RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-R03

Automation and Virtualization Simplify Life: Can They Simplify Security?

Rob Randell

Director, NSBU System Engineering
Vmware

Hadar Freehling

Staff Security Strategist
Vmware
@dfudsecurity

#RSAC

What can we do today?

Security and Automation

- Policy - What do I allow or don’t allow?
- Triggers - Event, activity, baseline differentials, etc.
- Actions - Block, log, accept, etc..
- Timer - How long should the change last?
- Reset - What is post incident normal?

Security and Automation

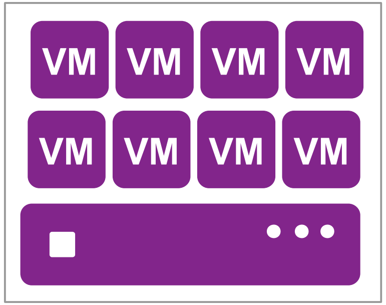
- Policy - No SSH within the Data center
- Triggers - SSH process started on a server
- Actions - Block traffic via firewall
- Timer - Check for alerts in near real time
- Reset - 5 minutes before firewall rule is removed

Demo

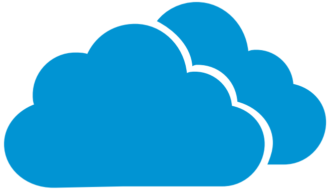
And now some history

Background on Virtualization

