SECURING THE SDDC WITH BEST OF BREED TECHNOLOGY PARTNER: VMWARE AND TREND MICRO

Mark Hong
Senior Technical Consultant, Trend Micro

Arup Deb
Senior Systems Engineer, Networking and Security, Southeast Asia & Korea, VMware
Forecasted Growth in Overall IT Spend

$3.7 Trillion in 2018

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

Growth in Security Spend

10.2%
(since 2017)

$91.4 Billion in 2018


Increase in Security Losses

26%
(since 2014)

$600 Billion in 2017

Source: Center for Strategic and Int’l Studies, Economic Impact of Cybercrime, February, 2018
Traditional security has little meaning in a borderless Software Defined Data Center

Insufficient visibility into East-West traffic & inter-VM attacks

Static policies cannot keep up with dynamic workloads

Service Provisioning is Slow, Complex & Error-prone

Disparate security solutions and lack of uniform policies across clouds creates an operational nightmare
Traditional approaches to reduce breaches inside Data Center perimeter...

Adding more internal security…
Requires placing more security controls across workloads

Physical Security Appliances
- Optimized for Data Center Perimeter
- Cost prohibitive: thousands needed
- Configuration and security policies restricted by network topology
- Inefficient “choke point”
- Impractical for lateral coverage

Virtual Security Appliances Today
- Lacks selective traffic inspection for smarter security
- Hair-pinning impacts performance
- Limited segmentation capabilities
- Lacks dynamic provisioning, deployment and scale out

Answer is Micro-Segmentation
SDDC with NSX Network Virtualization

Network and Security Services Now in the Hypervisor

- Load Balancing
- L3 Routing
- L2 Switching
- Firewalling/ACLs

Network and Security Services

- L2 Switching
- L3 Routing
- Firewalling/ACLs

Software

Hardware
Enables granular, scalable control

- High throughput rates on a per-hypervisor basis
- Every hypervisor adds additional east-west firewalling capacity
- Enforcement at virtual interface
Provides automated security operations

Platform-based automation

- Automated provisioning and workload adds/moves/changes
- Accurate firewall policies follow workloads as they move
- Centralized management of single logical, distributed firewall
Intelligent grouping of data center assets
Groups defined by customized criteria

- Operating System
- Machine Name
- Services
- Application Tier
- Regulatory Requirements
- Security Posture
• NSX Distributed Firewall provides security filtering functions on every host, inside the hypervisor and at kernel level
  – DFW is a East-West stateful firewall
  – Distributed enforcement of policy rules
• DFW offers centralized configuration
  – Using the vSphere Web Client
DFW Policy Enforcement

- DFW enforces rules at vNIC layer before encapsulation (or after de-capsulation)
  - Independent of transport network (VXLAN or VLAN)

Policy Rules:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>VM2, VM3</td>
<td>TCP port 123</td>
<td>Allow</td>
</tr>
<tr>
<td>VM1</td>
<td>VM2, VM3</td>
<td>any</td>
<td>Block</td>
</tr>
</tbody>
</table>

Note: there is no relationship between DVS ACL/Security capabilities and DFW
NSX Platform Extensibility…With Advanced Security

- Add leading security solutions to your micro-segmentation deployment for greater security
- Apply the SDDC operational model to 3rd-party security products
- Adapt to changing security conditions in the data center by enabling security solutions to share intelligence

Traditional Data Center

Static service chain
In a traditional data center, security services must be configured when the network is architected, meaning the “chain” of services is locked in once deployed. This is an inefficient use of resources and cannot defend against changing threat conditions.

NSX Data Center

Dynamic service chain
In an NSX data center, 3rd-party security solutions use NSX security tags to share intelligence, adapting to changing security conditions. NSX automatically applies the correct security function as needed.
NSX / Third Party End to End Workflow

1. Register Third Party Management platform with NSX Manager
2. Deploy Third Party VM Appliances (per ESX Cluster)
3. Consume Service!

NSX simple operational model now extended to Third Party services
Advanced Security Services Insertion in action
Extending with 3rd party security solutions

Allows multiple partner and VMware services to be “chained” together.

Each guest can have different combination of services.
Advantages of the NSX, Deep Security integration

- Simplified orchestration and automation
- Optimized performance, Minimal footprint & Higher VM density
- Seamless interoperability w/physical, virtual and cloud
- Provision services in minutes, not days
- Fast adds/moves/deletes
- Elastic protection, instant scale
- Enforcement of micro-segmentation and zero trust model
- Stronger threat defense with NSX tagging
- Policy follows workload
- Extend segmentation to public clouds
What is Trend Micro Deep Security?

