Tripwire Enterprise
Configuration Audit & Control

Brett Bartow - Account Manager
Kelly Feagans, Sr. Systems Engineer ITIL, CISA
March 4, 2009
Recognized leader in Configuration Audit & Control
Achieve & Maintain the integrity of all IT configurations

Pioneer in change detection
Founded in 1997
Patented Technology

Recognized market leader
Over 6,000 customers around the world
Analyst leadership recognition

Worldwide strategic partners
Infrastructure: VMware, Cisco, Sun, IBM, Oracle..
IT Service Management: BMC, HP, CA..
Integration: BearingPoint, EDS, IBM..

Thought leader in IT best practices
ITIL v3 content contributors
Co-author of The Visible Ops Handbook
Sample of Tripwire’s 6,000+ Global Customers
Tripwire enables companies to *achieve* and *maintain* a known and trusted state across the data center.

**Compliance**
- Achieve Known & Trusted State
- Configuration Assessment
- Automate controls & reporting to meet specific compliance requirements

**Security**
- Active monitoring and risk management across the data center

**IT Operations**
- Enforce configuration and change controls to help obtain operational excellence
Introducing Tripwire Enterprise 7

**Continuous Compliance Across the Datacenter**

**Achieve**

- Known, Trusted and Compliant State
- Proactively assess configuration settings using industry benchmarks
- Identify risks to ensure continuous compliance

**Maintain**

- Known, Trusted and Compliant State
- Detect all changes across the datacenter
- Gain visibility through actionable reports, reconciliation and remediation

Configuration Audit & Control Assures Continuous Compliance

Tripwire Enterprise 7
Configuration Control Mitigates Risks

- Continuous Compliance
- Lowers Costs
- Increases Security
- Reduces Risks
- Sustainable
Enterprise Configuration Control

Requires Comprehensive Coverage

**Servers**
- AIX
- HP-UX
- Red Hat Enterprise Linux
- SUSE Linux
- Windows 2000 Server
- Windows 2003 Server
- Solaris (SPARC)
- Solaris (x86)
- AIX
- HP-UX
- Solaris (SPARC)
- Solaris (x86)
- AIX
- HP-UX
- Solaris (SPARC)
- Solaris (x86)

**Virtual Environments**
- VMware ESX Server
- Solaris Zones

**Databases**
- Oracle 9i & 10g
- SQL Server
- Oracle 9i & 10g
- SQL Server
- Oracle 9i & 10g
- SQL Server

**Network Devices**
- Alcatel OmniSwitch
- Cisco IOS, CatOS & PIX OS
- Cisco VPN 3000 Series
- Cisco Catalyst 1900/2820
- Check Point (Nokia IPSO)
- Extreme
- F5 BigIP
- Foundry
- HP ProCurve Series
- ISS (Nokia IPSO)
- Juniper M/T Series
- Marconi ForeThought
- NetScreen
- Nokia IPSO OS
- Nortel Alteon & Passport
- POSIX-compliant appliances
- Alcatel OmniSwitch
- Cisco IOS, CatOS & PIX OS
- Cisco VPN 3000 Series
- Cisco Catalyst 1900/2820
- Check Point (Nokia IPSO)
- Extreme
- F5 BigIP
- Foundry
- HP ProCurve Series
- ISS (Nokia IPSO)
- Juniper M/T Series
- Marconi ForeThought
- NetScreen
- Nokia IPSO OS
- Nortel Alteon & Passport
- POSIX-compliant appliances

**Directory Services**
- Windows Active Directory
- Solaris Sun One Directory
- Novell eDirectory

**Applications**
- Executables
- Configuration Files

**Middleware**
- J2EE-based
- IBM WebSphere
- BEA WebLogic

**Databases**
- Schema Objects
- Application & Configuration Files
- Access Settings
- User Roles & Permissions
- Security & Configuration Parameters

**Operating Systems**
- Windows
- UNIX
- Linux

**Virtual Environments**
- VMware ESX
- Solaris Zones

**Network Devices**
- Routers
- Switches
- Firewalls
- Load Balancers
- VPN Concentrators

**EMS Integrations**
- HP Service Desk, Network Node Mgr.
- Remedy AR System, Atrium
- Open Web Services API

8
Tripwire Enterprise 7 - How it Works

Baseline, Assess & Validate Configurations Across the Data Center

Enterprise Risk Profile

1. Tripwire detects all change

2. "Are changes authorized?"

3. "Are changes Compliant?"

Achieve

Maintain

25%

"Are you within policy?"

Take Action

Notification

Reconciliation

Reporting

Tripwire detects all change

"Are changes authorized?"

