CONTINUOUS COMPLIANCE

Shifting from checking the box to real-time threat detection and response
After I drink coffee I like to show the empty mug to the IT guy to tell him that I've Successfully installed JAVA. He hates me!
Agenda

Continuous Compliance

- Introduction to the Compliance Objectives
- Current Vulnerabilities and Risks
- Current Compliance Reg’s and Best Practice
- Compliance Frequent Use Cases
- Best of Breed Security
- Demo Show Casing Use Cases
Arm Your Endpoints and Achieve Continuous Compliance

- **Real time Visibility** of in-scope systems and events
- **Control** over critical changes and system events
- “**Active Intelligence**” to Measure risk and Prioritize events

- Complete **Protection from ALL malware threats** on every in-scope system and beyond
- **Immediate Enforcement and Audit** of security compliance policy and BAUs
Merge Compliance and Security

You must validate both compliance and security with controls that:

1. Identify, Classify & Scope and Critical Business Processes
2. Monitor & Prevent Change
3. Measure, Identify & Analyze Risk
4. Detect & Prevent Malware
5. Actively Enforce Policy

1. Real Time Visibility
2. Stop Analyzing Change and Start Controlling it
3. “Active Intelligence” and Always-on Monitoring
4. Complete Protection from ALL Malware Threats
5. Immediate Enforcement and Audit of Security Compliance Policy

Achieve Continuous Compliance and Strengthen Your Security Profile
Current Vulnerabilities and Hazards
Security Challenges Facing Every Company Today

Traditional endpoint prevention does NOT stop targeted attacks

“Malware threats continue to overwhelm traditional defensive techniques.”

Gartner Research

Detection and Response take too long and cost too much

Mean Time to IDENTIFICATION: 256 days*
Mean Time to CONTAINMENT: 82 days*

Compliance is an extraordinary burden and expense

71% Businesses fell out of compliance within a year of audit**

** Verizon 2015 PCI Compliance Report
• 58% of businesses do not have a fully mature patch management process in place, and 12% do not have a patch management process in place at all.

* Trustwave 2014 State of Risk report

• Even if support package is purchased from MS you do not get the moderate and low patches only critically deemed ones.
The absence of vulnerability and security patches leaves businesses at risk for **satisfying compliance requirements** (PCI, HIPAA) and increases company-wide **LIABILITY**.

**Examples:**

- **PCI Requirement 6.2:** *update all critical in-scope systems with the latest security patches within 30 days.*
Cost of Support

• The estimated cost of premier support per 2K3 endpoint system is 3x cost of XP:
  *Taken from Microsoft yearly Premier Support

  • $200 per PC for the first year = $600
  • $400 per PC for the second year = $1200
  • $1,000 per PC for the third year = $3000

• Premier support provides:

  • **Critical patches only**
  • **Important patches are available at an additional price.** Historically, Microsoft labeled many patches as ‘important’ that should have been labeled as ‘critical’
  • No support for moderate-or low-priority security updates = **Widening Threat Window**
Windows Server 2003 End-of-Life Survey

Completed in March 2015, based on 500 IT leaders at medium and large enterprises in the US and UK:

- 34% of organizations are still using a combination of Windows XP and Windows Server 2003.

- Another 10% of organizations continue to use Windows XP exclusively.

- 30% plan to continue to run WS2K3 after the July 14 deadline, leaving an estimated 2.7 million servers unprotected.

- 57% of enterprises do not know when the end of life deadline is.

- 14% of enterprises do not yet have an upgrade plan for WS2K3
### No End to EOL Scenarios in Sight

<table>
<thead>
<tr>
<th>Operating System</th>
<th>EOL Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP Embedded SP3</td>
<td>Jan 2016</td>
</tr>
<tr>
<td>Windows Embedded for Point of Service SP3</td>
<td>Apr 2016</td>
</tr>
<tr>
<td>Windows Embedded Standard 2009</td>
<td>Jan 2019</td>
</tr>
<tr>
<td>Windows Embedded POSReady 2009</td>
<td>Apr 2019</td>
</tr>
</tbody>
</table>
Third Party Risk – Do you know TPISA?