Server

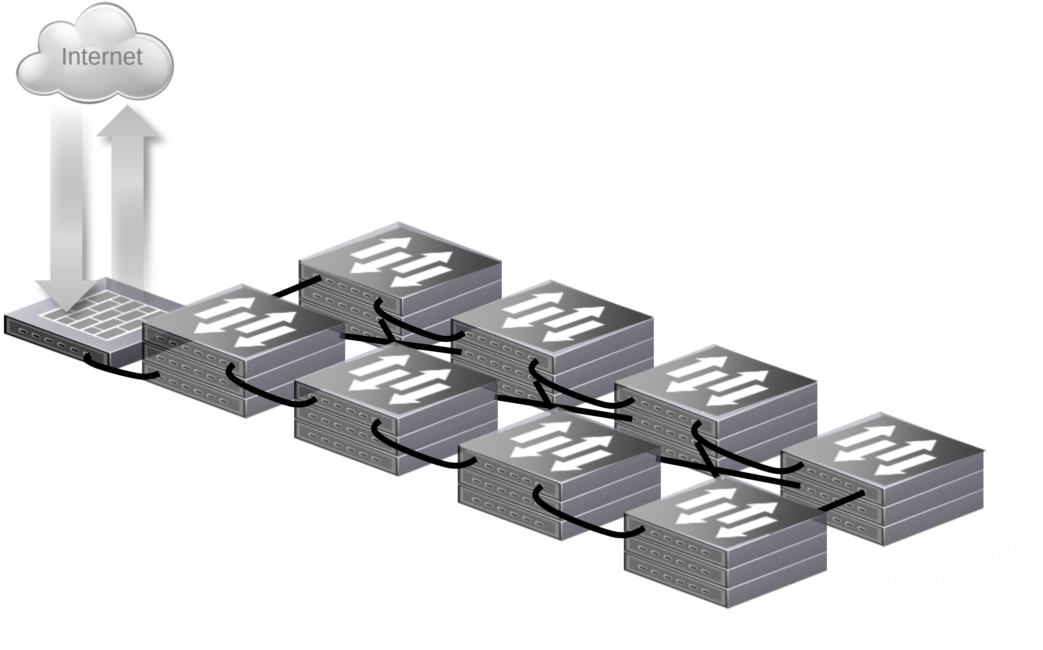


Virtual datacenter

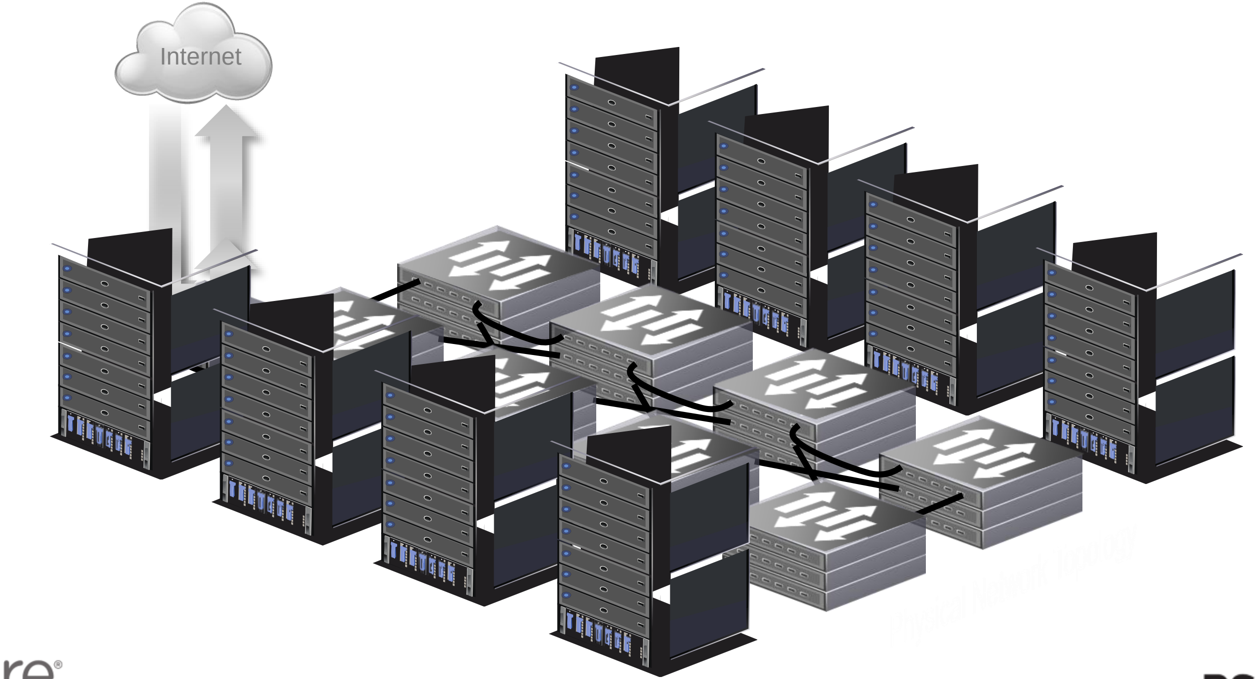


Virtual private cloud

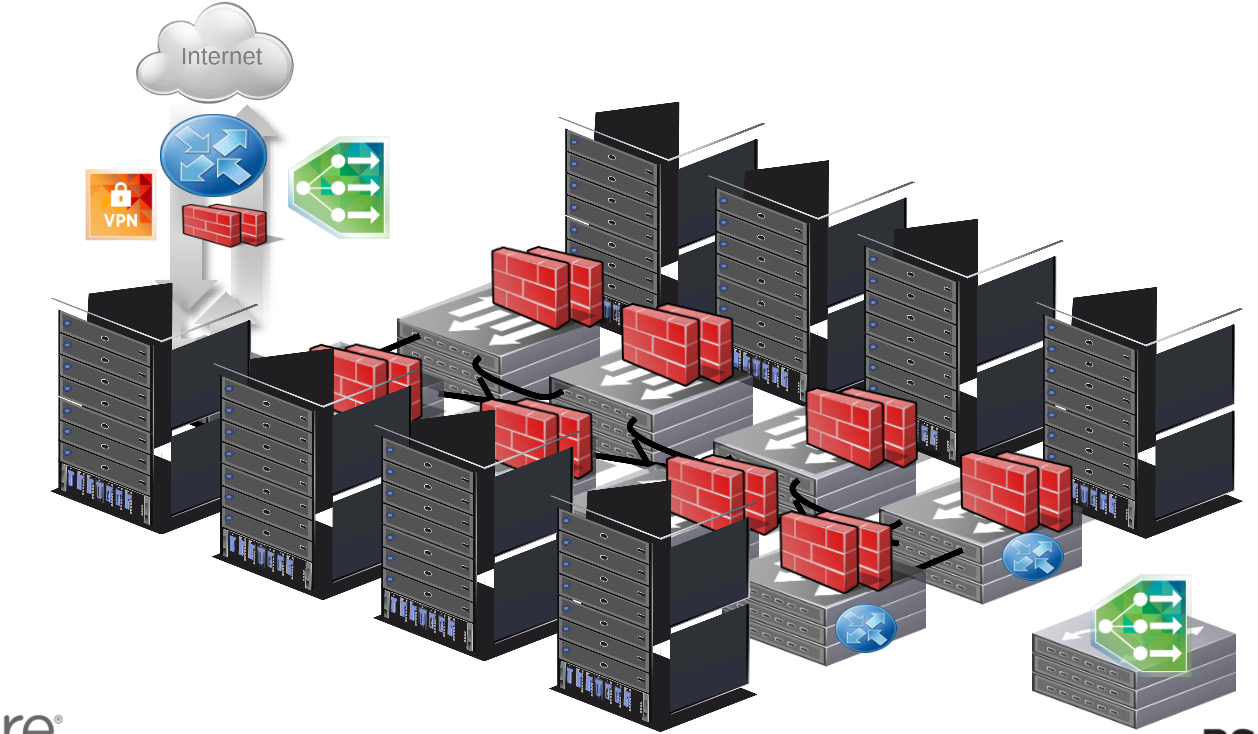
Laydown the Network



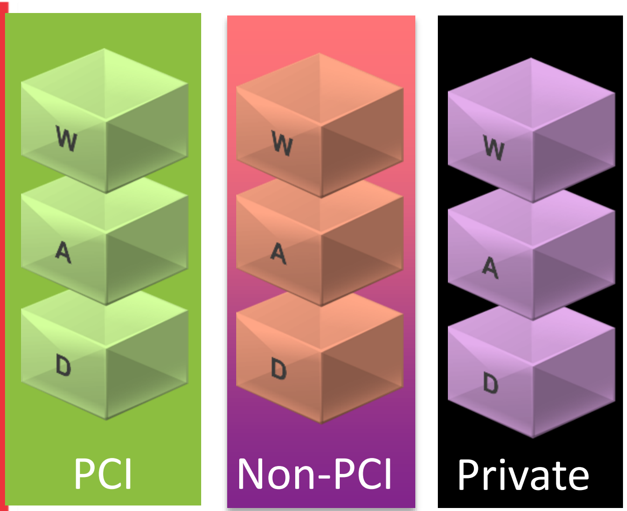
Add Compute



Now For The Complex Part



Mixing of Workloads

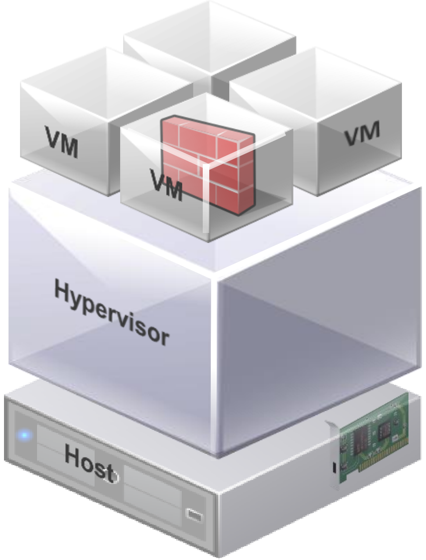


Compute and Automation

- Deploy from gold image
- PowerShell
- Scripts
- Puppet Chef
- Package deployments