"Are changes Compliant?"
Tripwire Enterprise demo

Kelly Feagans, CISA & ITIL Certified
Sr. Systems Engineer
kfeagans@tripwire.com
Appendix
Enterprise-Wide Configuration Assessments
Pre-configured, automated and proactive assessments of IT configurations

CMDB Integrations
Assures integrity and accelerates success: BMC Atrium 2.0, CA CMDB and HP Universal CMDB

Virtualization
Detect and control change in the dynamic datacenter: VMware & Solaris

Real-time, Tunable Change Detection
Flexibility to detect changes and assess configurations: ‘event-driven’ and/or ‘scan-based’

IT Service Management Integrations
Compliment BMC Remedy integration with new CA Service Desk integration

Configuration Rollbacks
Network device baseline rollbacks & trigger remediation via integrations
Tripwire helps answer two fundamental, business-critical questions:

- Is the change authorized?
- Is the change within policy?

Tripwire enables 100% control of change/compliance.

Independent, verifiable proof of all changes to configuration settings.

Unmatched breadth & depth.

Provides enterprise-wide visibility and control for the dynamic datacenter.

Process circumvention  Unintended changes

Tripwire ensures data integrity to help reduce risks and increase operational efficiencies.
Achieve Continuous Compliance
Stop IT process circumvention and achieve operational, regulatory and security compliance across the datacenter

Out-of-the-Box Compliance Audit Proof
Deliver holistic view of compliance for entire IT infrastructure

Experts in Configuration Audit & Control
Market-leading solution to close-the-loop on change

Speed to Value
Proactively determine unauthorized changes
  • Increase performance on key metrics in 90 days or less
  • Accelerate ROI of IT Service Management and ITIL projects

“In a recent survey, 73% of our clients reported that they must continually deal with unplanned infrastructure changes resulting in incidents and downtime.” Forrester
Tens of thousands of configuration assessments and reports!

**Operational**

**Change Process Policies**
- Authorized vs. Unauthorized
- Change Variance
- Change Frequency
- Change Rate
- Change Severity
- Change Window
- Change Attributes
- Changed Nodes
- Changed Elements

**ITIL Policies**
- Authorized vs. Unauthorized
- Change Window
- Inventory
- User Roles

**CMDB Policies**
- Configuration Item History
- Schema Control
- CMDB-related Change Policies
- Alerts & Notifications
- Change History

**Visible Ops**

**Configuration Compliance Profile**
- Compliance History
- Detailed Test Results
- Policy Scorecard

---

**Regulatory**

- Payment Card Industry (PCI)
- Sarbanes-Oxley (SOX)
- COBIT
- BASEL-II
- FISMA
- JSOX
- GLBA
- HIPAA
- 21 CFR Part 11
- NERC

---

**Security**

- CIS
- DISA
- Microsoft Security Standards
- Windows Hardening Standards
- ISO 17799

**Infrastructure Coverage**

- Servers
- Databases
- Network Devices
- Switches
- Routers
- Firewalls
- Active Directories
- Operating Systems
- Middleware
- Storage
- Applications
- Desktops
- Virtualization

---

**Ongoing Policy Installments**

- Tripwire Top-20
- Out-of-the-box templates
- Policy Manager - Create your own
The problem:
Over 45 million credit and debit card numbers stolen, dating back to 2003

Service impact:
Come under widespread criticism – negatively impacting company’s brand

Business impact:
20 class action lawsuits pending; Investigations pending in 30 states
Shares down 6.3% ; Sales down $2M and profits down $1M in Q1/07
Security upgrade - $100,000,000

Over $1B+ for an undetected security breach
**The problem:**
Occurred during loading of software to a critical component of the satellite broadcast system

**Service impact:**
Major 24 hour service outage to 8 million subscribers

**Business impact:**
Customers credited for 2 days worth of service outages $6,960,000
Shares down 1.4% - Market capitalization impact -$1,536,150
Middle of a merger with Sirius Satellite ???

*Consider XM Satellite*

“Problem occurred during the loading of software to a critical component…”

*XM Satellite Radio service restored following software problems*

WASHINGTON: XM Satellite Radio restored service Tuesday after a software glitch knocked out the signal from one of its four satellites and disrupted service to many of the company’s 8 million subscribers for about a day.

The problems began around noon Monday, the company said. They initially expected to fix the problem after a few hours, but service remained disrupted for about 24 hours.

Nearly $8.5M for a minor IT change
Why Tripwire?

- **Automate proof of compliance**
  - Avoid audit findings and associated costs of remediation
  - Spend less time preparing for audits and assessing configurations for policy conformance

- **Avoid penalties & fines**
  - Avoid regulatory fines & SLA penalties

- **Enhance security**
  - Reduce exposure to datacenter compromise and time spent resolving security incidents

- **Increase revenues and productivity (increase availability)**
  - Minimize revenues & productivity lost due to outages or service degradations

- **Increase staff capacity (reduce unplanned work)**
  - Spend less time troubleshooting service incidents and restore service faster
  - Reduce rework caused by failed changes
Maximize The Effectiveness of IT Tools and Processes
With Tripwire’s Configuration Audit and Control Solution
• Assess configurations to ensure conformance with policy and industry guidelines
• Detect process, policy and tool circumvention
• Provide comprehensive change history and actionable reporting