



Configuration Assessment &
Change Auditing Solutions



COMPLIANCE
SECURITY
CONTROL

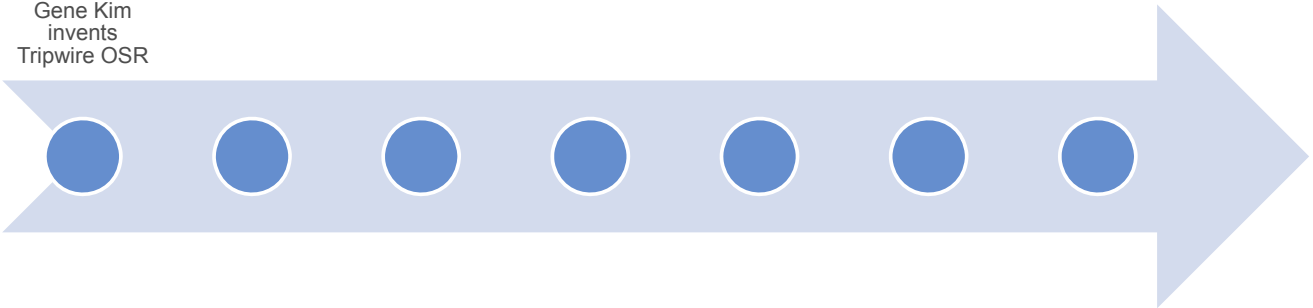
Gavin Millard
Technical Director - International

How a University project became
the standard in Data Integrity



Tripwire Evolution

1992
Gene Kim
invents
Tripwire OSR



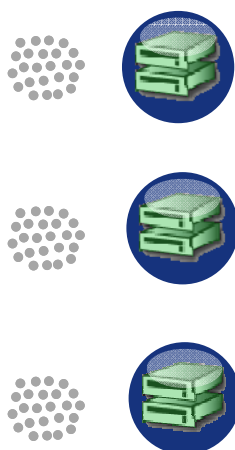
Tripwire born in Purdue University

- 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

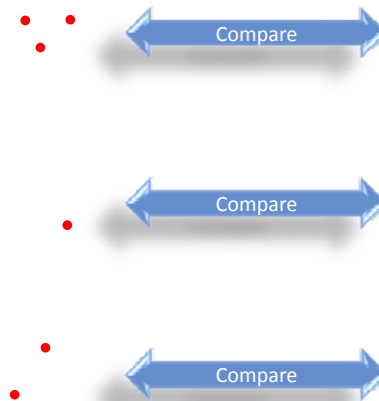
Tripwire Captures Baseline State as a
"Digital Fingerprint"