Security and Virtualizing

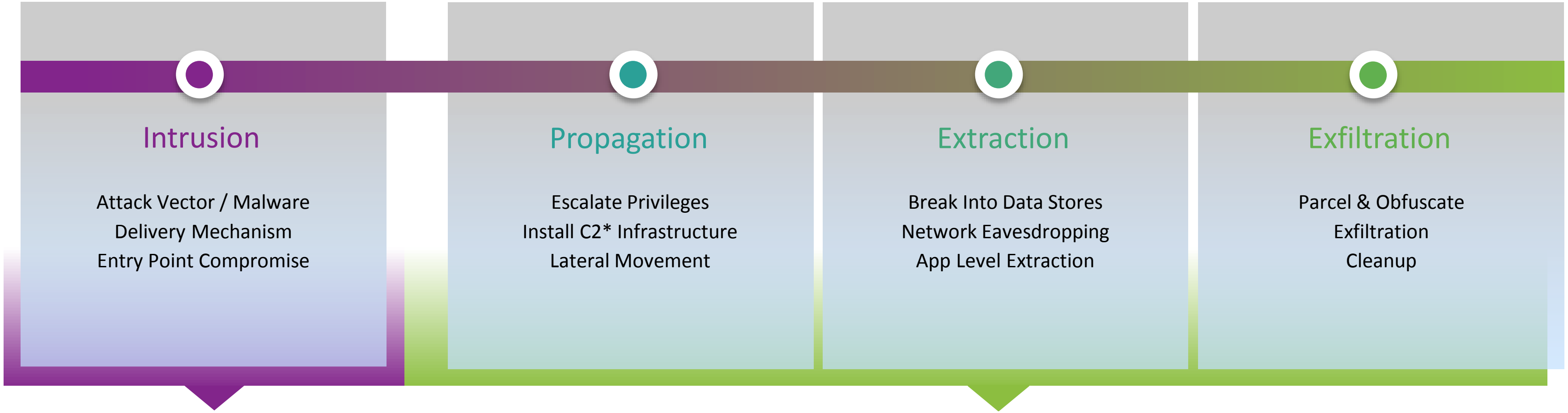
- Gen 1 virtual security
  - Virtual appliances – Functional, but limited
- Agentless AV
- Most enforcement still outside the virtual environment



“We cannot solve our problems
with the same way of thinking that created them.”

- Albert Einstein

Modern Attack: Targeted, Interactive, Stealthy



Intrusion

Attack Vector / Malware
Delivery Mechanism
Entry Point Compromise

Propagation

Escalate Privileges
Install C2* Infrastructure
Lateral Movement

Extraction

Break Into Data Stores
Network Eavesdropping
App Level Extraction

Exfiltration

Parcel & Obfuscate
Exfiltration
Cleanup

Stop Infiltration

80% of the investment is focused on preventing intrusion

The attack surface is simply too wide

Stop Exfiltration

20% of the investment is focused on addressing propagation, extraction and exfiltration.

Organizations lack the visibility and control inside their data center

Modern Attack: Targeted, Interactive, Stealthy

Intrusion

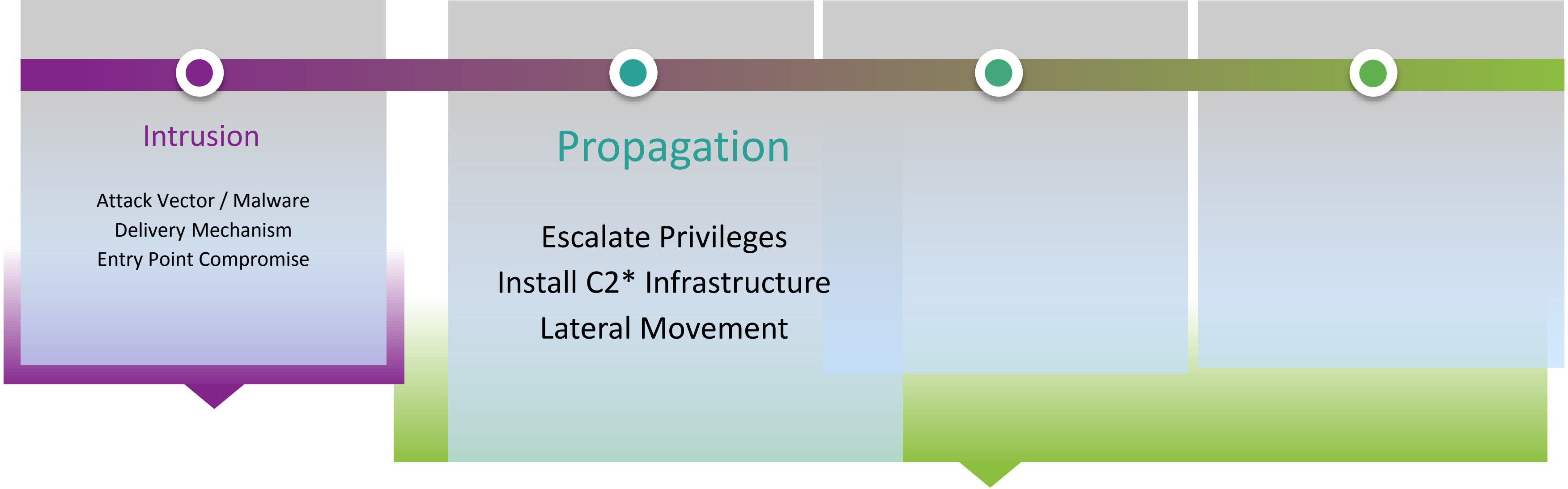
Attack Vector / Malware
Delivery Mechanism
Entry Point Compromise

