Ensuring Compliance using ClearPass OnGuard

bryan lechner – Security PLM
Agenda

What is Compliance?
Profiling Based Compliance
OnGuard Based Compliance
Questions
What is Compliance?
Compliance

- An Endpoint is compliant if it’s security posture meets the requirements of the Security Policy
- Applies to all endpoints connected to the network
- Compliance used to mitigate risk
- Risk based on
  - Value of asset / access
  - Level of potential attack (DDoS, Industrial Espionage, etc)
  - Risk Tolerance
Endpoints Must be Compliant
But Not All Endpoints are created Equal

• User Endpoints
  • Corporate owned
  • Windows, Mac, Linux
  • Phone, Tablet
  • BYOD

• Are all users equal
  • Different policies for
    • CIO, Engineering, HR, Reception, etc
    • Based on sensitivity and value of data or access, not position
Endpoints Must be Compliant
But Not All Endpoints are created Equal

- IoT Devices
  - Do not support Agents
  - Do not support 802.1x supplicant
  - Authorized by profiled device attributes

- If the endpoint is not compliant
  - Notify
  - Flag and quarantine
  - Open help desk ticket
  - Remediate
    - Auto remediate
    - Help user to self remediate
Is it Compliant
Different tools for Different Endpoints

• OnGuard
  • Computers
    • Windows
    • Linux
    • Mac OsX
• MDM
  • Mobile devices
• Profile
  • IoT devices
  • Subnet Scan
  • Triggered scan
Profiling Based Compliance
Mobile Device Compliance

MDM Integrations

Context server Integrations

![Add Endpoint Context Server](image-url)
# Mobile Device Compliance

## Normalized Tags

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Blacklisted App</td>
<td>false</td>
</tr>
<tr>
<td>2. Compromised</td>
<td>true</td>
</tr>
<tr>
<td>3. Description</td>
<td>Android_Amazon_Kindle_Fire_null</td>
</tr>
<tr>
<td>4. Encryption Enabled</td>
<td>false</td>
</tr>
<tr>
<td>5. Last Check In</td>
<td>2014-07-29 16:49:46</td>
</tr>
<tr>
<td>6. MDM Enabled</td>
<td>true</td>
</tr>
<tr>
<td>7. MDM Identifier</td>
<td>1371</td>
</tr>
<tr>
<td>8. Manufacturer</td>
<td>Android</td>
</tr>
<tr>
<td>9. Model</td>
<td>Android</td>
</tr>
<tr>
<td>10. OS Version</td>
<td>Android 4.1</td>
</tr>
<tr>
<td>11. Owner</td>
<td>bali</td>
</tr>
<tr>
<td>12. Ownership</td>
<td>Unknown</td>
</tr>
<tr>
<td>13. Phone Number</td>
<td>0</td>
</tr>
<tr>
<td>14. Required App</td>
<td>Installed</td>
</tr>
<tr>
<td>15. Source</td>
<td>airwatch</td>
</tr>
</tbody>
</table>
**Mobile Device Compliance**

**Actions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Label to Device</td>
<td>Apply label to identify when devices have attached to corporate Wi-Fi and apply corresponding policies</td>
</tr>
<tr>
<td>Get Labels</td>
<td>Get labels information for the device</td>
</tr>
<tr>
<td>Lock Device</td>
<td>Locks the device</td>
</tr>
<tr>
<td>Remote Wipe</td>
<td>Delete all information stored</td>
</tr>
<tr>
<td>Remove Label from Device</td>
<td>Remove label and corresponding policies</td>
</tr>
<tr>
<td>Retire/ Enterprise Wipe (Device MAC Address)</td>
<td>Delete only corporate information stored and remove device from MDM management</td>
</tr>
<tr>
<td>Retire/ Enterprise Wipe (UUID)</td>
<td>Delete only corporate information stored and remove device from MobileIron EMM management</td>
</tr>
<tr>
<td>Send Message</td>
<td>Send message to the device</td>
</tr>
<tr>
<td>Send Push Notification (UUID)</td>
<td>Send Push Notification (APNs for Apple iOS, C2DM/GCM for Google Android, WNS for Windows 8.1) message using UUID</td>
</tr>
<tr>
<td>Send SMS (UUID)</td>
<td>Send SMS Message (cellular devices only) using UUID</td>
</tr>
</tbody>
</table>
IoT Device Compliance