- Modules
- Automation
- Vulnerabilities & Protection
- Ease of Use
- Performance Advantage
- Summary
Deep Security Protection Modules
Anti-Malware

Detects and blocks malicious software intended to harm endpoints
Web Reputation

Tracks the credibility of websites to safeguard servers from malicious URLs
Allow or block network traffic through a bidirectional, stateful firewall
Intrusion Prevention

Examines all incoming and outgoing traffic at the packet level searching for any content that can signal an attack
Monitors critical operating system and application files to provide real-time detection and reporting of malicious and unexpected changes.
Log Inspection

Collects and analyzes operating system and application logs for suspicious behavior, security events, and administrative events
Application Control

Monitors computers for any software changes that drift away from an approved software inventory
Simplify Provisioning and Management with NSX

- Automated deployment of Deep Security using NSX
- View security events in vSphere and take automated actions

- Scale security seamlessly with your infrastructure
- No maintenance mode or re-boot required
- Automate workflow and interoperability through NSX tagging
- Improve control through rules-based workflow
Automatic Quarantining of a Virtual Machine using NSX tagging
Automatic Quarantining of a Virtual Machine using NSX tagging
Automatic Quarantining of a Virtual Machine using NSX tagging
Automate security specific to your data center with NSX and Deep Security

• Recommend and apply policies automatically – specific to your data center environment

• Automatically scale up and down across data center and cloud as required – with no security gaps

• Gain visibility – vCloud Director and vCenter Operations Manager integrations
Virtual Patching - Recommendation

- Operating System: Windows 2008 Server
<table>
<thead>
<tr>
<th>Rule ID</th>
<th>Description</th>
<th>Application Type</th>
<th>Priority</th>
<th>Mode</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10002061</td>
<td>Identified Suspicious JavaScript Encoded Shellcode</td>
<td>Web Client Common</td>
<td>2</td>
<td>Normal</td>
<td>Detect Only By</td>
</tr>
<tr>
<td>1000505</td>
<td>Microsoft Internet Explorer 'Print Table of Links' Crash</td>
<td>Web Client Internet Explorer</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10002888</td>
<td>Microsoft WordPad 'Ciao' File Remote Denial Of Service Vulnerability</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10003254</td>
<td>Microsoft Internet Explorer HTML Form Value Denial Of Service Vulnerability</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10002507</td>
<td>Microsoft Internet Explorer 'Modify' Object Remote Code</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10003470</td>
<td>Multiple Browser Certificate Regroup Parsing Heap Crash</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10003842</td>
<td>Multiple Certificate Parsing Remote Code Crash</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10003155</td>
<td>Identified Malicious Adobe PDF Document Crash</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10001683</td>
<td>Heuristic Detection Of Malicious PDF Documents Crash</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10004491</td>
<td>Adobe Flash Player Unspecified Code Execution Vuln</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10004500</td>
<td>Microsoft Internet Explorer CSS Parsing Remote Code Crash</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10004550</td>
<td>Adobe GIF File 'expidex.exe' Crash</td>
<td>Web Client Common</td>
<td>2</td>
<td>Prevent</td>
<td>Exploit</td>
</tr>
<tr>
<td>10004552</td>
<td>Adobe TIFF File Vulnerability Crash</td>
<td>Web Client Common</td>
<td>2</td>
<td>Normal</td>
<td>Detect Only By</td>
</tr>
<tr>
<td>10000959</td>
<td>Microsoft Internet Explorer ActiveX bgColor Property</td>
<td>Web Client Internet Explorer</td>
<td>2</td>
<td>Normal</td>
<td>Prevent</td>
</tr>
<tr>
<td>10001383</td>
<td>Identified Suspicious Usage Of Shellcode For Client</td>
<td>Web Client Common</td>
<td>2</td>
<td>Normal</td>
<td>Prevent</td>
</tr>
<tr>
<td>10003628</td>
<td>Multiple Web Browsers Denial Of Service Vulnerability Crash</td>
<td>Web Client Common</td>
<td>2</td>
<td>Normal</td>
<td>Prevent</td>
</tr>
<tr>
<td>10003716</td>
<td>Microsoft Windows RDP Connection Denial Of Service Crash</td>
<td>Remote Desktop Protocol Server</td>
<td>2</td>
<td>Normal</td>
<td>Prevent</td>
</tr>
<tr>
<td>10009239</td>
<td>Microsoft Internet Explorer Null Pointer Dereference Crash</td>
<td>Remote Desktop Protocol Server</td>
<td>2</td>
<td>Normal</td>
<td>Prevent</td>
</tr>
<tr>
<td>10004058</td>
<td>Microsoft Windows Lan File 'expidex.exe' Crash</td>
<td>Web Client Common</td>
<td>2</td>
<td>Normal</td>
<td>Prevent</td>
</tr>
<tr>
<td>10004121</td>
<td>Identified Obfuscated JavaScript For Internet Explorer Vul</td>
<td>Web Client Internet Explorer</td>
<td>2</td>
<td>Normal</td>
<td>Prevent</td>
</tr>
<tr>
<td>10004141</td>
<td>Multiple Browsers OlaD Denial Of Service</td>
<td>Web Client Common</td>
<td>2</td>
<td>Normal</td>
<td>Prevent</td>
</tr>
<tr>
<td>10004159</td>
<td>Microsoft Internet Explorer CSS 'expression' Remote Code</td>
<td>Web Client Internet Explorer</td>
<td>2</td>
<td>Normal</td>
<td>Prevent</td>
</tr>
</tbody>
</table>
Vulnerability Information