Current running state

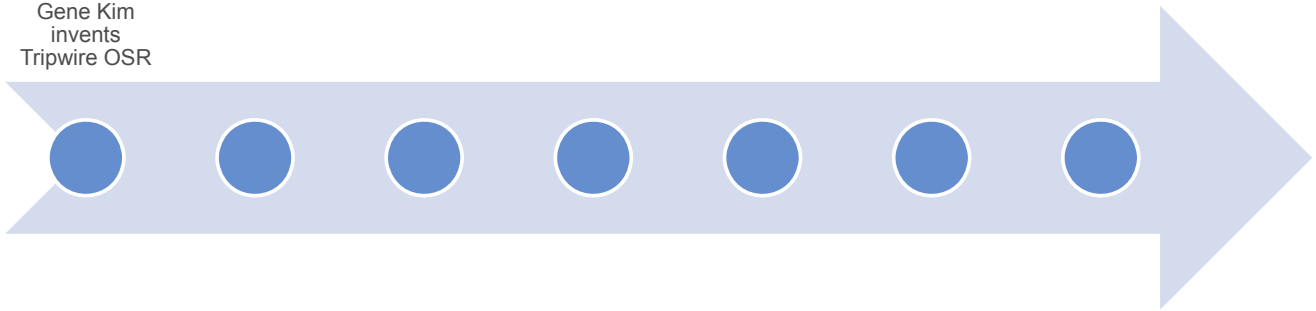
New changes
determined

Baseline State



Tripwire Evolution

1992
Gene Kim
invents
Tripwire OSR



Data Integrity Gave Much Needed Visibility

Change Auditing Detect & Enforce

All changes are recorded

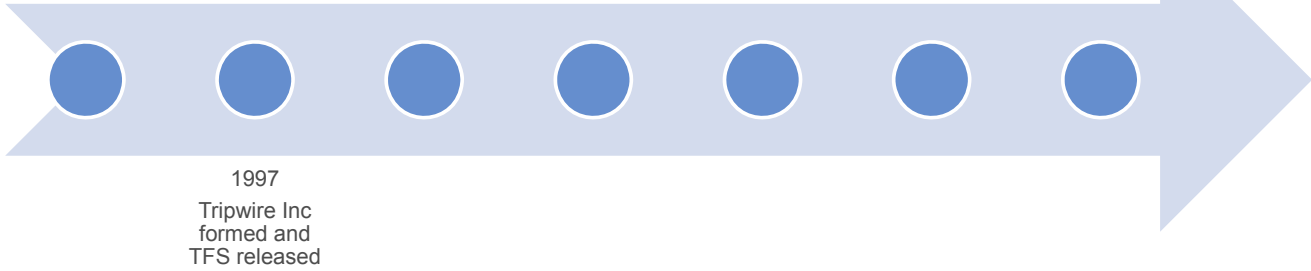
Full visibility of all change to reduce MTTR and increase MTBF

When systems are hacked you know exactly what changed

Helps address audit failures

Tripwire Evolution

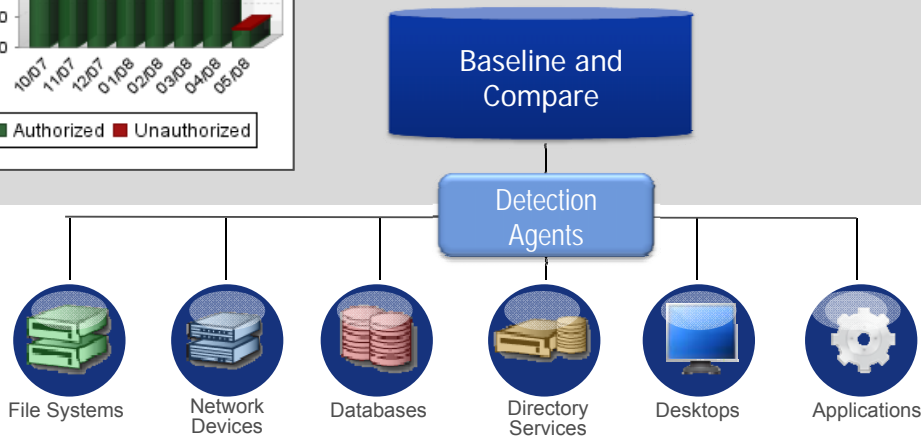
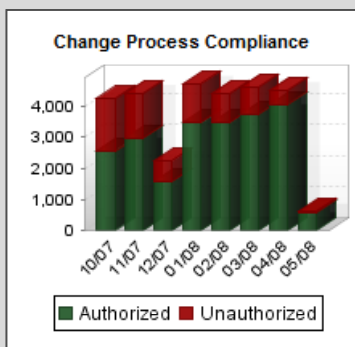
1992
Gene Kim
invents
Tripwire OSR



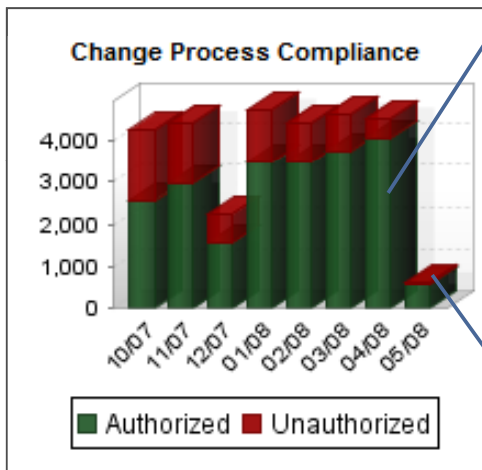
1997
Tripwire Inc
formed and
TFS released