- Many IoT devices originally designed for isolated networks
- They were built for speed and reliability and lack security
  - No access rules
  - No key mgmt.
  - No encryption
  - No firewalls
  - Do not support Agents
  - Do not support 802.1x supplicant
- Authorized by profiled device attributes
IoT
Passive Profiling

- DHCP
  - Helper
  - Span
- TCP fingerprint
  - Span
- ARP Monitoring
  - Span
- HPPT User Agent
  - Span
- MAC OUI
- CDP
- LLDP

- Microsoft Exchange Server Active Sync Plugin
- Netflow / IPFIX
- sFlow
- SNMP MAC Notification Trap
- SNMP Link Up Trap
- EMM / MDM
- Onboard
- OnGuard
IoT
Active Profiling

Subnet Scan
- Nmap scanner
- Open ports scanner

Device Discovery
- WMI
- SSH
- SNMP Read
## IoT
### Active Scanning

### Schedule Scan

- **Scan Type:** 
  - Network Scan
  - Subnet Scan

- **Zone:** default

- **IP Subnet(s):** 192.168.1.0/24

- **Frequency of Scan:** On Demand

- **Start Time of Scan:** (optional)

---

### Endpoint Profiler

- **Total Devices:** 51405
- **Smart Devices:** 24257 (47%)
- **Computers:** 19979 (38%)
- **Other Devices:** 7169 (14%)

<table>
<thead>
<tr>
<th>Device Category</th>
<th>Device Family</th>
<th>Device Name</th>
<th>MAC Address</th>
<th>Hostname</th>
<th>Device Category</th>
<th>Device OS Family</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Device</td>
<td>Dräger</td>
<td>Dräger Medical Device</td>
<td>00:16:00:00:00:40</td>
<td>Medical Device</td>
<td>Dräger</td>
<td>Unknown</td>
<td></td>
</tr>
</tbody>
</table>
IoT Compliance
It's all about Profiling

Access Control Point

- Multi-vendor switching
- Multi-vendor WLANs

Access Rights

- PLCs
- Meters
- Vision
- Sensors

ClearPass

Device type

Contrac tors

Vision

Sensors

PLC s
Behavior Based Profiling
Does It Behave Compliantly

Which One is Different then the Others

- Users
- Devices
- IoT

Behavior monitored by

- IntroSpect
- SIEM
Policy Manager
Putting It all together

Assign Role
Notify Enforcement Point

Evaluate Compliance

Profiling Collectors
EMM / MDM
OnGuard
IntroSpect

Device Attributes
Posture
Posture
UEBA
Policy Manager
Aruba 360 Secure Fabric

Evaluate Compliance

Assign Role
Notify Enforcement Point

Risk
Posture
Attributes
Compliance

UEBA
SIEM
NG Firewall
EDR
EMM / MDM
OnGuard Based Compliance
OnGuard

Deployment Options

• Dissolvable Agent
  • Contractors
  • Guests

• Persistent Agent
  • Corporate devices
  • Managed devices
  • Download agent
  • Group policy push

• Agentless (new in 6.8)
  • Zero touch
  • Transparent to user
OnGuard Options

Regular OnGuard
- Supports Windows, macOS, and Linux
- Triggered by PostAuth
- Persistent and Dissolvable
- Run as system or user

Agentless OnGuard
- Only supports managed Windows computers
- Still requires configuration of managed systems
- Triggered by existing in Insight DB
- Does not trigger instantly, typically a couple minutes to get into/update the DB
Agentless OnGuard
High Level Process

