



Surviving the Siege:
Medieval Lessons in Modern Security

The Enterprise IT Security Portfolio *A Technological Survey*

By: Patrick R. Turner, Vice President and CIO



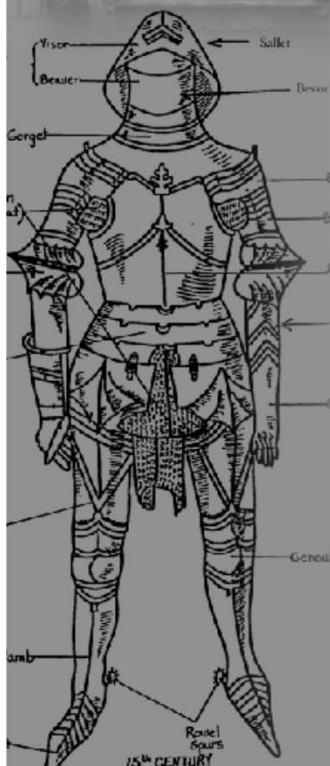
Play [CyberHunt](#), the game within the SecureWorld app!
Have fun, network and win great prizes.



Don't forget to take the [survey](#) on the SecureWorld App.
It will also be emailed to you at the conclusion of the conference.



After this presentation, view the [slides](#) on the SecureWorld App.



Agenda

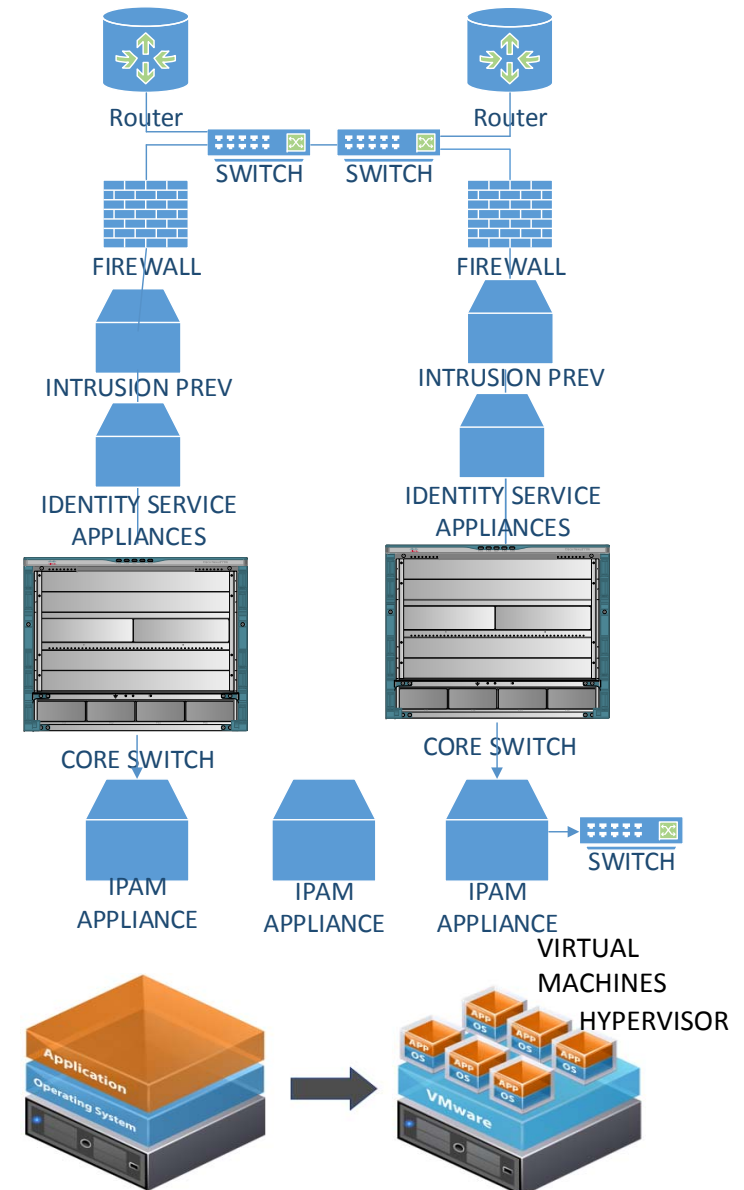
- Security stats and Questions to ask yourself
- Antivirus
- Firewall
- Switching with VLAN network segmentation
- Encryption
- TLS/SSL certificates
- ISE (Identity Services Engine)
- IPS (Intrusion Protection System)
- Automated Penetration and Vulnerability Analysis
- DLP (Data Loss Prevention)
- Zero Day Threat Mitigation
- Next Generation Firewalls for APT(Advance Persistent Threat)
- DDOS – Volumetric Attack Mitigation
- IPAM (IP Architecture Management)
- Secure DNS (Domain Name Server)
- Password Policies
- Multi-Factor Authentication
- Password Lockers
- Social Engineering Training
- Development of an Enterprise Security/ Privacy Policy
- Incident Response Management
- Virtualization
- Micro-Segmentation
- SDN (Software Defined Networking)
- Monitoring - Analysis

Where they all live...

