Transforming Security Part 2: From the Device to the Data Center

**John Britton**
Director, EUC Security
VMware
@RandomDevice
The datacenter as a hospital
Digital transformation impacts IT and security
“We believe that data is the phenomenon of our time. It is the world’s new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry.

If all of this is true – even inevitable – then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world.”

- Ginni Rometty, IBM Chairman, CEO and President
60% of employees would prefer to use a personal device for work and play.

- Increased Productivity
- Greater Business Efficiency
- Improved User Satisfaction
- Greater Engagement
Of organizations rely on their users to protect personally owned devices.

>50% of employees have received no instruction in the risks of using their own devices at work.
How do we secure the interaction between users, applications, and data...

We have a large and growing surface area that needs to be secured
Who is my USER teenager?

Identity Management
• Shadow IT
• Unknown applications
• Unknown data locations
• Unknown security

65% of consumers download business-specific apps for more convenient access to information.
How do we secure the interaction between users, applications, and data...

We have a large and growing surface area that needs to be secured
Who is my User?

User

- Employee
- Contractor
- Customer
- Privileged
- R&D
- Sales
- Marketing
What tools does my User carry?

Device

- iOS
- Win10
- Android
- Unmanaged
- Managed
- BYOD
- Corp Issued
What Applications does my User use?

- Web
- Mobile
- Virtual
- Low Security
- High Security
- External
- Internal
How is my User connecting?

Network

- In Network
- Out Network
- Low Beacon
- 3G/4G
- Geo
What is my User doing?

Data

- Copy/Paste
- Passcode
- Open-In
- Watermark
- Encryption
- Expire
The User
How do we solve the problem?

- Conditional Access
  - More Restrictive Authentication
- Constrained Actions
- Limited Access
- Adaptive Management
What have they done?
Security is an Endpoint Problem

[Logos of Heartbleed, Target, Home Depot, SONY, Anthem, and JPMorgan Chase & Co.]
What does the data say about security issues?

- 80-90% of security issues could be mitigated with implementation of best known methods (Configurations, Patching)

- 10% of security issues are advanced and require enhanced intelligence and approaches
The simplest questions are sometimes the hardest...

How many assets do I have on the corporate network?

“Government agency couldn't transition 1,300 of its workstations from Microsoft Windows XP to Windows 7 because the agency couldn't find them all”
If you don’t know how many, how do you answer...

How many of the assets on my corporate network are impacted by the vulnerability that was just announced?
50% of employers will require employees to use their own devices for work.
The Uncomfortable Reality – An Example

- **30,633** number of known, managed endpoints
- **8,998** number of discovered unmanaged assets
- **6,335** number of SCCM clients not communicating
- **77%** percent missing six or more critical updates
- **91%** percent of endpoints with a vulnerable version of Adobe Flash

Source: Findings during Tanium security hygiene assessment
Key Challenges

- Data Accuracy, Timeliness, and Completeness
- Security Hygiene
- Barriers between Security and IT Ops
- Reaction Time
- Complex Architecture
- Infrastructure and Agents
Next Generation Threat Detection and Remediation

<table>
<thead>
<tr>
<th>Ask</th>
<th>Know</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>a question in plain English</td>
<td>what is happening on your endpoints at all times</td>
<td>by changing all of the impacted endpoints as needed</td>
</tr>
<tr>
<td>Google for IT Data</td>
<td></td>
<td>Deploy a Patch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kill a Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Uninstall an Application</td>
</tr>
</tbody>
</table>

- **Ask**: What are the computer names of the machines with critical patches missing?
- **Know**: In 15 Seconds
- **Act**: Deploy a Patch, Kill a Process, Uninstall an Application
Unparalleled IT Asset Visibility

- Live software asset inventory and utilization data
- Detailed and up-to-date resource utilization data from all environments
- Unmanaged asset discovery without network impact
- Enrich your existing systems with TrustPoint for complete enterprise-wide visibility
Unmatched Efficiency and Accuracy for IT Operations