• 68% of businesses transfer sensitive data between locations; 58% of businesses use third parties to manage sensitive data, yet almost half (48%) do not have a third-party management program in place. Trustwave 2014 state of risk report

Things to consider in your TPISA Program:

• Full data lifecycle analysis
• GRC programs for managing risks and contract changes
• Escrow agreements and contract language
• SSAE16 standardized review and reporting
• Use cases and certifications
POS and ATMs

CNN Money ATM Bank Hacking

Servers

Block execution on every system

Terminals

Block execution on every system

Card Reader

Block execution on every system

Backend Servers

Block execution on every system

Loyalty Servers

Block execution on every system

Transactional Data servers

Payment Processors
And Integrate Systems
Current Compliance Requirements and Best Practice Standards for Continuous Monitoring
Regulations with a Big Bite

- PCI
- NERC
- FISMA
- HIPAA
- Sarbanes-Oxley Act
The Compliance Impact

Questions to Consider

✔ Is your organization held to any compliance regulations or standards?

✔ How does your organization validate and measure its compliance posture and risk to that posture?

✔ How does your organization control in-scope assets and collect compliance information?

✔ Does your organization use a 3rd party assessment entity? Who is that entity, and what do they provide to help meet compliance?
The Payment Card Industry Data Security Standard is designed to protect cardholder information.

Compliance with PCI-DSS is mandatory for all organizations dealing with credit, debit and ATM cards, as defined by the PCI Security Standards Council.

PCI-DSS is comprised of 12 major requirements that aim to considerably strengthen the security of the cardholder information that the organization manages and/or transacts.

Cost of non-compliance or breach:
- Loss of credit card privileges
- Loss of brand confidence and image
- Financial loss due to reoccurring fines and penalties
- Financial loss due to re-assessment costs
PCI DSS is full of Opportunities

- 100% of Companies that were breached in 2015 were non-Compliant
- 100% of Companies Were Failing Compliance

0 IN TEN YEARS

“Of all the companies investigated by our forensics team over the last 10 years following a breach, not one was found to have been fully PCI DSS compliant at the time of the breach.”
Industries and Sectors Where you’ll find PCI DSS:
- Retail / Finance / Healthcare
- Chain Restaurants
- Department / Large Stores
- Gas Stations, Convenience & Liquor Stores
- Hospitality / Resorts / Casinos
- Hospitals
- Pharmacies and Pharmaceutical
- Banks and Insurance Companies
- Educational Institutions
HIPAA

- The Health Insurance Portability And Accountability Act is designed to protect the confidentiality and security of patient information.
- HIPAA regulations were established to protect the integrity and security of health information, including protecting against unauthorized use or disclosure of the information.

Cost of non-compliance:
- Civil and criminal penalties
- Financial loss due to fines even if the loss of data was not willful
- Investigations and internal audits in the event of a loss

- According to the Fifth annual Ponemon study research, the average cost of a data breach for healthcare organizations is estimated to be more than $2.1 million.
SOX/GLBA

- The Sarbanes-Oxley Act of 2002 requires all public companies and public accounting firms to show the auditors the accuracy of their financial reporting.
- SOX requires companies to implement processes and controls to protect financial data.

Cost of non-compliance:
- Financial loss due to fines
- Criminal penalties including imprisonment
- Brand loss due to data leakage
NERC/FERC CIP-005-1-R1.6 states that “an electronic Security Perimeter should be established that provides . . . Monitor and Log Access 24X7X365.”

FISMA/FISMA 2—FISMA and FISMA 2 also require continuous monitoring activities that include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting.
NIST and ISO

- **NIST 800-53:**
  
  describes automated inspection items in connection with a CA-2 (security assessment), CA-4 (security certification) and CA-7 (continuous monitoring and vulnerability detection) continuous monitoring program.