Stop Infiltration

80% of the investment is focused on preventing intrusion

The attack surface is simply too wide

Modern Attack: Targeted, Interactive, Stealthy



Intrusion

Attack Vector / Malware
Delivery Mechanism
Entry Point Compromise

Propagation

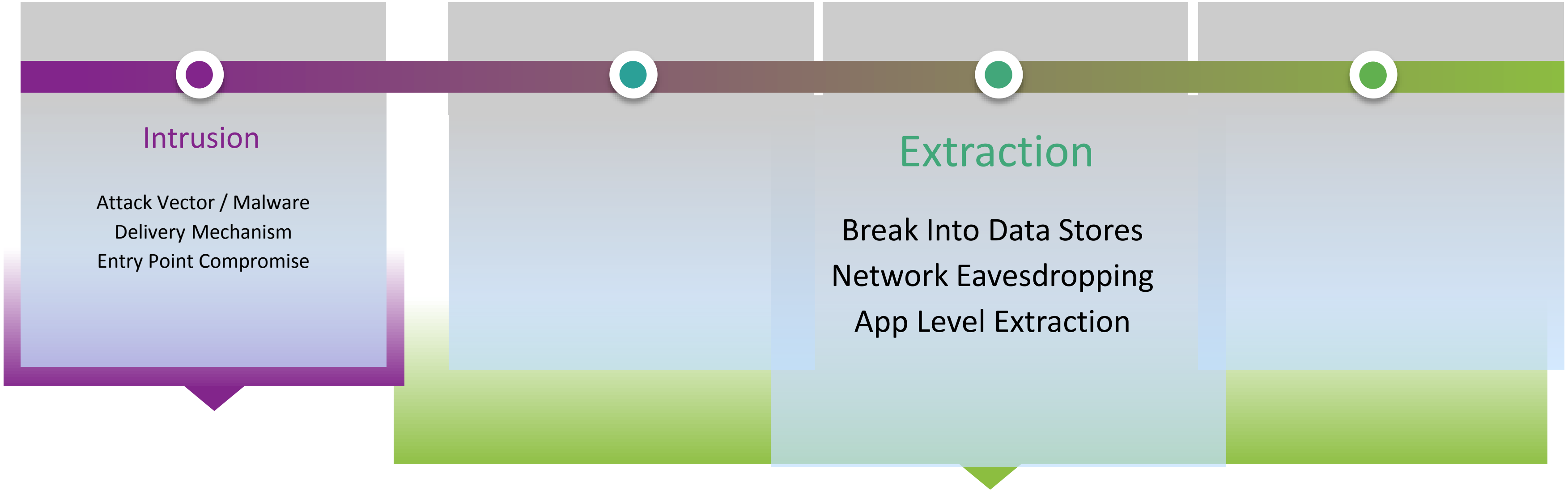
Escalate Privileges
Install C2* Infrastructure
Lateral Movement

Stop Exfiltration

20% of the investment is focused on addressing propagation, extraction and exfiltration.