SECURITY HAPPENS AT ALL LAYERS OF THE NETWORK

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	Routers IP/IPX/ICMP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgement • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub	



Cyber Security Stats

- Cyber attacks continue to rise – attackers are becoming more stealthy
- DDOS attacks in the thousands on a monthly basis
- Windows 7 has over 500 vulnerabilities and is the most popular OS
- Balance out expenditures and degree of protection – conversation becomes at what cost is your enterprise's level of security enough to sustain an attack
- Consider “Enterprise Umbrella” insurance in relation to cyber attacks



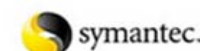
Security questions to ask yourself

- What makes your enterprise a target
- What are the specific threats:
 - Users exposing data unintentionally
 - Privilege elevation or rooting
- What types of data are leaving the company
- What types of public access are allowed
- How are you protecting against social engineering and phishing attacks
- What types of traffic are you denying at the firewall



Antivirus

- Frontline defense for PCs, servers, and other endpoints
- Antivirus software is a class of software that can prevent, detect and remediate malware infections on individual endpoint computing devices and IT systems
- Physical machines, Sophos, Norton™, McAfee®, Trend Micro™ for PC's - Office 11, etc.
- Virtual Desktops: Trend Micro™, SOURCEfire® AMP, Bitdefender™, etc.
- A must have as the most basic layer of IT security
- Especially important on laptops that leave the enterprise security environment – “Out in the Wild”


ウイルスセキュリティ

Firewall

- A firewall is a network security system, primarily a network perimeter security device, when paired with endpoint virus protection, represent the most basic components in network security
- Firewalls can be either hardware or software-based, which control incoming and outgoing network traffic based on a set of rules
 - Port-based access control – most common are ports 80, 443, 25, etc.
- Creates a collection of isolated networks
- VLAN segmentation hinders access to system attack surfaces
 - Defined in switching, traditionally is most common for isolating parts of networks
 - Utilized to separate categories of traffic from each other – DMZ, internal, internet, application layer, DBMS layer, CCTV security
- NAT – Network Address Translation – Only expose certain external IP addresses to the world while protecting internal IP addresses keeping them private
 - NAT (Network Address Translation) is important to limit traffic to certain devices
- Cisco® ASA, Juniper® software firewall on server and PC operating systems, etc.



Switching with VLAN Network Segmentation

- A Switch configuration has many constructs used to “improve” security
- Switch Layer 2 – (broadcast traffic to all devices) or Router Layer 3 (only see subnet traffic)
- **Layer 2** – Local Area Network (LAN)
 - **MAC address** (Media Access Control)
 - ARP (Address Resolution Protocol) table maps MAC to IP
 - Broadcast domain
 - Spanning Tree Protocol (STP) – loops
- **Layer 3** – Wide Area Network (WAN)
 - IP Address (Internet Protocol)
 - Router
 - Routing tables – IP & next hop device
 - Sub-netting
 - Broadcast domain restricted
- VLAN segmentation hinders access to system attack surfaces
 - Creates a collection of isolated networks
 - Traditionally is most common for isolating parts of networks
 - Utilized to separate categories of traffic from each other – DMZ, internal, internet, application layer, DBMS layer, CCTV security
 - Various firewall commands are used to provide security features, NAT (Network Address Translation), is important to limit traffic to certain devices
- Cisco®, Dell®, HP, etc., etc.

Encryption

- Most effective way to achieve data security
- Encrypted data is referred to as cipher text
- Must have a secret/private/public key to decrypt cipher text
- Primary purpose is to protect the confidentiality of digital data stored on computer systems or transmitted via internet or other computer networks
- Encryption algorithms play a vital role in the security assurance of IT systems and communications
- Encryption is the most important component in a data loss prevention (DLP) strategy (can't read it), but is the best tool to use to steal data too...



TLS/SSL – OSI Layer Security Methods

- A standard security technology for establishing an encrypted link between a server and a client built into a network communication protocol – web related – Layer 5 (Session) of the OSI model (above the transport layer)
- A “Cert” (Certificate) is used to encrypt traffic
- The extra processing it takes to encrypt and decrypt network traffic degrades performance
- SSL encryption creates a network monitoring blind spot unless traffic is decrypted for deeper inspection
- Anatomy of an SSL Session:
 - **Public/Private keys** – These are the keys used for authenticating parties to a transaction and generating encryption keys
 - **Certificates** – A document that identifies an entity and associates that identity with a public key that is also stored in that document
 - **Certificate Authority** or CA – A trusted third-party used to verify the authenticity of a certificate
 - **Distinguished name** – the format used for identifying the owner of a certificate
- The steps in the SSL protocol negotiation are as follows:
 - The client signals the server with a message known as the “Client Hello”
 - The server responds with a “server hello” message and its certificate
 - Authentication and Pre-Master Secret
 - Decryption and Master Secret
 - Generate Session Keys – both use the master secret to generate the session key
 - Encryption with Session Key – both exchange messages to inform that future messages will be encrypted
- TLS – Transport Layer Security – is a protocol that ensures privacy between communicating applications and their users on the internet
- TLS ensures server/client traffic is free of third-party eavesdropping or tampering
- TLS is the successor to the Secure Sockets Layer (SSL)

