Tackling Security Challenges in the Hybrid Cloud

Sasha Pavlovic
Head of Cloud Security
Trend Micro | ANZ
What we’ll cover today…

• State of datacenter security
• Top datacenter security concerns
• What enterprises are struggling with
• Security strategy for a hybrid cloud datacenter
The data center has evolved faster than everyone imagined...
Today’s Datacenter Deployment

- Mix of traditional datacenter & cloud infrastructure
- Increased architectural options & complexity
- Statistically, more breaches occurring in the on-prem datacenter

SANS Institute: the State of Dynamic Data Center & Cloud Security in the Modern Enterprise
Existing security concerns still apply…

- Application/OS Vulnerabilities
- Advanced persistent threats
- Malware infections (ransomware)
- Social engineering
- Insider threats
- Identity and Access Management
- DDoS
Top Root Cause of Compromise

- App Vulnerabilities
- Malware Infections
- Social Engineering, poor security habits
- DDoS
- Advanced Persistent Threats
- Insider Threats
- Identify Access Mgmt.
- False Alarm
- Others

SANS Institute: the State of Dynamic Data Center & Cloud Security in the Modern Enterprise
App Vulnerability

- Which version of the patch
- Compatibility with mission critical applications
- Time to test
- What servers, VMs, instances need to be patched
- When can we reboot the system?

Vulnerability Disclosed or Exploit Available

Virtual Patching

Patch Available → Test → Begin Deployment → Complete Deployment

Time

Window of exposure 30-90 day
“Virtual Patching is not a luxury, it’s a necessity”
The convergence of on-premise and cloud... we’ve hit a crossroad

- Still struggling with efficiently protecting on-premise datacenter
- Dynamic cloud computing environments
The story behind all the headlines....
Traditional Security Strategy

• Perimeter Focused

• Firewall, network IDS/IPS and antivirus

• Lack visibility of East-West traffic
Paradigm Shift in Security: From Castles to Maximum Security Cells
“Enterprise Security Needs to Evolve beyond the Perimeter to the Host level”
"I need to ensure security and protection is applied unilaterally, across environments!"
Cloud Security is a Shared Responsibility

Facilities
Physical security of hardware
Network infrastructure
Virtualization infrastructure

Cloud Provider

Cloud User

Platform
Operating systems
Applications
Data
Identity & Access Management
When Conventional Security Meets Cloud Dynamic Computing Environment

- Lack of Automation & API support for Cloud DC operations
- Lack integration with Cloud security services & management tools
- H/W security appliances have no place in the cloud
Challenge of Network Security in the Cloud

Lack of Visibility into Cloud Provider’s network environment

Lack of Cloud Provider Support of Security Technology

Lack of Security Vendor Options for cloud environment

Lack of Compatibility with Vendor Hypervisor Infrastructure

Others

SANS Institute: the State of Dynamic Data Center & Cloud Security in the Modern Enterprise
Automation: Workload-Centric Security

- Automatically set IPS policies based on O/S and application context
- Increase Performance by reducing unnecessary rules
- Leave policy creation to the experts
Integration: Visibility

- Identify **important** security alerts
  - Registry Changes
  - Brute Force attempts
  - File Changes
  - Login Issues
- Comprehensive audit trail for the entire infrastructure
Automation: Remediate & Respond

- Automatically respond to security events
- Isolate compromised instances automagically
- Security at DevOps speed

Security Tools

Amazon SNS
AWS Lambda
Prevalent Security Controls

On-premise vs In-the-Cloud
“Don’t try and Forklift Traditional Security Controls into the Cloud”
A Customer’s Real World Journey
Healthdirect Australia
Healthdirect Overview

No matter where people live, or what time of the day or night it is, they can talk to a professional, find trusted advice online about how to manage their issue, and locate the closest appropriate and open service that meets their needs.
Healthdirect Australia Timeline

2006/2007: Established as the National Health Call Centre Network
2008: healthdirect 24/7 nurse triage helpline
2010: Pregnancy, Birth and Baby service
2011: after hours GP helpline
2012: mindhealthconnect (mental health website)
2013/2014: National Health Services Directory
2015: Carer Gateway
2012: My Aged Care Gateway
Security is critical for Healthdirect Australia

- Together Government and Healthcare made up over 40% of all data breaches in 2015
Security Challenges

- Information Security Manual Compliance
  - HIDS/HIPS mandatory
  - Patching controls
- Small security staff complement for large diverse platform
- Privacy Act and sensitive data protection
- Perimeter is NOT good enough any more
- Moving security staff from gatekeepers to participants
- Effective management of log and monitoring data
- More frequent sophisticated attacks
Trend Micro Deep Security to the Rescue

- DISA certified
- Host based firewalling and intrusion prevention
- Single management ‘pane of glass’
- Antivirus and anti-malware
- Host protection
- File integrity monitoring
- Log inspection
- Trusted SSL certificate issuing
Corporate environment protection

• End-point security for user fleet
• Email filtering
• Email inspection
• Network traffic inspection
• Cloud application protection for O365
• Document protection
Why Trend Micro Works for Us
“Security tools that enact policies closer to the workload themselves…may prove more effective in dynamic environments.”

- SANS Institute
THANK YOU

Richard Sheng
Trend Micro
richard_sheng@trendmicro.com