Extending the Concept across the infrastructure

Tripwire Enterprise Console



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

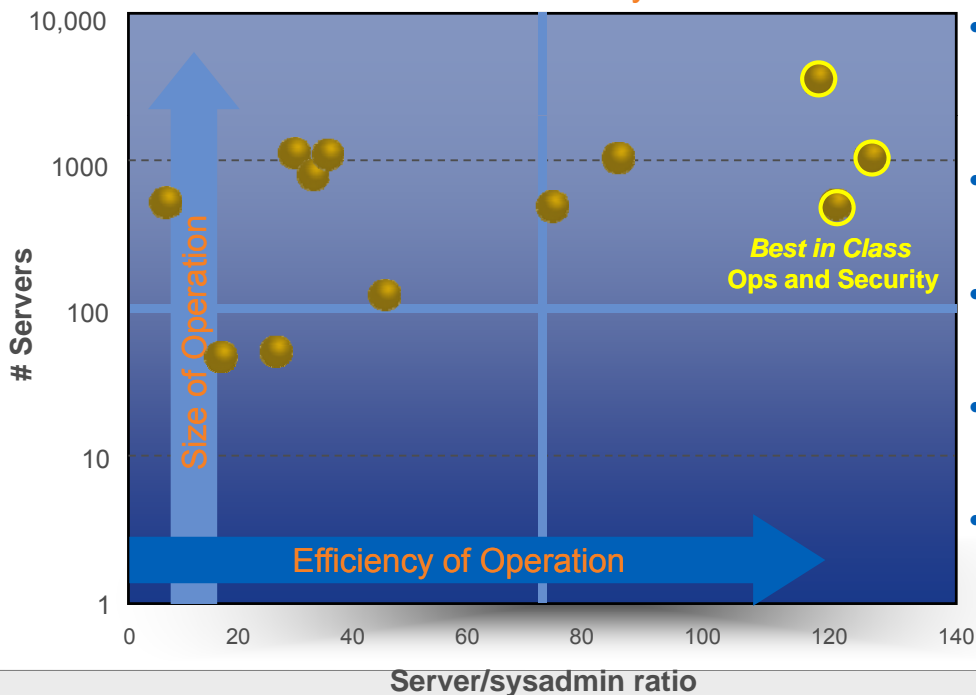
Researching Why Change Matters

- 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

N = 98	IT Employees	IT Budget
Average	483	\$114 million
Min	3	\$5 million
Max	7,000	\$1,050 million

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

11

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)

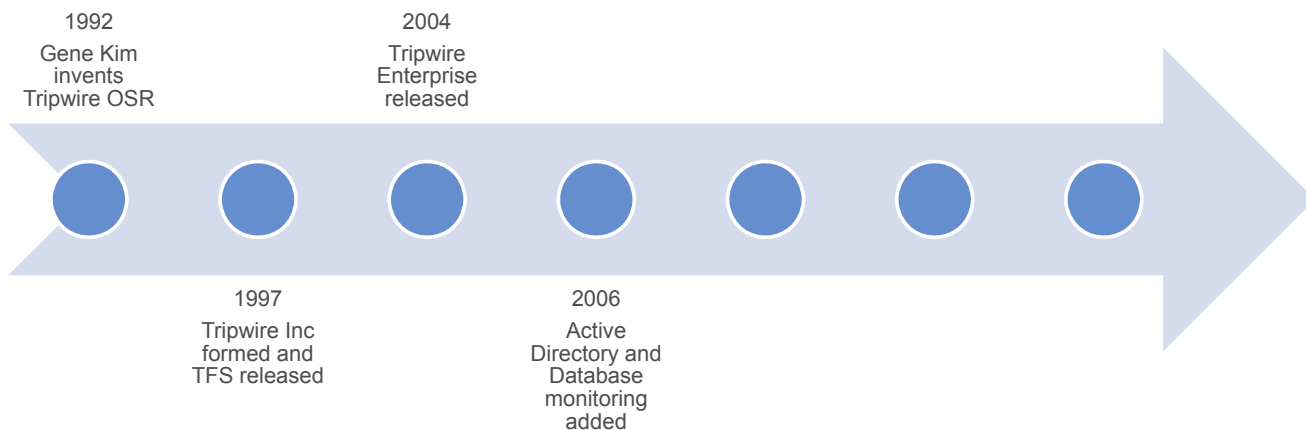
Compliance and continual reduction of operational variance

