Gavin Millard
Technical Director - International

How a University project became the standard in Data Integrity

Tripwire Evolution

1992
Gene Kim
invents
Tripwire OSR

2007
Configuration
Automated
Virtualisation

2009
Configuration
Assessment
capabilities
added

2006
Active
Directory and
Database
monitoring

2008
Industries
largest
catalogue of
policies
monitoring
added

compliance | security | control
Tripwire born in Purdue University

- Gene Kim and Eugene Spafford created concept in 1991
- Created to help detect Morris worm
- Started the whole concept when looking into the mathematical probability of hash clashes
- Then realised had huge benefits in operations and other security issues

Tripwire Compares Baseline State to Running

Tripwire Captures Baseline State as a “Digital Fingerprint”
Tripwire Evolution

1992
Gene Kim
invents
Tripwire OSR

1997
Tripwire Inc
formed and
TFS released

2004
Configuration

2006
Active
Directory and
Database
monitoring

2007
Automated
Virtualisation

2009
Configuration
Assessment
capabilities
added

2008
Virtualisation
security
program
released

2009
Industries
largest
catalogue of
policies
monitoring
added

Data Integrity Gave Much Needed Visibility

**Change Auditing**
Detect & Enforce

- All changes are recorded
- Full visibility of all-change to reduce MTTR and increase MTBF
- When systems are hacked you know exactly what changed
- Helps address audit failures

compliance | security | control
Tripwire Evolution

1992
Gene Kim invents
Tripwire OSR

1997
Tripwire Inc formed and
TFS released

Tripwire Enterprise

Baseline and Compare

Detection Agents

File Systems Network Devices Databases Directory Services Desktops Applications

compliance | security | control

Extending the Concept across the infrastructure

compliance | security | control
Improved the Concept of Authorised and Unauthorised

Authorised changes followed some kind of expected process including:
- Change ticket
- Change occurred in expected change window
- Tested before deployment
- Non critical “Business as Usual”

Whereas non authorised changes did not follow any process or contravened rules defined within Tripwire. These changes cause the most issues within your environment.

Researching Why Change Matters

- ITPI launched the IT Controls Performance Study to find answers to the following questions:
  - Do high performers really exist?
  - Are all ITIL processes and COBIT controls created equal?
  - What controls have the highest impact on performance?
- 350 organizations were benchmarked

<table>
<thead>
<tr>
<th>N = 98</th>
<th>IT Employees</th>
<th>IT Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>483</td>
<td>$114 million</td>
</tr>
<tr>
<td>Min</td>
<td>3</td>
<td>$5 million</td>
</tr>
<tr>
<td>Max</td>
<td>7,000</td>
<td>$1,050 million</td>
</tr>
</tbody>
</table>
The Highest Performing IT Organizations Get Results

Operations Metrics Benchmarks:

*Best in Class: Server/sysadmin ratios*

- Highest ratio of staff for pre-production processes
- Lowest amount of unplanned work
- Highest change success rate
- Best posture of compliance
- Lowest cost of compliance

Common Traits of the Highest Performers

**Culture of...**

**Change management**
- Integration of IT operations/security via problem/change management
- Processes that serve both organizational needs and business objectives
- Highest rate of effective change

**Causality**
- Highest service levels (MTTR, MTBF)
- Highest first fix rate (unneeded rework)

**Compliance and continual reduction of operational variance**
- Production configurations
- Highest level of pre-production staffing
- Effective pre-production controls
- Effective pairing of preventive and detective controls
Seven Habits of Highly Effective IT Organizations

1. Have a culture that embraces change management
2. Monitor, audit, and document all changes to the infrastructure
3. Have zero tolerance for unauthorized changes
4. Have specific, defined consequences for unauthorized changes
5. Test all changes in a preproduction environment before implementing into production
6. Ensure preproduction environment matches production environment
7. Track and analyze change successes and failures to make future change decisions