Identity Services and Port Level Security

- Is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the company's routers and switches with a level of flexibility of custom access not common
- Allows a user's port-level access to "follow" them around the enterprise by changing port-level access rights on the fly (NAC – Network Access Control)
 - A student's access is "internet only" no matter what wall port or wireless access point they are connected to..... The CIO has the same access from his office or the cafeteria
- Port level security stops others from being able to plug into your infrastructure
- This technology uses 802.1x and user account profiles (i.e., credentials, permissions), the endpoint devices based on MAC address, IP, and device profile
- Cisco® ISE (Identity Services Engine), SmartDraw® Legal Edition, abmpegasus™



IPS – Intrusion Prevention Systems

- This is a preemptive approach to network security used to identify potential inbound threats and stop them when detected
- This technology is typically based on the use of “sensors” that are inserted in the network traffic flow and “inspects” traffic for anomalies or malicious traffic
- Threats fall into the following categories
 - Malware – pattern matching using file level hash
 - Email phishing – is an attempt to acquire sensitive information
 - Website vulnerabilities – injection of malicious HTML or client side scripts
 - Non-standard communications – a way for hackers to get around port based security
 - Known bad IP addresses – malicious or suspected in malware and spamming activities
- Cisco SOURCEfire®– fireSIGHT® and now firePOWER®, Palo Alto Networks®, McAfee®, Check Point®, FireEye™
- SNORT® is an open source IDS (Intrusion Detection System) only which is the basis of some commercial based systems – it basically “finds problems”

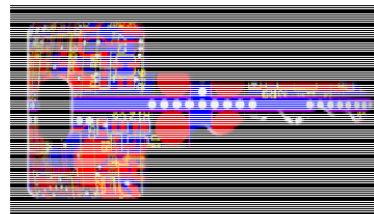
Automated Penetration & Vulnerability Analysis

- Identifying network security weaknesses before they are exploited internally or externally
- Qualys® penetration testing – Outside/In testing of targeted IPs
 - Detailed threat description
 - Discussion of the threat impact/risk
 - Provide detailed mitigation instructions
- Metasploit® penetration testing software
- Open source refers to a program in which the source code is available to the general public – Linux distributions with pen tools
 - Rapid 7™ Nexpose®
 - Kali Linux™
 - BackBox Linux



DLP – Data Loss Prevention

- A strategy for making sure that end users or malicious entities do not send sensitive or critical information outside the corporate network
 - PII – Personally Identifiable Information – CC#, SS#, DOB, financials, etc.
- There are software products that help a network administrator identify and control what data end users can transfer
 - Scanning of email, web traffic, data at rest, data in flight for patterns of data
 - Other Policy Sets – PCI, HIPAA, SOX, GLBA, Title 9, FERPA, Cyber Bullying, Profanity...
 - Encrypted email content/web traffic – decrypt, scan, and re-encrypt
- Helps protect end users who may be unaware that they are transmitting unsecure data that should be secure
- Forcepoint, Cisco IronPort™, etc.
- Education and training



Zero Day Threat Mitigation

- “Zero Day” – A payload hash never seen before – just change one line...
- Exploit OS vulnerabilities: Mitigating a full blown attack via “Sandboxing”:
 - An unknown malicious payload/attachment is downloaded into your network
 - The detection system intercepts/sends the payload to the cloud for analysis by spinning up a VM similar to the sending endpoint device – deleted when done
 - Payload is detonated (opened/executed) then monitored for malicious activity
 - If malicious activity is detected, a hash of the payload is uploaded to malware cloud for future recognition and the download to your network is aborted
- Attackers engineer malicious software to exploit common file types
- Used in both IPS or NGFW (Next Generation Fire Wall)
- Palo Alto Networks®, Check Point®, Fortinet®, Cisco®, FireEye®
- Feeds known malware library services
- New vectors: Google Docs, Dropbox, Box, OneDrive, etc.