- 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



Change Audit and Configuration Assessment

Policy Compliance

Assess & Validate



Change Auditing

Detect & Enforce



Configuration Assessment Gave us a Second Lens

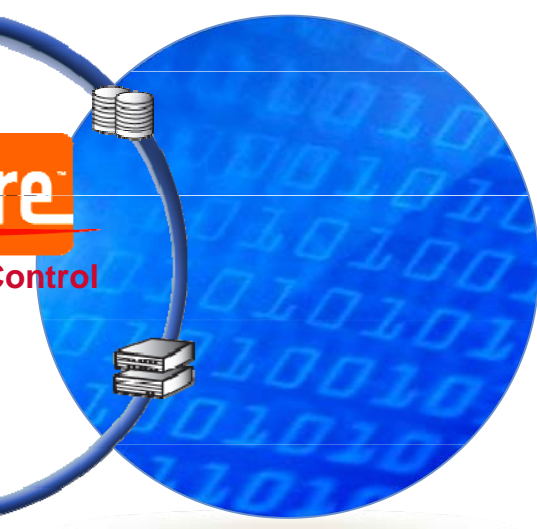
Policy Conformance

Assess & Validate



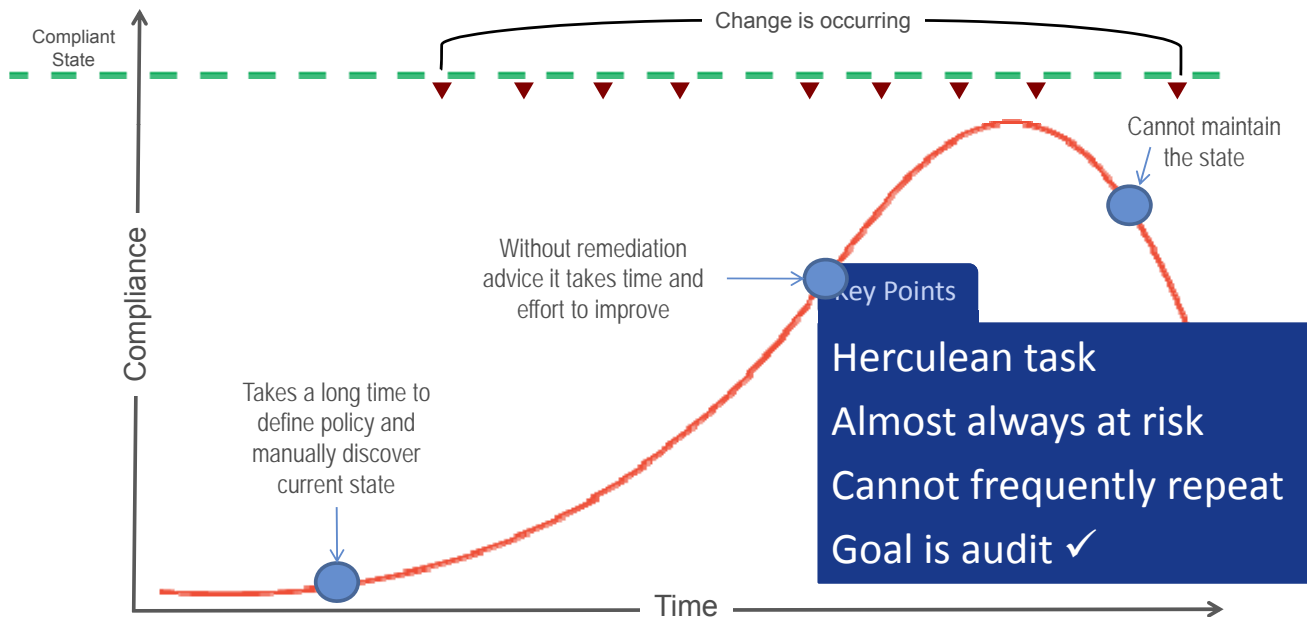
Change Auditing

Detect & Enforce

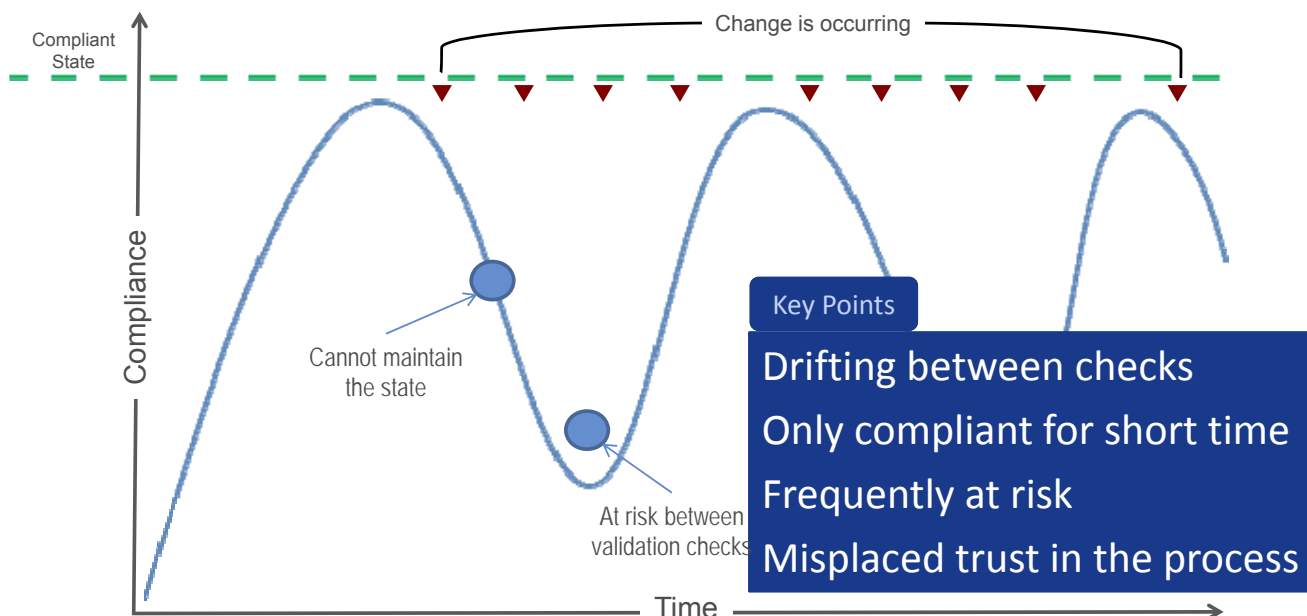



Configuration Control

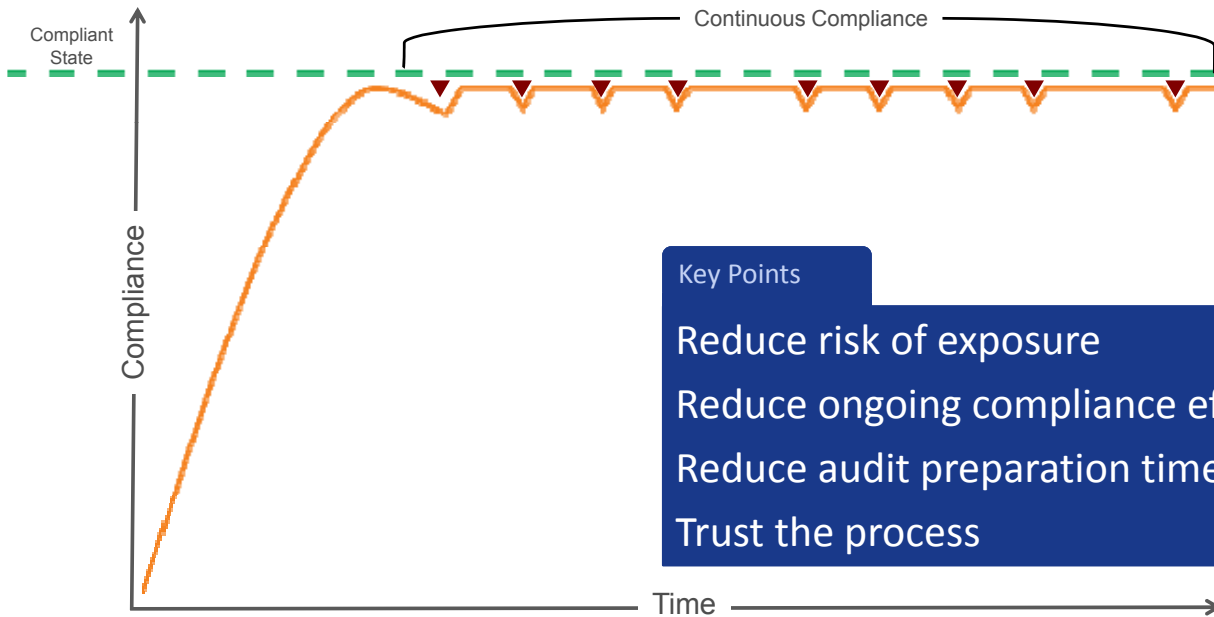