- Configure ClearPass for Agentless OnGuard
- ClearPass detects the system on the network
- ClearPass copies small (helper) file to computer by SMB
- ClearPass executes WMI command to execute helper file
- Helper downloads new OnGuard process and executes it locally
- New process is similar to Dissolvable Agent, but has abilities of Persistent Agent
## OnGuard Deployment Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Persistent Agent</th>
<th>Dissolvable Agent</th>
<th>Agentless</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run as Service</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Run a User</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Run as Service &amp; User</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Auto-remediation</td>
<td>Yes</td>
<td>No</td>
<td>Most*</td>
</tr>
<tr>
<td>Windows support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes**</td>
</tr>
<tr>
<td>macOS support</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Linux support</td>
<td>Yes***</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>End User UI</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

* Limited to remediation available to running as a service (e.g. a system account)
** Managed Windows computers with appropriate configuration
*** Supports Ubuntu, RedHat, and CentOS without Java in 6.8
Computer Endpoints

Compliance

Restrict by Role

Role determined by Authorization

Posture Policies

- Policy Name: Sensitive Data Access
- Description:
- Posture Agent: OnGuard Agent (Persistent or Dissolvable)
- Host Operating System: Windows
- Plugin Version: 2.0
- Restrict by Roles: CXO, Sensitive Data Access
- Select or type role names

Remove

Add
Computer Endpoints
Sensitive Data Access

Policy Checks
- AV
- Firewall
- Patches / hotfixes
- USB
- VM
- Network Connections
- Disk Encryption

ClearPass Windows Universal System Health Validator

<table>
<thead>
<tr>
<th>Network Connections</th>
<th>Windows 10:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Auto Remediation:</td>
<td>true</td>
</tr>
<tr>
<td>Enable User Notification:</td>
<td>true</td>
</tr>
<tr>
<td>Network Connection Types Check Enabled:</td>
<td>true</td>
</tr>
<tr>
<td>Network Connections Allowed:</td>
<td>Allow Only One</td>
</tr>
<tr>
<td>Network Connection Types Allowed:</td>
<td>Wireless Wired</td>
</tr>
<tr>
<td>Network Connection Types Remediation Action:</td>
<td>Disable Network Connection</td>
</tr>
<tr>
<td>Allow Bridge Network Connection:</td>
<td>false</td>
</tr>
<tr>
<td>Bridge Network Connection Remediation Action:</td>
<td>Disable Network Connection</td>
</tr>
<tr>
<td>Allow Internet Connection Sharing:</td>
<td>false</td>
</tr>
<tr>
<td>Internet Connection Sharing Remediation Action:</td>
<td>Disable Internet Connection Sharing</td>
</tr>
<tr>
<td>Allow Adhoc/Hosted Wireless Networks:</td>
<td>false</td>
</tr>
<tr>
<td>Adhoc/Hosted Wireless Networks Remediation Action:</td>
<td>Disconnect Adhoc Hosted Networks</td>
</tr>
</tbody>
</table>
Computer Endpoints
Sensitive Data Access

Posture Policy
• AV
• Firewall
• Hotfixes
• USB
• VM
• Encryption
• Network Connections
Computer Endpoints
Employee Access

- AV
- Firewall
- Patches / hotfixes
- Network Connections

Posture Policies

<table>
<thead>
<tr>
<th>Policy</th>
<th>Posture Plugins</th>
<th>Rules</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name:</td>
<td>No sensitive data access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Posture Agent:</td>
<td>NAP Agent</td>
<td>OnGuard Agent (Persistent or Dissolvable)</td>
<td></td>
</tr>
<tr>
<td>Host Operating System:</td>
<td>Windows</td>
<td>Linux</td>
<td>Mac OS X</td>
</tr>
<tr>
<td>Plugin Version:</td>
<td>2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restrict by Roles:</td>
<td>Employee restricted</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Select or type role names