Next Generation Firewall for APT Protections

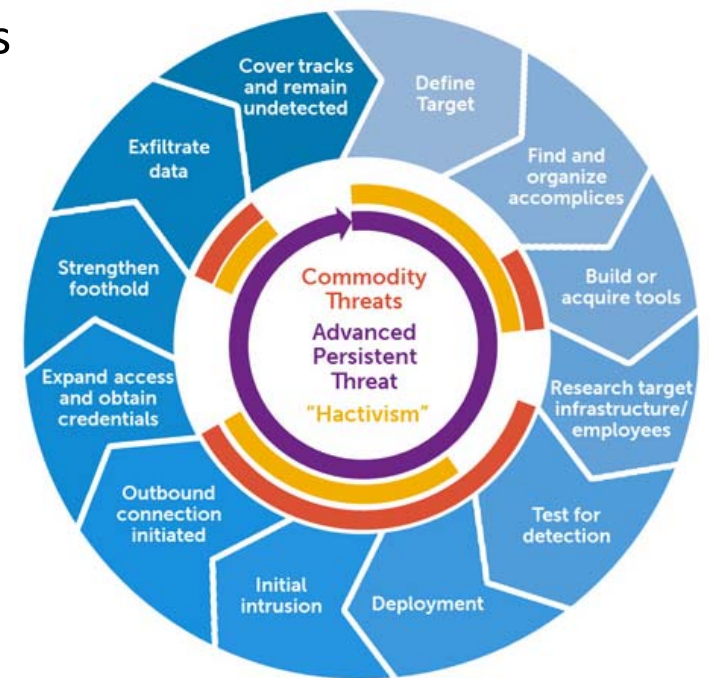
Gartner defines an NGFW as:

“A wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks”

Defining the Next-Generation Firewall – Gartner RAS Core Research note G00171540, John Pescatore, Greg Young, 12

October 2009, R3210 04102010

- Is a hardware or software based network security system that is able to detect and block sophisticated attacks by enforcing security policies at the application, port, and protocol level
- Advanced Persistent Threat (APT) – a set of stealthy and continuous computer hacking processes to get data out
 1. Breach perimeter
 2. Deliver malware – set up command and control
 3. Lateral movement – “east - west” traffic
 4. Ex-filtrate data – copy to less secure – ftp via SSL port...
- Sandboxing – sends unknown threats to cloud
- Palo Alto Networks®, Check Point® security systems
- Creates a new way to analyze the issue



DDOS – Volumetric Attack Mitigation

- DDOS – Distributed Denial Of Service attacks – sending a flood of traffic to your network such that it exceeds the bandwidth capacity of your carrier circuits or network gear
- Can be purchased on internet with a credit card for \$100, 2Gb for 30 minutes
- Mitigation:
 - Have bigger capacity circuits and gear than the typical attack
 - “Black-hole” the target IPs
 - Pay a traffic cleaning service, Radware, Prolexic Technologies, AT&T®, Merit Networks, XO™ Communications, etc.
 - Don’t be a target... “security by obscurity” (this is really hard)
- Many other flavors of DDOS (i.e., non-volumetric, etc.)

IPAM – IP Administration and Management

- Is a means of planning, tracking, and managing the Internet Protocol address space used in a network – a.k.a. DDI – DNS DHCP IPAM
- The key is to create security event correlation – single picture of net space
- Integrates DNS and DHCP
- Gives a centralized location to manage from
- IP address tracking – can make it harder to go back and find
- Helps you clean up orphan IPs and apply a consistent set of rules for a given network or subnet
- BlueCat™, SolarWinds®, Infoblox®, Windows



Secure DNS (Domain Name System)

- DNS provides a mechanism for resolving host names into IP addresses
- Secure DNS is done through security extensions to increase security
- DNSSEC allows DNS servers to talk to each other using certificates
- Helps to make sure only authorized systems are able to make changes/updates to other DNS
- Many systems do this:
 - BlueCat™
 - Microsoft®
 - Infoblox®



Password Policies

- The most difficult/important part of Cyber Security training
 - Authentication - AD (Active Directory), LDAP, SAML, 802.1x, RADIUS, etc...
- Password policies
 - Never use same password for separate accounts
 - Password history – enhance security by ensuring old passwords are not reused continually
 - Create maximum password age – time a password can be used before requiring user to change it
 - Complexity requirements – password length and character requirements (caps, special, numeric)
- Account lockout policies
 - Duration – number of minutes a locked out account remains locked before becoming unlocked
 - Threshold – how many invalid attempts before user is locked out
 - Reset – how many minutes must elapse after failed logon before threshold counter is set back to zero
- Security options
 - Prompt user to change password prior to expiration – determine how many days in advance
 - Number of logons to cache in case domain controller is not available
- Recent Changes: NIST to emphasize “Pass Phrase Length” only!



Multi-factor Authentication

- A requirement that users provide more than one form or method of authentication from independent categories of credentials to verify a users identity for login or other transactions
- Important for mitigation – passive compared to password change
- Phone/email/security questions
- Types:
 - Password/Pin
 - Prox Card
 - Biometrics
 - RSA key
 - Multi-device verification – smartphone