Snapshot approach Validating Critical Controls...Manually



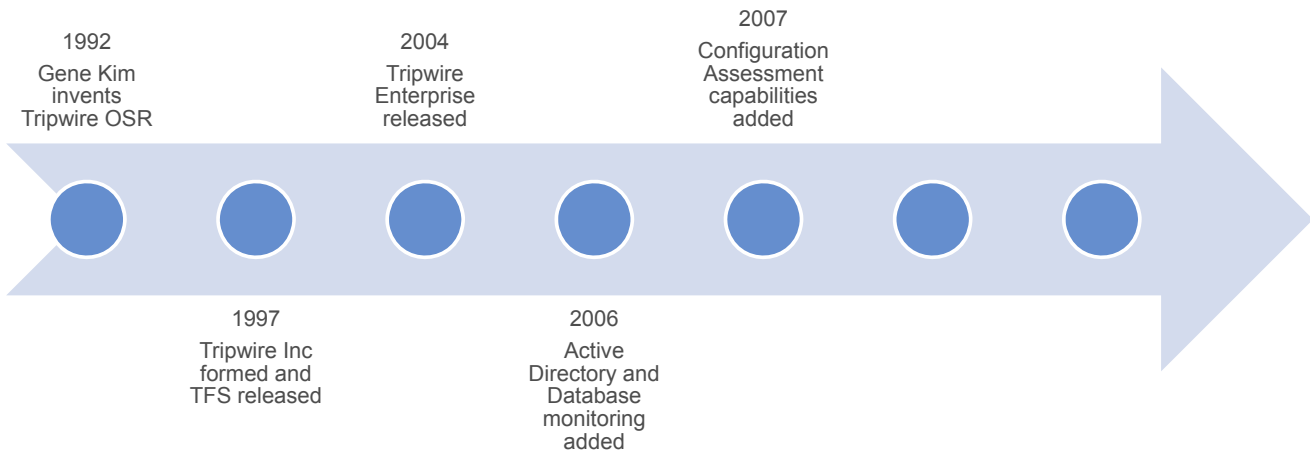
Snapshot approach Validating Critical Controls...Periodically



Enhanced File Integrity Monitoring to... Achieve & Maintain a Compliant State... **Continuously**