Remove

Add
OnGuard
Global Settings

Configure Global Agent Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Cache Credentials Interval (in days)</td>
<td>= 15</td>
</tr>
<tr>
<td>2. Enable to install VPN component</td>
<td>= false</td>
</tr>
<tr>
<td>3. Subnets for Wired access</td>
<td></td>
</tr>
<tr>
<td>4. Cache Credentials Interval (in days)</td>
<td></td>
</tr>
<tr>
<td>Delay to bounce after Logout (in minutes)</td>
<td></td>
</tr>
<tr>
<td>Enable OnGuard requests load-balancing</td>
<td></td>
</tr>
<tr>
<td>Enable access over Remote Desktop Session</td>
<td></td>
</tr>
<tr>
<td>Enable to hide Logout button</td>
<td></td>
</tr>
<tr>
<td>Enable to use Windows Single-Sign On</td>
<td></td>
</tr>
<tr>
<td>Keep-alive Interval (in seconds)</td>
<td></td>
</tr>
<tr>
<td>OnGuard Health Check Interval (in hours)</td>
<td></td>
</tr>
<tr>
<td>Run OnGuard As</td>
<td></td>
</tr>
<tr>
<td>Server Certificate Validation</td>
<td></td>
</tr>
<tr>
<td>Server Communication Mode</td>
<td></td>
</tr>
<tr>
<td>Support Team Email Address</td>
<td></td>
</tr>
<tr>
<td>Use Current OS Language (Windows only)</td>
<td></td>
</tr>
<tr>
<td>VPN Device Names (Windows only)</td>
<td></td>
</tr>
<tr>
<td>More choices</td>
<td></td>
</tr>
</tbody>
</table>

Save  Cancel
OnGuard Posture Policy
Determine if it's compliant

ClearPass Windows Universal System Health Validator

- Enable checks for Windows 10
- USB Devices
  - Remediation checks: Auto Remediation
  - User Notification
- Remediation Action for USB Mass Storage Devices
  - Remove USB Mass Storage devices

Agent and Endpoint details

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Attributes</th>
<th>Posture Info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Posture Request

- Client: Operating System: Windows 10
- OS: Service Pack: 0
- OS: Version: Windows 10
- USBMassStorageDevices: Present: E:

Posture Response

- ClientVersion: Healthy
- USBDemo: HealthStatus: Not Healthy

Posture Evaluation Results

- USBMassStorageDevices:NotAllowed: [E:]
# Profiling

## Profile Attributes

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Attributes</th>
<th>Fingerprints</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>c4346b6bba02</td>
<td>IP Address</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>Static IP</td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td>Hostname</td>
</tr>
<tr>
<td>Device Category</td>
<td></td>
<td>Device OS Family</td>
</tr>
<tr>
<td>Device Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Added By</td>
<td>Policy Manager</td>
<td></td>
</tr>
<tr>
<td>Online Status</td>
<td>Online</td>
<td></td>
</tr>
<tr>
<td>Connection Type</td>
<td>Wireless</td>
<td></td>
</tr>
<tr>
<td>Access Point</td>
<td>AP-225</td>
<td></td>
</tr>
<tr>
<td>Network SSID</td>
<td>CIPGuest</td>
<td></td>
</tr>
<tr>
<td>Last Profiled At</td>
<td>Mar 04, 2019 20:50:00 CST</td>
<td></td>
</tr>
</tbody>
</table>

**Endpoint Fingerprint Details**

- **TCP Fingerprint**: tcp:syn+ack, len=52, win=5297, tti=64, df=false, opts=mss:1382, nop: ws: 0, nop: nop: sok
- **TCP Device Category**: Hewlett-Packard JetDirect
- **Host Device Type**: |
- **Host User Agent**: |
- **DHCP Options**: 53, 61, 12, 55
- **DHCP Option55**: 6, 3, 11, 15, 66, 67, 13, 44, 12, 81, 252
Profiling
Determine if It's Compliant
All ClearPass Related Documentation
Policy Manager
Enforcing Security Policy