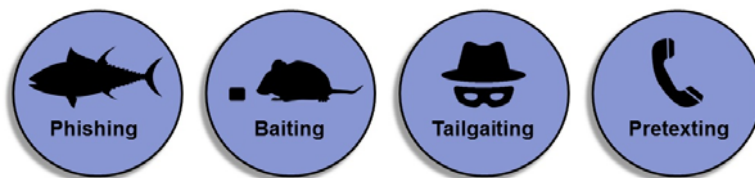
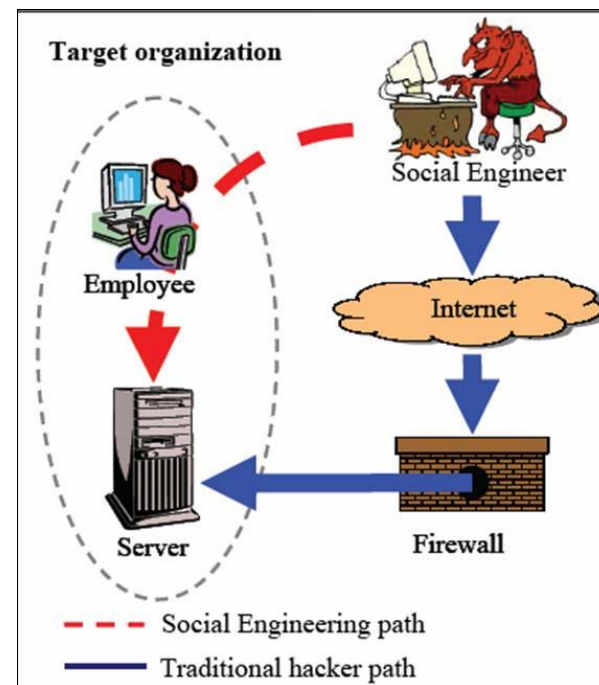
Password Lockers

- A secure password management program, which saves in one location:
 - Passwords
 - Recovers passwords
 - Form-fill internet user names and passwords
- Web-based options – store passwords in encrypted databases in the cloud – more vulnerable
 - LastPass, Secure Auth, others
- Local password managers – store encrypted passwords in a file on a device – not as convenient – lack of accessibility
 - KeePass
 - 1Password
- Secret Server – web-based – dual-authentication
- Key to success of a password change policy



Social Engineering Training

- Attacker uses influence and persuasion to deceive – through convincing/manipulating individuals, e.g., phishing
- UBA – User Behavioral Analysis (Varonis®)
- Physical “pen” testing (penetration)
- Preventative actions (SANS Video Library)
 - Employee awareness training
 - Non disclosure agreements
- Develop policies and procedures
- Humans are the weakest security link



Development of an Enterprise Security Policy

- Define what is and is not acceptable
- Policies, Procedures, Guidelines
 - Collection of controls and security measures to protect information assets
 - Data classification
- Incorporate security practices from different organizations
- Risk Analysis – need to understand the security risks an enterprise is facing
- Response Management – detailed and mandated response policy – “say what you do and do what you say!” consistency is key!
- Audit compliance, eDiscovery, regulators
- NIST and SANS are tools that can facilitate the development of an enterprise security policy



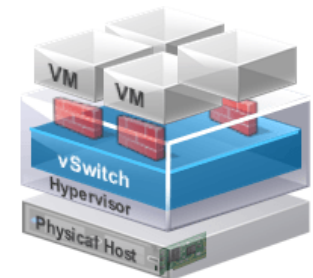
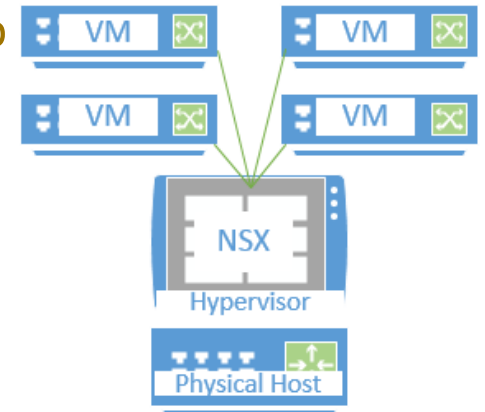
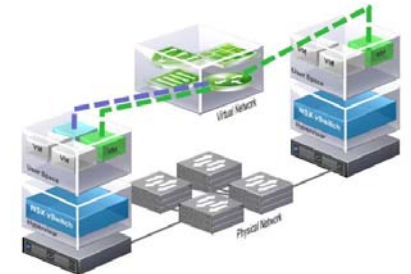
Virtualization – Security is Changing...

- Security is no longer defined between ports or physical devices but between software programs – security exists in the hypervisor fabric/layer
- SDN (Software Defined Networking) – networking functions can be parameterized, merged, or relocated by programming or copying files rather than re-plumbing hardware
 - vSwitches, vRouters, vFirewalls, etc.
- A virtual appliance sits on each blade or in the hypervisor, and protects all VMs (VSI & VDI) on that blade – rather than a client on every VM
 - Trend Micro™ is a malware scanner that exists as a virtual appliance on a host and scans all VMs
- Impact of servers and desktops in the same “virtual net space”
- Allows software to run separately from underlying hardware
- All Windows desktops security patches are up-to-date automatically
 - Newly created servers or desktops automatically will have the same updates
- Reduces IT costs through policy-enabled workflow automation



