SESSION ID: SPO3-T07

HOW CLOUD, MOBILITY AND SHIFTING APP ARCHITECTURES WILL TRANSFORM SECURITY: GAINING THE HOME-COURT ADVANTAGE

Tom Corn
Senior Vice President/GM Security Products
VMware
@therealtomcorn
$3.7 Trillion in 2018

Gartner Press Release, Gartner Says Global IT Spending to Reach $3.7 Trillion in 2018, January 16, 2018

$91.4 Billion in 2018


$600 Billion in 2017

Source: Center for Strategic and International Studies, Economic Impact of Cybercrime, February, 2018

Forecasted Growth in Overall IT Spend

Growth in Security Spend

26%
(since 2014)

Increase in Security Losses

4.5%

10.2%
(since 2017)
Modernization

Data Center / Cloud Infrastructure
- Compute
- Network
- Storage

End User Infrastructure
- Users
- Devices
- Access

Threat Landscape
- Nation States
- Organized Crime
- Hacktivists

Agile
Dynamics of an Attack

Attacker

Defender

Infiltration  Propagation  Extraction  Exfiltration
Dynamics of an Attack

Infiltration

Propagation

Extraction

Exfiltration

Attacker

Defender
Home-court advantage

*noun*

the advantage that you have over an opponent when a sports contest takes place at your own sports field or court.

Macmillan Dictionary
Home-court advantage
Home-Court Advantage Comes From...

Understanding how your family uses your home, and using that context to shrink your security posture
If You Want Home-Court Advantage
Take advantage of what you know better than an attacker

Detect Threats

Shrink the Attack Surface

Family
Why don’t we get home-court advantage in cyber security?
We Keep All the Lights On, and All the Rooms Open
We See Through an Infrastructure Lens

- Monitor Perimeter For Threats
- Monitor Network For Threats
- Monitor Endpoint For Threats
If We Compartmentalize at All, it’s Aligned to an Infrastructure Lens

- Bedrooms
- Bathrooms
- Kitchens
- Living Rooms
We Should Focus More on Core Protection Strategies

Gartner Market Guide for Cloud Workload Protection Framework

Figure 1. Cloud Workload Protection Controls
Hierarchy, © 2018 Gartner, Inc.

Source: Gartner, Market Guide for Cloud Workload Protection Platforms, Neil MacDonald, March 26th 2018. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designations. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document.
And We Should Focus on Applications and Data

And how they use the infrastructure – versus focusing just on the infrastructure
Cyber Threats
Residual Risk

Cyber Hygiene
Attack Surface

Micro-Segmentation  Least Privilege  Encryption  Multi-Factor Authentication  Patching

Apps  Data

©2018 VMware, Inc.
Can the unique properties of cloud and mobile be the solution versus the problem?
Secure Infrastructure

Apps

Data

Home-court advantage

Compute

Network

Data

Users

Devices

Access
Changing the Application Security Model
From chasing bad to ensuring good

Chasing Bad

75,000,000

Ensuring Good

75
Uniquely Leverage the Hypervisor

Application

What was Provisioned

What is Running

Isolation

Automation

Devices

Users

Access

©2018 VMware, Inc.
Capture & Analyze

Capture the purpose and intended state of applications and VMs

Learn

Off-the-shelf apps
- OTS
- Software
- Database

Custom apps
- CI/CD pipeline
  [Provisioning systems]
  [Automation frameworks]

Machine Learning

Intended State Engine

App Scope

Manifest

Detect

ESX

ESX

Respond

Manifest

Manifest

Provisioning systems

Automation frameworks

vCenter

Users

Network

Data

Compute

Devices

Access
Detect

Runtime application attestation and secure manifest store

Learn
Capture & Analyze

Protect

Respond

Detect

AppDefense Monitor

Manifest

Protected zone

OS

Processes

Processes

Processes

AppDefense Monitor

Manifest

Protected zone

OS

Processes

Processes

Processes

AppDefense Monitor

Manifest

Protected zone

OS

Processes

Processes

Processes

vm

vm

vm
Respond
Orchestrated incident response routines for the SOC
Review and Readiness
Collaboration between security teams and application teams
Review and Readiness
Collaboration Between Security Teams and Application Teams

Figure 2: DevSecOps: Secure Development as a Continuous Improvement Process © 2017 Gartner, Inc.

Source: Gartner, 10 Things to Get Right for Successful DevSecOps, Neil MacDonald, October 03 2017. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designations. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document.
Demo
Secure Infrastructure

Security Controls

Apps

Data

Compute
Network
Data
Users
Devices
Access
Enabling Richer Security Controls

Source: Momentum Partners Cyberscape 2017
Secure Infrastructure

Security Controls

Apps

Data

Home-court advantage

Home-court advantage

Compute

Network

Data

Users

Devices

Access
Secure Infrastructure

Security Controls

Apps

Data

Compute
Network
Data
Users
Devices
Access
Enabling Richer Security Controls

Source: Momentum Partners Cyberscape 2017
Secure Infrastructure

- Apps
- Data

Home-court advantage

Secure Infrastructure

Compute
Network
Data
Users
Devices
Access
Secure Infrastructure

- Apps
- Data

Home-court advantage

- Compute
- Network
- Data
- Users
- Devices
- Access
Validate and Verify
Right user + right device + right app
Enabling Richer Security Controls

Source: Momentum Partners Cyberscape 2017
If You Want Home-Court Advantage

Take advantage of what you know better than an attacker

Detect Threats

Family

Shrink the Attack Surface
Transforming CYBERSecurity

Source: Momentum Partners Cyberscape 2017
Go beyond: Securing Cloud & Mobility
To using: Cloud & Mobility to Secure
HOW CLOUD, MOBILITY AND SHIFTING APP ARCHITECTURES WILL TRANSFORM SECURITY: GAINING THE HOME-COURT ADVANTAGE

Tom Corn
Senior Vice President/GM Security Products
VMware
@therealtomcorn
Transforming CYBERSecurity

Security Controls

Context

Secure Infrastructure

Source: Momentum Partners Cyberscape 2017