Tripwire Evolution

1992
Gene Kim invents Tripwire OSR

2004
Tripwire Enterprise released

1997
Tripwire Inc formed and TFS released

2006
Active Directory and Database monitoring added
Change Audit and Configuration Assessment

**Policy Compliance**
Assess & Validate

- Policy based Regulatory and Security compliance testing
- Current Configuration state is assessed against documented & expected standards
- Every change detected is validated against defined best practice policies

**Change Auditing**
Detect & Enforce

- All changes are recorded
- Full visibility of all change to reduce MTTR and increase MTBF
- All changes achieve the desired/expected/appropriate results
- All changes follow the right process

Configuration Assessment Gave us a Second Lens

**Policy Conformance**
Assess & Validate

**Change Auditing**
Detect & Enforce

- Configuration Control

<table>
<thead>
<tr>
<th>compliance</th>
<th>security</th>
<th>control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>compliance</th>
<th>security</th>
<th>control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>16</td>
</tr>
</tbody>
</table>
**Snapshot approach**

**Validating Critical Controls...**

**Manually**

- Time
- Compliance
- Compliant State
- Change is occurring
- Without remediation advice it takes time and effort to improve
- Key Points
  - Herculean task
  - Almost always at risk
  - Cannot frequently repeat
  - Goal is audit ✓

**Periodically**

- Time
- Compliance
- Compliant State
- Change is occurring
- Key Points
  - Drifting between checks
  - Only compliant for short time
  - Frequently at risk
  - Misplaced trust in the process
Enhanced File Integrity Monitoring to…
Achieve & Maintain a Compliant State…Continuously

Key Points
Reduce risk of exposure
Reduce ongoing compliance effort
Reduce audit preparation time
Trust the process

Tripwire Evolution

1992
Gene Kim invents Tripwire OSR

2004
Tripwire Enterprise released

2007
Configuration Assessment capabilities added

1997
Tripwire Inc formed and TFS released

2006
Active Directory and Database monitoring added
Out-of-the-Box Policies – Over 170 of Them

Security
- CIS: ISO 27001
- DISA: V13 Hardening Guidelines
- NIST: Microsoft Security Guide

Compliance
- PCI DSS: COBIT
- SOX: FISMA
- NERC: FDCC

Operational/Performance
- Microsoft Exchange Server 2003
- Microsoft IIS
- Oracle 10g

Organizational
- Custom
- Internal ‘Golden’ Policy

Tripwire Evolution

1992
- Gene Kim invents Tripwire OSR

1997
- Tripwire Inc formed and TFS released

2004
- Tripwire Enterprise released

2006
- Active Directory and Database monitoring added

2007
- Configuration Assessment capabilities added

2008
- Industries largest catalogue of policies
The Virtualization Paradox

Benefits
- Reduce costs
- Enhances availability
- Increase consolidation
- Rapid deployment & provisioning
- Improved agility
- Less power consumption
- Increased resource utilization
- Simpler management
- Enhance recovery efforts
- Lower TCO
- Optimize system performance

Risks
- Lack of visibility
- Lack of control
- Misconfigurations
- Virtual sprawl
- Mobility
- Configuration drift
- Lack of skills, experience & resources
- Best practice and standards are immature
- Multiple points of entry & attacks
- Additional complexity
- Lack of processes, policies or tools

To reap the benefits of virtualization requires proper visibility, management & control of configurations, compliance and security.

Know and Secure your VI

- Gain visibility of the entire VI stack
- Apply security & compliance rules & policies
- Identify VI objects that are moved, changed or not managed
- Continuously monitor & detect deviations from trusted state
- Alert & report on policy compliance changes to enable corrective action
- Know mission critical VMs & hypervisor relationship

23

compliance  |  security  |  control

24

compliance  |  security  |  control
In Conclusion

System Misconfiguration & Unauthorized Change Introduce Risk To Your Organization

Achieve & Maintain a Known & Trusted State

- Proactively assess & validate IT configurations against policy
- Rapidly detect & reconcile all configuration changes

Tripwire Delivers a Single Point-of-Control for Your Physical and Virtual Environments

- Configuration Assessment
- Change Auditing

Automate Compliance
Mitigate Risks
Increase Operational Efficiency

Questions?