- Faster, easier, more reliable patching across cross-platform environments
- Incident/problem scoping and remediation with live and recorded endpoint data to fix outages
- Distribute software and endpoint configurations at scale across multiple platforms
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.) Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through
To pay the fine, you should enter the digits resulting code, which is located on the back of your code in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
Why is Enterprise a Target

Any mission critical asset can be held ransom

Large amounts of data

Vulnerable Applications

Revenue stream for criminals

Ransom has been paid
How can the enterprise prevent ransomware

User Education

Comprehensive Backup System

Limit Lateral Movement

Patching

Host Based Security

Content Scanning
How to solve this complex problem

- Patch and secure the end user device
- Zero Trust with Micro-segmentation
- Containing Lateral Movement with Automation
- Virtualizing the End User Computing Environment
A converged infrastructure means virtual desktops run on the same infrastructure as servers...

Bringing desktops into the data center opens up new risks for attack.

And a matrix of policies is needed on centralized, choke-point firewalls for the correct security posture.
Micro-segmentation simplifies network security:

- Each VM can now be its own perimeter
- Policies align with logical groups
- Prevents threats from spreading
Simplify VDI and creates a Zero Trust environment

- Firewall and filter traffic based on **logical groupings**
- **Simplified, programmable, automated** application of network/security policy to desktop users/pools
- **Service-chaining** with AV and NGFW partners to deliver automated, policy-integrated AV / malware protection, NGFW, IPS, etc.
Contain Lateral Movement with Behavior Detection

Recomposable Virtual Desktops and Segmentation

Hypervisor Enforced Security
Where were you last night?
Privacy Concerns Affect Adoption

End User Privacy Concerns + Inability to Abide by Regulations → Lack of Adoption
Privacy is a Regulatory Issue for Organizations

- Depending on where data is collected, organizations may be subject to data residency laws.
- Handling of data by third-party analytics groups may violate regulations depending on method of data transfer.
Takeaways

- Privacy is a growing concern for end users
- Privacy concerns often affect end user adoption
- Privacy is a regulatory issue for organizations
- Privacy Controls for Organizations enable compliance with privacy laws and regulations
- Have clear communication to mitigate the effects of negative media via our Transparency to End Users approach
- Occasionally revisiting your privacy configuration page ensures accurate data collection practices
- Educate end users about the AirWatch tools such as the user and Privacy app

Privacy is a regulatory issue for organizations. Privacy concerns often affect end user adoption. Have clear communication to mitigate the effects of negative media via our Transparency to End Users approach. Occasionally revisiting your privacy configuration page ensures accurate data collection practices. Educate end users about the AirWatch tools such as the user and Privacy app.
Comprehensive Endpoint Security with VMware

- **Predict Threats**
  - IOC Detect

- **Prevent Impact**
  - Deploy Patches
  - Kill Processes
  - Uninstall Apps
  - Re-image Devices

- **Detect Incidents**
  - Harden OS
  - Client Health Attestation
  - Data Loss Prevention

- **Respond Quickly**
  - 15-sec Visibility & Control
  - Process-level Accuracy
  - Visibility at Scale

- **Visibility and Compliance**
  - 45

- **Policies and Management**

---

*RSA Conference 2017*
Top 5 Reasons VMware End User Computing (EUC) is Better

Multi-cloud Desktops and Applications Delivered

Unified Endpoint Management
- OS/App Lifecycle Management
- Asset Analytics Tracking, Inventory
- IT Automated Workflows
- Over the Air Configuration

Leading Virtual Apps & Desktops
- App Delivery
- User Environment Management
- Monitoring & Analytics

Identity-Defined Workspace
- One Touch SSO & MFA
- Conditional Access
- Unified App Catalog
- Productivity Apps

Comprehensive Cloud Service
- Cloud
- Hybrid
- Hosted & Remote Services
- Offline

Security
- Endpoint Security
- Identity Integration
- Micro-segmentation
- Data Loss Prevention
Transforming Security Part 2: From the Device to the Data Center

John Britton
Director, EUC Security
VMware
@RandomDevice