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Tips:Role EQUALS Registered-Device)</td>
<td>HP User or Device - VLAN 2001, Update HP Wired Endpoint Location</td>
</tr>
<tr>
<td>(Tips:Role EQUALS Phone)</td>
<td>HP Voice-SDN - VLAN 2000, Update HP Wired Endpoint Location</td>
</tr>
<tr>
<td>(Tips:Role EQUALS Access Point)</td>
<td>HP User or Device - VLAN 2001, Update HP Wired Endpoint Location</td>
</tr>
<tr>
<td>(Tips:Role EQUALS Network Device)</td>
<td>HP User or Device - VLAN 2001, Update HP Wired Endpoint Location</td>
</tr>
<tr>
<td>(Tips:Role EQUALS Computer)</td>
<td>[Deny Access Profile], Update HP Wired Endpoint Location</td>
</tr>
<tr>
<td>(Tips:Role EQUALS Unknown Device)</td>
<td>HP Profiling - VLAN 4000, Update HP Wired Endpoint Location</td>
</tr>
</tbody>
</table>
Compliance Reports and Alerts
Insight - Dashboards

<table>
<thead>
<tr>
<th>Count</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>77</td>
<td>OnGuard Devices</td>
</tr>
<tr>
<td>50</td>
<td>Healthy OnGuard Devices</td>
</tr>
<tr>
<td>27</td>
<td>Unhealthy OnGuard Devices</td>
</tr>
<tr>
<td>64%</td>
<td>Healthy OnGuard Device Percentage</td>
</tr>
<tr>
<td>35%</td>
<td>Unhealthy OnGuard Device Percentage</td>
</tr>
</tbody>
</table>

Unhealthy OnGuard Device Distribution across Device Family

OnGuard Device Distribution across Health Status

Windows (36)
Apple Mac (11)
## Compliance Reports and Alerts

### Insight – Detail

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>User</th>
<th>SPT</th>
<th>Authentication</th>
<th>Authentication At</th>
<th>Hostname</th>
<th>Agent Version</th>
<th>Agent Type</th>
<th>Added At</th>
</tr>
</thead>
<tbody>
<tr>
<td>9405b65c82f7</td>
<td>owenj</td>
<td>HEALTHY</td>
<td>User</td>
<td>2/8/18 5:21</td>
<td>WIN7-CP-01</td>
<td>&quot;6.6.8.100017&quot;</td>
<td>&quot;OnGuardAgent&quot;</td>
<td>8/25/17 8:24</td>
</tr>
<tr>
<td>001c42bf3a0c</td>
<td>001c42bf3a0c</td>
<td>HEALTHY</td>
<td>None</td>
<td>2/10/18 22:33</td>
<td>YONGCHUANGO77C5</td>
<td>&quot;6.6.8.100017&quot;</td>
<td>&quot;OnGuardAgent&quot;</td>
<td>2/10/18 22:06</td>
</tr>
</tbody>
</table>
Compliance Reports and Alerts
Policy Manager Dashboard
Rate this session
Access this survey via the mobile app and let us know what you think.

Locate this session:
- Agenda
- Select Date
- Find this session
- Click Survey

Download the Event App
Gain access to the latest event information.
Join the Airheads Community
Scan the QR code to sign up now!

Ask Aruba
- Session 1: Tuesday, 24 Sep, 2:00pm – 2:45pm
- Session 2: Wednesday, 25 Sep, 1:45pm – 2:30pm
- Location: Town Hall at Tech Playground
Submit your Ask Aruba questions using the mobile app now!

Scan. Play. Win.
Play Now! Switch your thinking, say goodbye to the old ways and get ready for new innovations.
Visit the Tech Playground now!
Thank You