Micro-Segmentation

- Divides a network into “unit level” zones and provides protection by making security adaptive and multilayered
 - Adaptive, because security rules attach to VMs or groups of VMs – creating a no unmanaged traffic network
 - Security rules can be defined for a class of servers as a group
 - Reduces firewall maintenance because when a VM goes away, its firewall rules automatically go away with it
 - Much cheaper than providing physical firewalls between servers
 - No host-to-host traffic without security policy control
- Provisions services closer to the applications
- Used to limit “east-west” traffic (server-to-server); i.e., unauthorized lateral movement
- VMware NSX® – reduces the time to provision multi-tier networking and security services from weeks to seconds
- VMware® vRealize Network Insight & Log Insight for network design and search engine-like troubleshooting



The Changing Security Landscape

Signature-based

Focused on “known bad” threats

- Antivirus
- IPS
- Vulnerability management

Challenges

- Narrow focus
- Misses zero-day threats

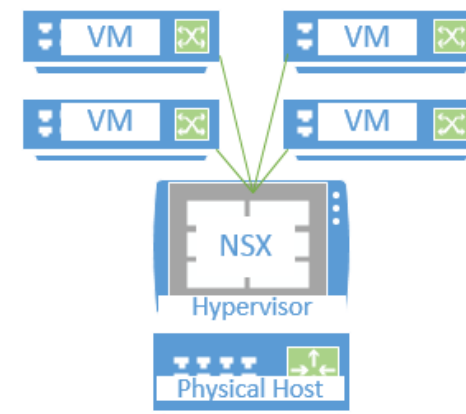
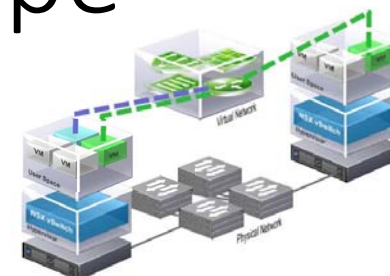
Behavioral/Forensic

Focused on “unknown bad” threats

- Machine learning
- AI
- Security analytics
- SIEM

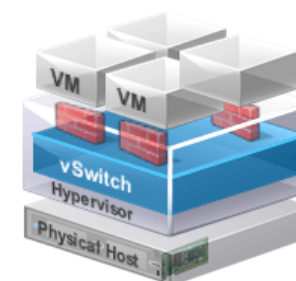
Challenges

- Broad focus
- High false positive rate



Let’s “Flip it” and focus on the “known good!”

- Automated collection of intended state across app lifecycle
- Compare intended state against run-time state to detect deviations



