane
  - Tracks everything in the infrastructure
  - Translates declarative security into specific rulesets for the technology of your choice

vmware

All areas of research evolving rapidly… lots of opportunities

On a personal note…. We are expected to provide security

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY TRANSFORMATION DEVOPS BUSINESS HARDW

Security

152k cameras in 990Gbps record-breaking dual DDoS

Hacked low-powered cameras and internet-of-things things

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY TRANSFORMATION DEVOPS BUSINESS HARDWARE

Security

No wonder we're being hit by Internet of Things botnets. Ever tried patching a Thing?

Akamai CSO laments pisspoor security design practices

IEEE
COMMUNICATIONS
SOCIETY

Ever Wonder Why They Don’t Build These Anymore ?

vmware

Thank you

vmware