Tripwire Evolution



Out-of-the-Box Policies – Over 170 of Them

Security

CIS ISO 27001
 DISA VI3 Hardening Guidelines
 NIST Microsoft Security Guide

Compliance

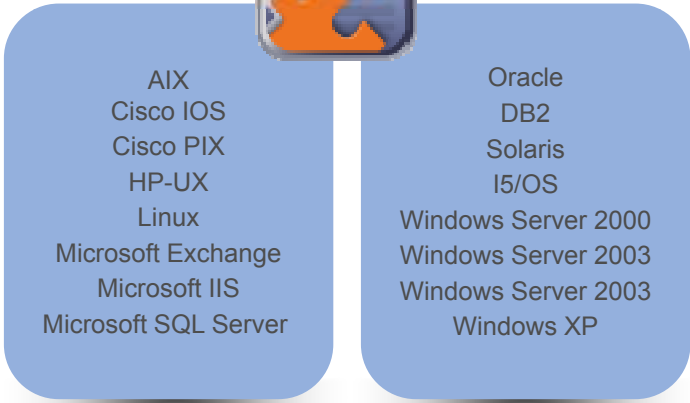
PCI DSS COBIT
 SOX FISMA
 NERC FDCC

Operational/Performance

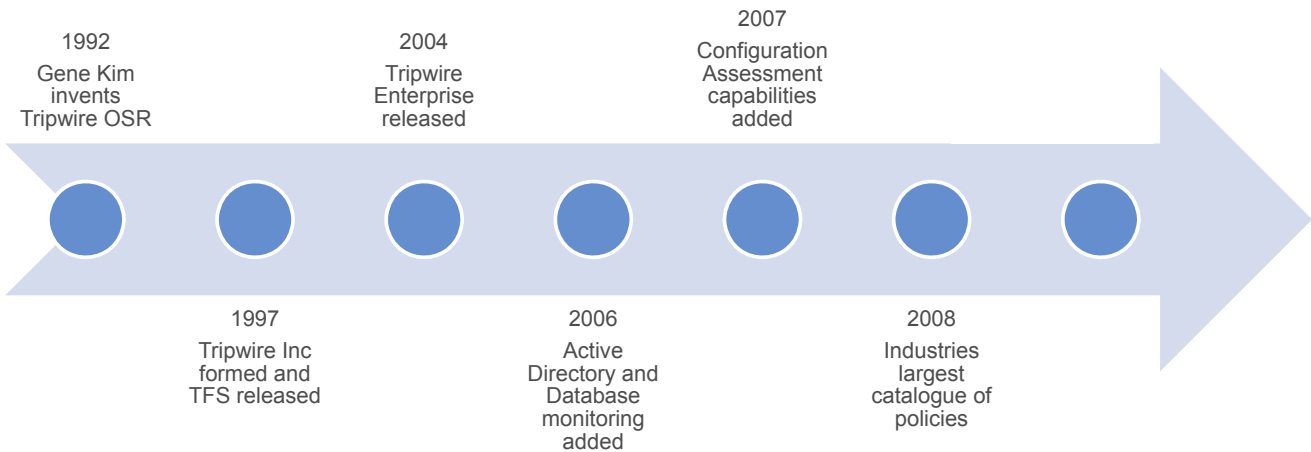
Microsoft Exchange Server 2003
 Microsoft IIS
 Oracle 10g