Organizations lack the visibility and control inside their data center

Modern Attack: Targeted, Interactive, Stealthy



Intrusion

Attack Vector / Malware
Delivery Mechanism
Entry Point Compromise

Extraction

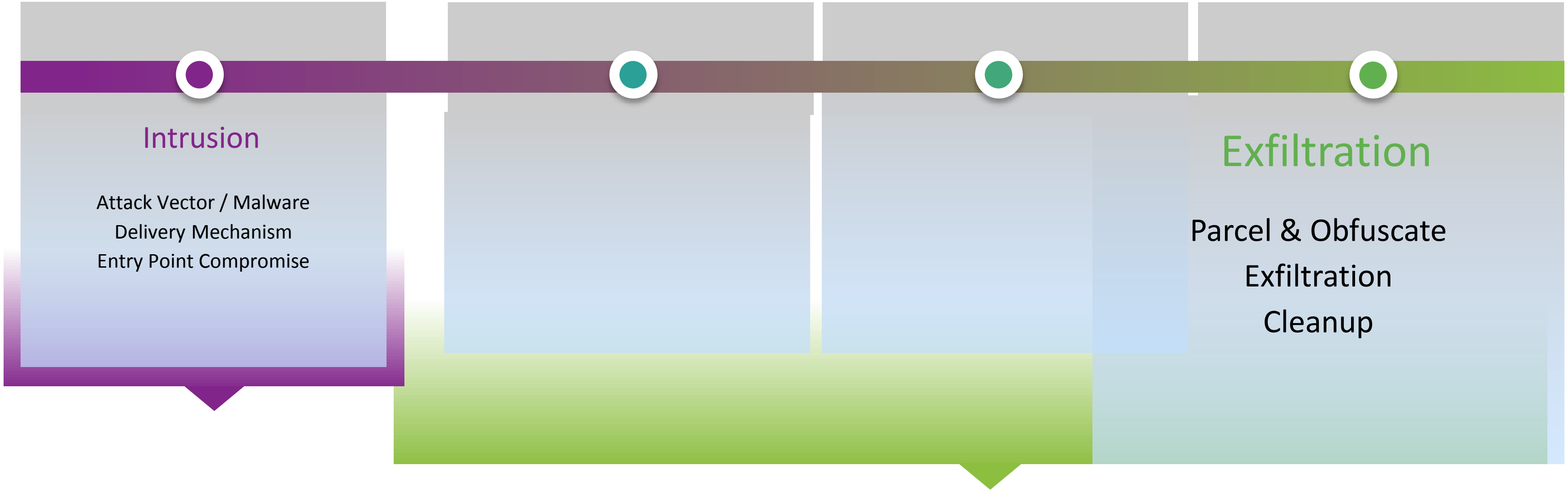
Break Into Data Stores
Network Eavesdropping
App Level Extraction

Stop Exfiltration

20% of the investment is focused on addressing propagation, extraction and exfiltration.