Remote Desktop Protocol Vulnerability (CVE-2012-0002)

Date Reported: March 13, 2012

Type: Other

Severity: (Critical)

Description:
The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability." More Info:
http://technet.microsoft.com/en-us/security/bulletin/MS12-002 By default, the Remote Desktop Protocol is not enabled on any Windows operating system. Systems that do not have RDP enabled are not at risk. Note that on Windows XP and Windows Server 2003, Remote Assistance can enable RDP.

Solution:
Apply this rule.

External References:
Microsoft MS12-000
Mitre CVE-2012-0002
Secunia SA1738
Secunia SA1777
Secunia SA2107
Secunia SP2201

Vulnerable Software and Versions:
microsoft windows_xp
microsoft windows_server_2003
microsoft windows_server_2008
microsoft windows_server_2008_r2
microsoft windows_vista
microsoft windows_xp
Elastic Protection to increase security, reduce cost & scale better with Deep Security

- Reduce risk of exposure to vulnerability exploits – especially as you scale
- Save money avoiding costly emergency patching
- Patch at your convenience

Virtually patch with Trend Micro Intrusion Prevention

- Vulnerability Disclosed or Exploit Available
- Patch Available
- Test
- Begin Deployment
- Soak
- Complete Deployment
- Deployment
- Patched
Multi-layered approach

1. Stateful Firewall
   - Allow known good

2. Exploit Filters
   - Stop known bad

3. Vulnerability Filters
   - Shield known vulnerabilities

4. Smart Filters
   - Shield unknown vulnerabilities (Zero-day)

5. Custom Filters
   - Protect specific applications
Protect Against Advanced Threats

LEGEND
- Known Good
- Known Bad
- Unknown

Anti-Malware & Web Reputation
Intrusion Prevention (IPS) & Firewall
Integrity Monitoring & Log Inspection
Application Control

Machine Learning
Behavioral Analysis
Custom Sandbox Analysis

Safe files & actions allowed
Malicious files & actions blocked
Single pane Infrastructure and Security visibility for effective Management

Deep Security Adapter for VMware vCenter Operations

- Identifying Performance impact by correlating Performance stats with Security events
- Less Security Events = More Compute Resources available

Deep Security Heatmap

- Quickly view computer security status
- Each heatmap entry is clickable for a more detailed view in the form of a metric graph
Optimized performance for virtual environments

- Management
- Network Usage
- Scan Speed
- CPU/Memory Usage
- IOPS
- Storage
Optimized performance for virtual environments

- Up to 20X Faster* Full Scans
- Up to 5X Faster Real-time Scans
- Up to 2X Faster VDI Login
- Up to 30% More VM density

ESXi
SAN

Virtual Appliance
Scan Cache

VM
VM
VM
DISK
DISK
DISK

Optimized performance for virtual environments
Avoid security sprawl with too many disconnected security solutions

Multiple point security solutions

Disconnected solutions with limited data sharing

Integration gaps can introduce inefficiencies and new vulnerabilities

Resource intensive

Uncorrelated Threat data, reports & dashboards

Repetition of basic underlying activities

Separate policies and provisioning leads to huge management overhead

Trend Micro Deep Security Platform

Integrated solution working together across clouds

Smarter protection with system & network introspection

Optimized performance & resource efficient

Efficient mgmt., simplified provisioning, single dashboard, unified reporting

Seamless data sharing between modules

Event correlation for better threat intel
Bringing together the best of both worlds to infuse security into the datacenter fabric

- Granular, unit-level Datacenter security through Micro-segmentation
- Faster provisioning, deployment, distribution of advanced services
- Automated operations through tagging and service chaining
- Scalable control without compromising on throughputs

- **Stronger threat defense** with NSX micro-segmentation and advanced security controls for system and network security
- **Elastic protection** through automated policy and security controls
- **Consistent policies and unified operations** across physical, private and public environments
- **No-compromise and non-disruptive** Scale securely without compromising on performance, using existing tools & processes

- **Multi-vector protection** through integrated System and Network security solutions in a single platform
- **Optimized performance** for virtual environments
- **Seamless interoperability** w/physical, virtual and cloud
- **Automated, scalable and instant-on security** purpose built for agile borderless datacenters
Securing the Software Defined Data Center
with VMware NSX and Trend Micro Deep Security

Thank You...
INNOVATION begins WITH YOU