Organizational

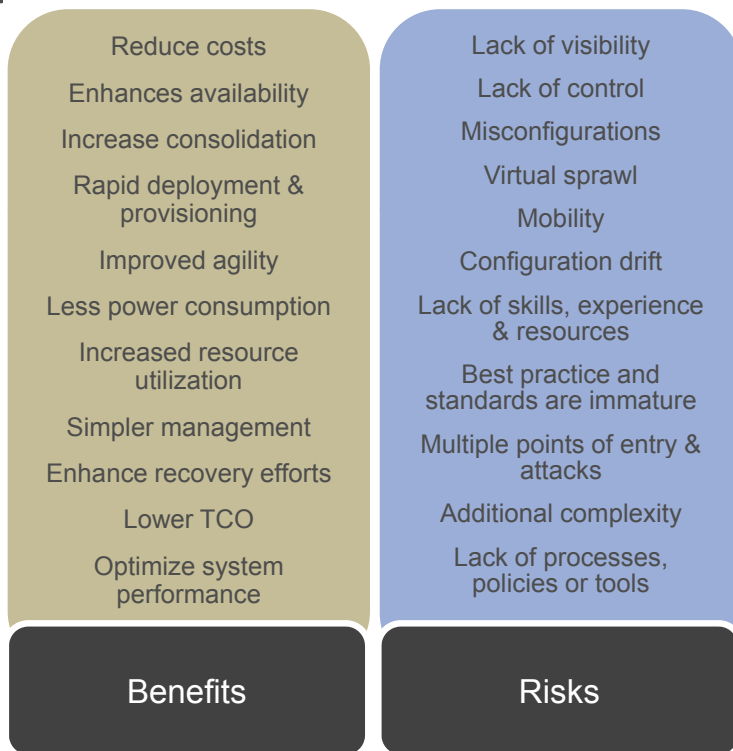
Custom
 Internal 'Golden' Policy



Tripwire Evolution

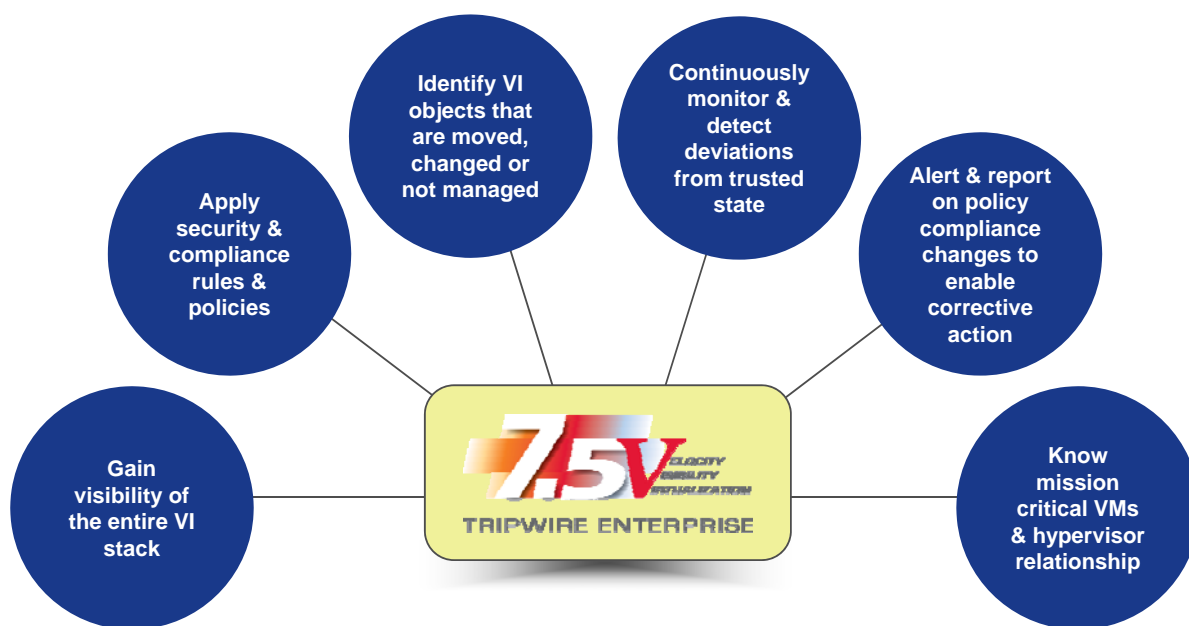


The Virtualization Paradox



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

Know and Secure your VI



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



Configuration Assessment & Change Auditing Solutions



COMPLIANCE
SECURITY
CONTROL

Questions?