Organizations lack the visibility and control inside their data center

Modern Attack: Targeted, Interactive, Stealthy



Intrusion

Attack Vector / Malware
Delivery Mechanism
Entry Point Compromise

Exfiltration

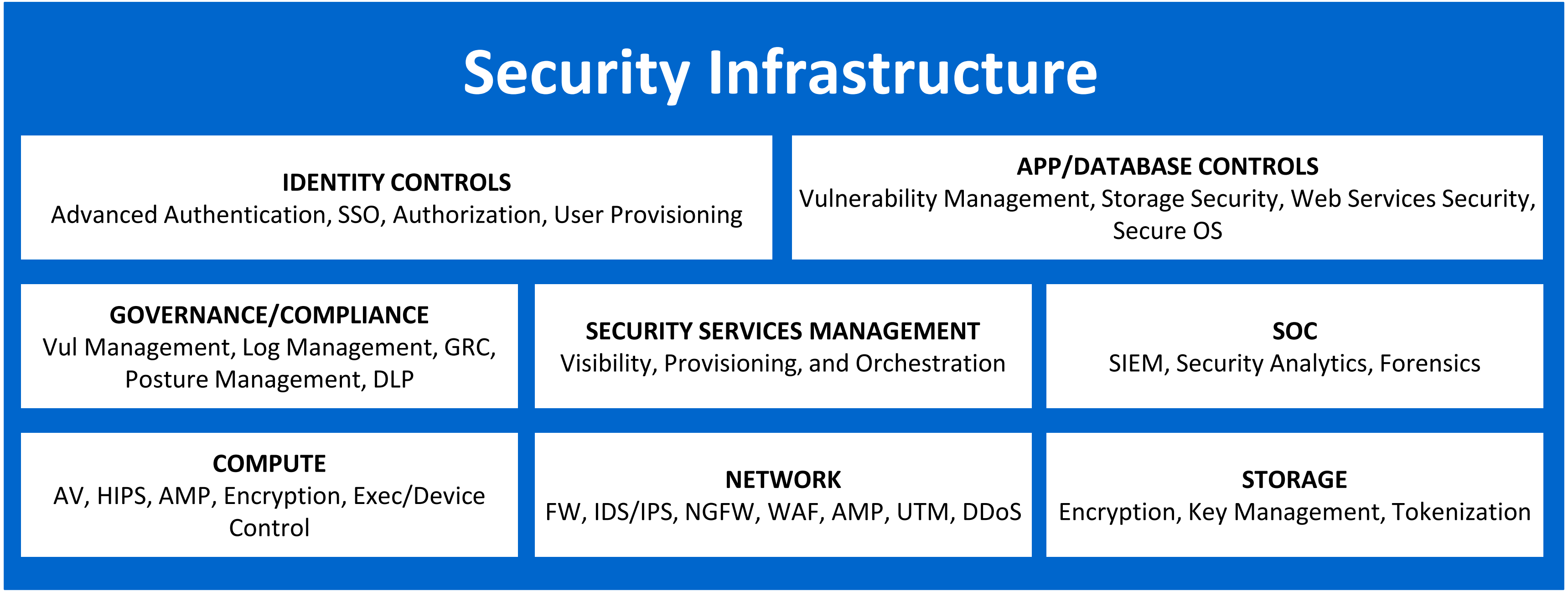
Parcel & Obfuscate
Exfiltration
Cleanup

Stop Exfiltration

20% of the investment is focused on addressing propagation, extraction and exfiltration.

Organizations lack the visibility and control inside their data center

The Security Tool Belt



Security Infrastructure

IDENTITY CONTROLS
Advanced Authentication, SSO, Authorization, User Provisioning

APP/DATABASE CONTROLS
Vulnerability Management, Storage Security, Web Services Security, Secure OS

GOVERNANCE/COMPLIANCE
Vul Management, Log Management, GRC, Posture Management, DLP

SECURITY SERVICES MANAGEMENT
Visibility, Provisioning, and Orchestration

SOC
SIEM, Security Analytics, Forensics

COMPUTE
AV, HIPS, AMP, Encryption, Exec/Device Control

NETWORK
FW, IDS/IPS, NGFW, WAF, AMP, UTM, DDoS

STORAGE
Encryption, Key Management, Tokenization

Impact of Architecture

Distributed application architectures

+

Comingled on a common infrastructure

=

Massive misalignment

1. Hyper-connected compute base

2. Distributed policy problem

How do we fix this?

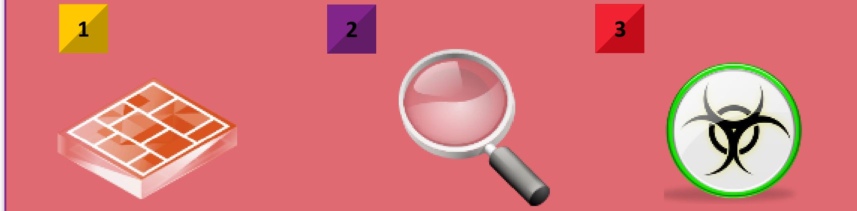
Security and Virtualizing Gen 2

- Virtualization security is a reality
- NextGen Firewalls and IPS systems are integrating into the fabric
- Endpoint and network monitoring leverage virtualization

Automating and Security

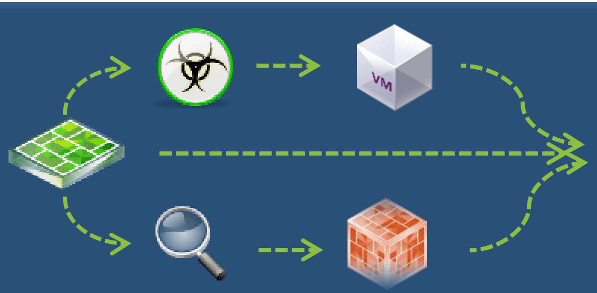
- New levels of information and visibility
- RestAPI is common
- Why not leverage this?

Leveraging Virtualization



Traditional Data Center

Static service chain



Virtualized Data Center

Dynamic service chain

Design and Leverage

- Enhanced security and service insertions
- Automatic remediation & automatic response
- Network isolation on demand
    - DMZ anywhere