- **ISO/IEC 27001:**
  
  provides a description of an information security management system that calls for continual process improvement in information security. To accomplish this goal, an organization must continuously monitor its own security-related processes and improve according to feedback from objective measurements.
Security Monitoring:

- Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by monitoring network and host activity to identify policy violations and anomalous behavior;

- **Monitoring** host and network condition to identify unauthorized configuration and other conditions which increase the risk of intrusion or other security events;

- Analyzing the results of monitoring to accurately and quickly identify, classify, escalate, report, and guide responses to security events; and

- Responding to intrusions and other security events and weaknesses to appropriately mitigate the risk to the institution and its customers, and to restore the institution's systems.
FFIEC Cybersecurity Assessment Tool

Maturity Assessments

The FFIEC tool helps to determine the maturity of your organization's cybersecurity practices. It provides a structured framework to assess and improve your cybersecurity posture. The tool includes a maturity assessment matrix that categorizes your organization's cybersecurity capabilities into five levels: awareness, development, implementation, measurement, and optimization.

FFIEC Cybersecurity Assessment Tool: An Annotated Guide
FFIEC Cybersecurity Assessment Tool

Inherent Risk Profile

- Low Inherent Risk
- Minimal Inherent Risk
- Moderate Inherent Risk
- Significant Inherent Risk
- Most Inherent Risk

Cybersecurity Maturity

Domain 1: Cyber Risk Management & Oversight
Domain 2: Threat Intelligence & Collaboration
Domain 3: Cybersecurity Controls
Domain 4: External Dependency Management
Domain 5: Cyber Incident Management and Resilience
Benefits to Institutions

• Identifying factors contributing to and determining the institution’s overall cyber risk

• Assessing the institution's cybersecurity preparedness.

• Evaluating whether the institutions cybersecurity preparedness is aligned with its risks

• Determining risk management practices and controls that could be taken to achieve the institutions desired state of cyber preparedness

• Informing risk management strategies.
How to use the CAT

1. **Gather Information**
   - Select a planning committee for business unit alignment and information gathering.

2. **Complete Inherent Risk Profile**
   - Answer with accuracy and define thresholds for risk appetite.

3. **Calculating Risk Maturity Relationship**
   - Define desired maturity levels and map achieved targets.
   - Update as frequently as possible the inherent risk profile or maturity questionnaire when anything changes.

4. **Domains 1 - 5 Cyber Security Questionnaire**
   - Ensure business lines agree on responses and identify automated sources of information.

5. **Update for Changes**
   - Update for changes.
SANS – Top 20 Controls

CIS Critical Security Controls for Effective Cyber Defense Now

• 20 controls on actionable ways to prevent cyber attacks.

• Realized need for continuous monitoring and detection.

• Provide quick wins on how to achieve a majority of the control to combat the vulnerability.
Frequent Compliance Uses Cases
## Compliance Use Case:

### File Integrity Monitoring and Control

<table>
<thead>
<tr>
<th>Compliance Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>• PCI-DSS</td>
</tr>
<tr>
<td>• HIPAA</td>
</tr>
<tr>
<td>• SOX/GLBA</td>
</tr>
<tr>
<td>• NERC-CIP</td>
</tr>
<tr>
<td>• CSC 20</td>
</tr>
<tr>
<td>• Aus DOD 35</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ideal Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satisfies the requirement outright for multiple Regulations and Best Practices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best of breed Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrow your scope and identify critical change</td>
</tr>
</tbody>
</table>
Compliance Use Case:

Proactive Monitoring of Endpoints for Events and Incidents

Compliance Area
- PCI-DSS
- HIPAA
- SOX/GLBA
- NERC-CIP

Ideal Solution
Augments many individual requirements in many regulations
Helps consolidate overlapping technologies

Best of Breed Security
Continuous monitoring for real time threat alerts and prevention.
### Compliance Use Case:

**Replacement or augmentation (compensating control) for malware protection**

<table>
<thead>
<tr>
<th>Compliance Area</th>
<th>Ideal Solution</th>
<th>Best of Breed Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• PCI-DSS</td>
<td>Can be used to replace AV or to re-enforce protection and compliance</td>
<td>Next Gen Endpoint security</td>
</tr>
<tr>
<td>• HIPAA</td>
<td>Protection as certified Compensating Control</td>
<td>Block all unknown and bad from running</td>
</tr>
<tr>
<td>• SOX/GLBA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NERC-CIP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Compliance Use Case:**