The Changing Security Landscape

VMware® App Defense™

Automated collection
of intended state
across app lifecycle

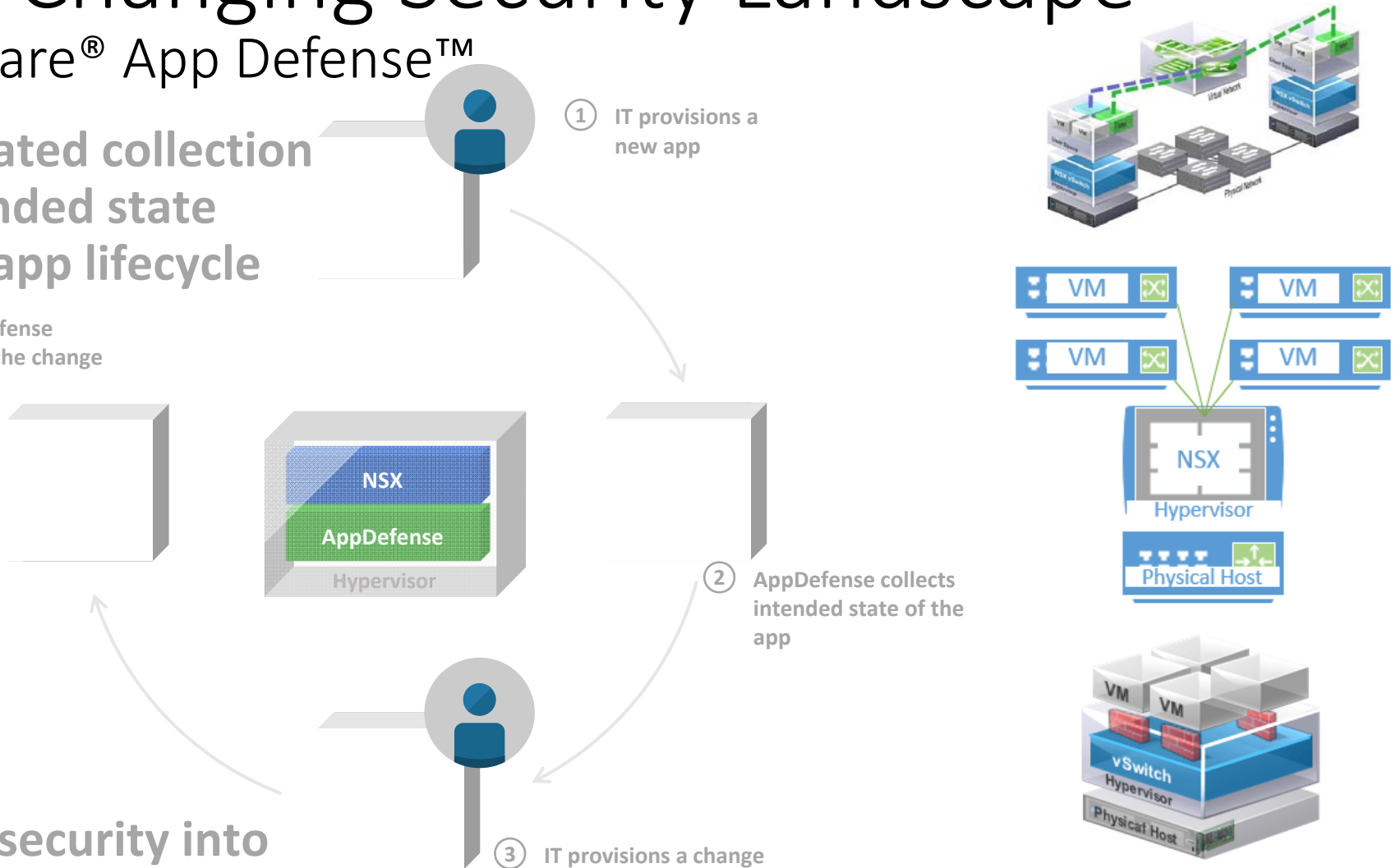
④ AppDefense
notes the change

Insert security into
DevOps process

① IT provisions a
new app

② AppDefense collects
intended state of the
app

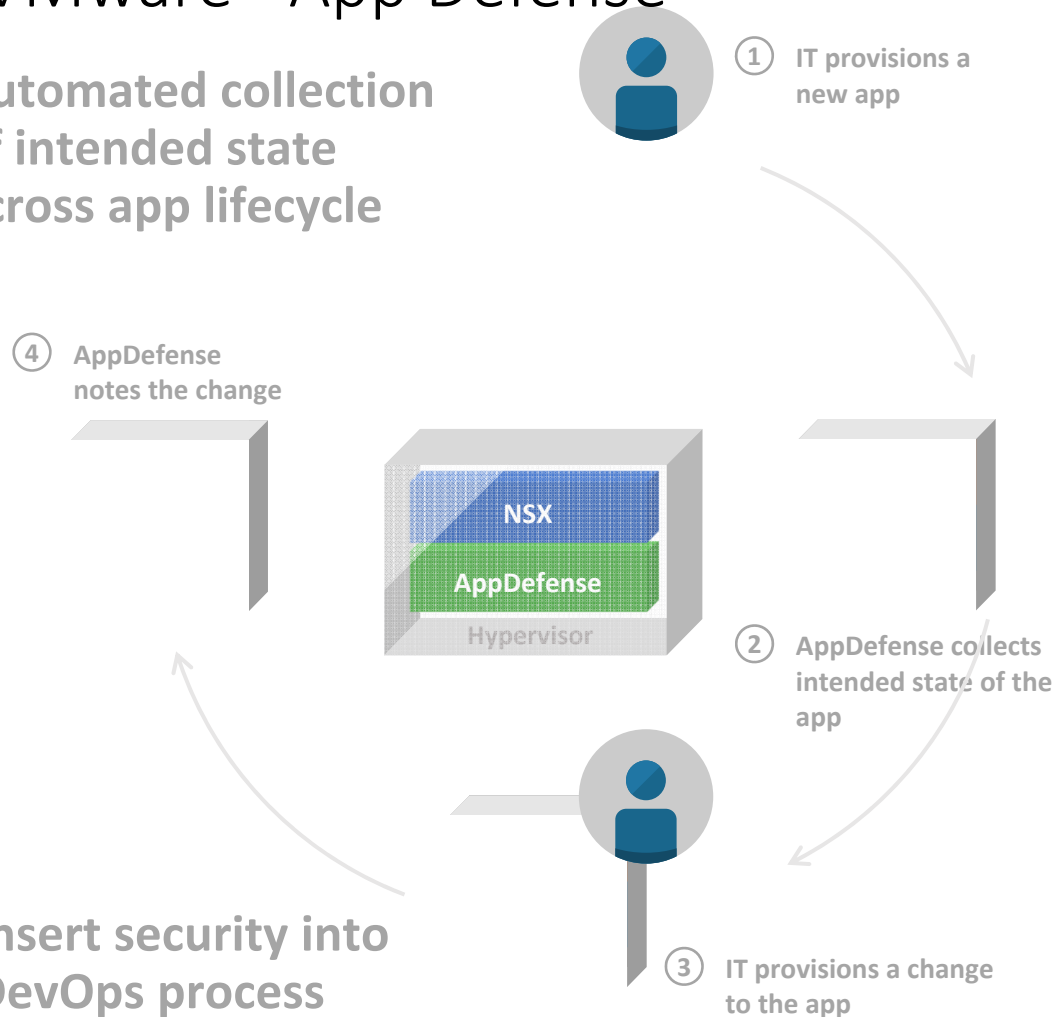
③ IT provisions a change
to the app



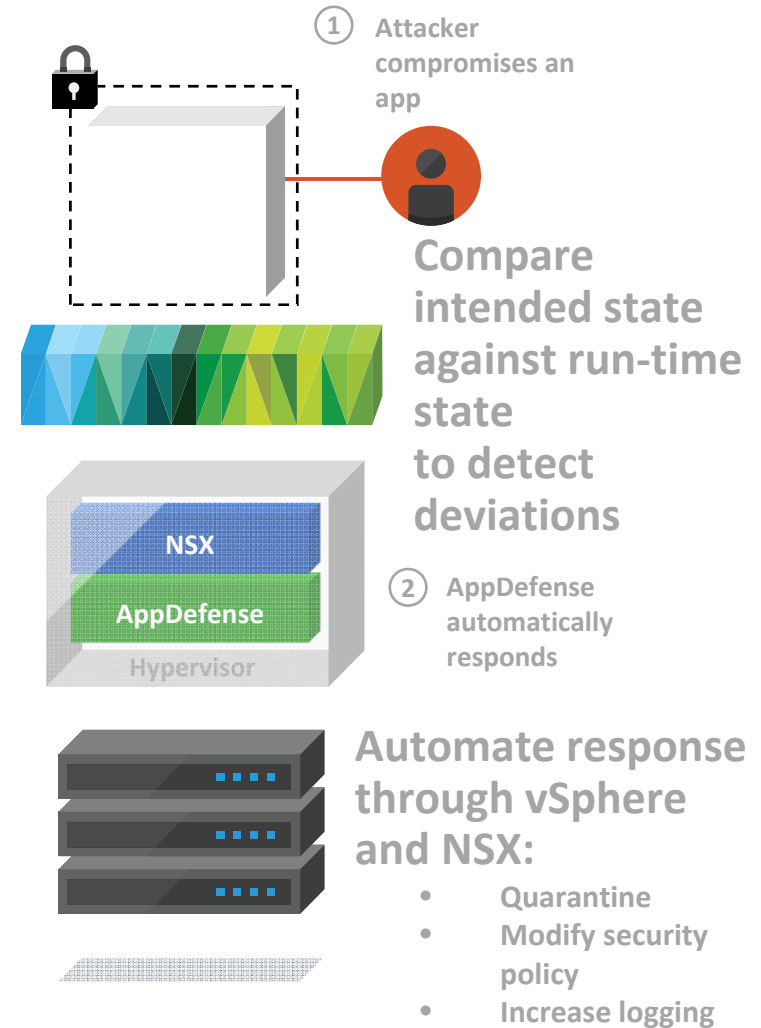
The Changing Security Landscape

VMware® App Defense™

Automated collection
of intended state
across app lifecycle



Insert security into
DevOps process

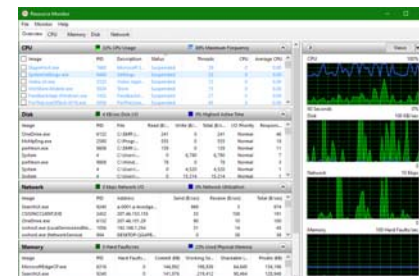


SDN - Software Defined Networking

- Open networking foundation
- Allows network administrators to be more agile and flexible in the management of network services
- Accelerates application deployment and delivery
- Reduces IT costs through policy-enabled workflow automation
- Allows software to run separately from underlying hardware
- Architecture in layers
 - Application
 - Physical Network
 - SDN Controller
- VMware NSX®, Cisco® Secure Access Control System, SDN

Monitoring – Analysis – Correlation

- Security Information and Event Management (SIEM) – is an approach to security management that seeks to provide a holistic view of an organization's information technology security
- Log and Event Correlation – if unauthorized user is added to a group; SIEM sends an alert to the security team
- Logging Analysis Tool – gives an analyst tools to create correlation events for detecting unwanted activity on the network
- Network Visibility – gives a view of logs and events from different systems from a central location
- Record Management
- Use with NGFW for heuristic correlation
- McAfee™, Intel®, Splunk®, LogRhythm®



Parting Thoughts...

- This presentation is a technological survey... not a strategy
- Just because you can... doesn't mean you should! What's the problem?
- The most important thing to start with in security is the fundamentals:
 - Strong user authentication – password complexity/change policy
 - Up-to-date patching on all systems – particularly endpoints
 - Encryption everywhere you can
- Prioritization: locate your private data, define most common attack vectors to that private data (how it would be accessed), and invest in technologies that mitigate attacks along those vectors
- Regardless of what technologies you decide to implement, make sure your personnel can digest and react to the output of those technologies ON AN ONGOING BASIS – most big breaches ignore warnings from some of the security systems described in this presentation

CYBER INSURANCE?

Is it a replacement for Security Technology!

- Many claims are denied
- Covers needed Identity Protection services for Victim, but not law suit awards
- Trend is away from cyber insurance
- Is it really the answer to “The Question?”

QUESTIONS?

Thank you for your attention!