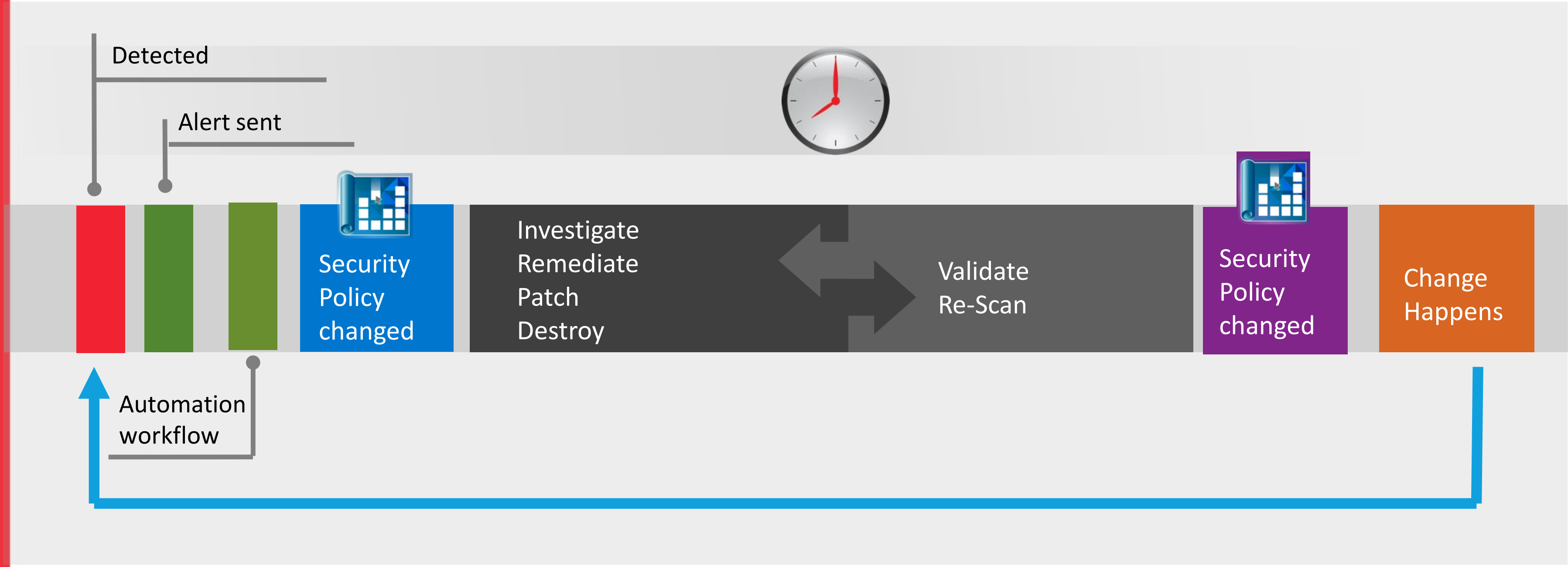
Adaptable Security Response

- All this based on changing meta data of your systems….
- What it was is not what it is today...
- Adaptable security for an ever adapting world

Security and Automation [PTATR]

Policy -	What do I allow or don't allow?
Triggers -	Event, activity, baseline differentials, etc.
Actions -	Block, log, accept, etc..
Timer -	How long should the change last?
Reset -	What is post incident normal?

The Automation Security Workflow



Detected

Alert sent

Security Policy changed

Investigate
Remediate
Patch
Destroy

Validate
Re-Scan

Security Policy changed

Change Happens

Automation workflow

Automation Risk Reduction

- How long does it take to respond?
- What is the size of team?
- Can you reduce remediation time and time to investigate ?

How to get started

- Things to consider?
  - Is your organization ready for this?
  - What is your hypervisor?
  - How much are your virtualized?
  - Is IT silo or integrated
  - What is your automation platform, if you have one?
  - Are there low hanging fruit we can attack with this?

Apply What You Have Learned Today

- Next Step:
  - Talk to your virtualization team and find out what you have deployed
- Build a plan:
  - Understand the integration points with your security products and your hypervisor
  - Define remediation workflows (PTATR)
- Put it into action:
  - Deploy a initial security remediation workflow to help with non-business critical systems security alerts
  - Increase integration points and develop playbooks for security remediation automation

Why Not Now

- Stateless built fashion
  - Wipe at random (just in case) – temporary systems
  - Containers and read only systems
  - Why write?
- Change control paradigm change
  - Auto updates/changes based on automation....

Future is Bright

- Automate based on dynamic variables
  - Encryption on the fly
  - Enhanced trusted context from the endpoint
  - Look at app memory via hypervisor
  - Honeypot on demand
  - Integrate into development

Q&A

Hadar Freehling hfreehling@vmware.com
Rob Randell rrandell@vmware.com