- **Enforcement and protection of unsupported systems**

<table>
<thead>
<tr>
<th>Compliance Area</th>
<th>Ideal Solution</th>
<th>Best of Breed Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI-DSS</td>
<td>Goes above and beyond original security requirement for EOL</td>
<td>Lock down legacy systems in High enforcement</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Compliance cycle post migration</td>
<td>Monitor and alert on policy in real time</td>
</tr>
<tr>
<td>SOX/GLBA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NERC-CIP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSC 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 27001</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Best of Breed
Compliance
Security
Leverage Security Controls for Clarity of Regulatory Policy

Visibility and control
Eliminate the noise associated with monitoring controls like File Integrity Monitoring and immediately identify critical changes

Proactive analysis of risk on in-scope endpoints
Proactive monitoring for of regulatory scope - Gain immediate Risk, threat and trust measure across the entire enterprise

Positive posture or trust-based malware protection
Replacement and enhancement of malware protection - Eliminate the burden of negative technologies and the maintenance associated

Enforcement and protection of all in-scope systems in-scope - BA and CE
Ensure total enforcement, compliance, and audit with security policy; Move from patch mitigation to threat mitigation
## From Checking the Box to Becoming Innovative in Security

<table>
<thead>
<tr>
<th></th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Visibility</strong></td>
<td>None</td>
<td>Polling, scanning</td>
<td>Real-time visibility &amp; continuous recording of endpoint state</td>
<td>Real-time visibility &amp; continuous recording of endpoint activity</td>
</tr>
<tr>
<td><strong>Detection</strong></td>
<td>AV signatures, Only detects known malware</td>
<td>Reputation data, Algorithms</td>
<td>Single-source threat intelligence, Simple indicators</td>
<td>Aggregated, multi-vendor threat intel, Patterns and behavior</td>
</tr>
<tr>
<td><strong>Prevention</strong></td>
<td>AV signatures, Only stops known malware</td>
<td>Remove admin rights, Basic whitelisting, Anti-exploitation</td>
<td>Custom bans</td>
<td>Policy-based default-deny, Customizable forms of prevention</td>
</tr>
<tr>
<td><strong>Integration</strong></td>
<td>None, Silos</td>
<td>Alerts, logs consolidated in SIEM</td>
<td>Data correlated with network security, SIEMS, etc.</td>
<td>Customized integration via open APIs</td>
</tr>
</tbody>
</table>
Every second counts

Continuous record, centralize and retain activity from every endpoint

- **Record:** Continuous, always on, never sleeps, because you can’t know what is bad ahead of time.
- **Collect:** The right data, based on our offensive security expertise.
- **Centralize:** Stream all data to an aggregated “system-of-record.” Single source of truth. Manage as key IT asset.
- **Retain:** Persistent history of attacker’s every action, root cause, patterns of behavior.
- **Non-Intrusive:** Never impact endpoint or user.
- **Benefits:**
  - Visibility. Know what’s happening on every endpoint.
  - Scope an incident in minutes.
  - Historical traceability for investigations.
  - Apply new detection rules retrospectively.

*Track an attacker’s every action*
Discussion Before Demo
Continuous measuring and monitoring of the operational benefits of compliance drives increased understanding and support for data protection, compliance, and eventually the acknowledgment that compliance can make a substantial contribution toward more effective business management.

How do you put a value on compliance?

Unlike many business investments, the ROI of compliance may not be immediately obvious in terms of bottom-line benefits.

* Verizon Report 2015
Value Proposition for Continuous Monitoring

Security
• Immediate visibility into everything running in your environment to prevent, detect & respond to threats that evade traditional security defenses
• Mitigate weakness in third-party applications
• Go beyond scanners point in time snapshots & signatures to prevent “alert fatigue”, identify threats in real-time & rapidly respond
• Eliminate the risk from malicious, illegal and unauthorized software.

Compliance
• Compliance governing automation
• Support for legacy, orphaned, or end-of-life application & operating systems
• No need for scans or other performance burdensome procedures
• Aggregate big data to relieve data fatigue – integrate your data to personalize compliance stance in real time
Questions?