FORTRA®

WHITE PAPER (TRIPWIRE)

Tripwire and Visible Ops

A Four-Phase Approach to Instituting Change Management

Simultaneous Demands — Where Do You Start?

While annual business plans focus on strategic initiatives designed to keep the enterprise competitive or to mitigate risk, it's the day-to-day operations that consume the most time and resources. For many IT organizations, it seems that just keeping the computers running and the lights on occupies the majority of their time. And according to research — it does.

Maintaining existing systems and applications consumes anywhere from 40 to 90 percent of the development budget, leaving a limited amount available for new project investment.[1] A Forrester survey found that four in 10 IT leaders foresee their IT budget increasing less than five percent for the following year.[2] Add to this burden the voluminous security, regulatory, and legal issues that enterprises now face, and IT is stretched to the limit.

Where do you begin to address all of these demands? Fortunately, they all have one element in common — *change*. When you can consistently and effectively control change in an IT production environment, you have taken a significant step forward in operational effectiveness, resource efficiency, and risk mitigation. Effective change management processes appropriately blend process, people, and technology — and helping IT organizations institute them is the goal of the IT Process Institute's Visible Ops methodology. The Visible Ops methodology delivers clear, concise guidance on how to improve processes by controlling change.

Start at the Top

Every IT organization that begins to implement effective change management processes encounters opposition from staff members who do not want any change controls. For this reason, controlling change begins at the top of the organization, with the C-level leaders like the CIO, who set the cultural tone for the organization. When defined processes and controls are established and enforced, change management policies can deliver significant benefits in security, compliance, and operational quality of service.

Defined processes should encompass pre-production and production environments. From scrutinizing and authorizing proposed changes, to identifying unauthorized changes made to production systems, change management processes are intended to prevent human error and malicious changes from finding their way into production. Ninety-five percent of cybersecurity incidents are the result of human error according to the World Economic Forum.[3] Human error can be classified into the following categories:

- **The wrong people doing the wrong things:** These can be changes implemented by an unauthorized individual, regardless of the type of change made, or they may be malicious acts. These unauthorized changes may also constitute reportable criminal incidents.
- **The right people doing the wrong things:** That is, unauthorized changes made by authorized individuals.
- **The right people doing things incorrectly:** These changes may exceed the scope of the authorization, be implemented at the wrong time or against the wrong assets, or be proper changes implemented incorrectly and not verified properly.

Each unauthorized change that occurs increases the amount of unplanned work required to rectify the situation.

Fig 1. Factors causing IT downtime

Obviously, IT organizations would prefer to conserve resources for strategic initiatives rather than spend them on preventable errors. Effective change management processes include a mechanism for quickly identifying unauthorized changes and facilitating corrective action.

A rigorous change management culture also enables the IT organization to collect a tremendous amount of process improvement data. W. Edwards Deming, the noted quality scholar, observed "Inspection with the aim of finding the bad ones and throwing them out is too late, ineffective, and costly. Quality comes not from inspection but from improvement of the process." With effective change management controls, the data obtained plays a vital role in ongoing development, testing, and release management improvement. In the end, poor availability, weak security, and uncontrolled levels of unplanned work are the symptoms of poor-quality processes.

Implementing Visible Ops

The IT Process Institute's Visible Ops methodology is grounded in Information Technology Infrastructure Library (ITIL) best practices and lessons learned from working with high-performing IT organizations since the year 2000. Visible Ops is based on three distinct project phases, followed by ongoing process improvement efforts. The phases are:

1. **Stabilize the Patient**
   This phase focuses on reducing the volume of unplanned work enough to free resources for working on strategic projects.
2. **Catch & Release and Find Fragile Artifacts**
   During this phase, we create a configuration item (CI) inventory and identify systems that are so fragile they should be rebuilt or replaced.
3. **Create Repeatable Builds**
   In this phase, engineers focus on creating repeatable system configurations — or builds. Repeatable, or standard, builds reduce or eliminate variation between systems so that it becomes more resource-effective to rebuild them than to debug them.
4. **Continuous Improvement**
   Once standard configurations and builds are in place, and are supported by effective change management controls, the IT organization can shift its focus from improvement projects to identifying opportunities for ongoing improvement based on metrics.

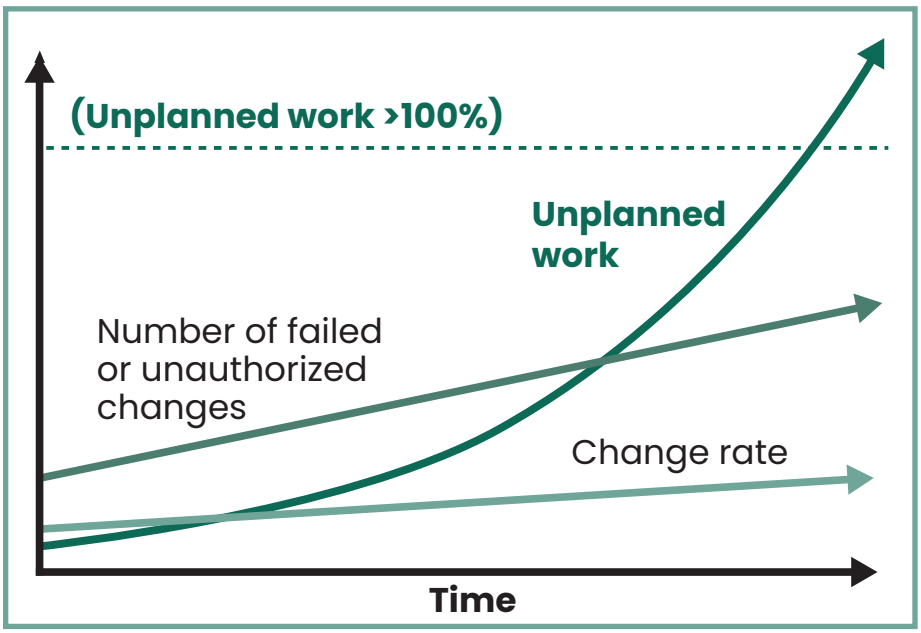


Fig. 2. The effect of failed and unauthorized change on unplanned work

Visible Ops was designed to be implemented quickly and to immediately return value. Only by rapidly demonstrating its value can it "catalyze" the cultural change and become sustainable.

Preparation: A Critical Element of Project Success

Organizations embarking on Visible Ops must recognize that they are doing far more than defining and implementing processes. Rather, they are shepherding organizational change, which necessitates a change in culture. This is why change control begins at the top of the organization and why there must be steadfast support from senior management. The tone at the top can help the project succeed or ensure its failure.

Creating awareness and setting proper expectations is critical. You must be able to communicate:

- Policies and procedures are vital and must be followed · All changes will be detected using a change auditing solution, such as Fortra's Tripwire® Enterprise
- Unauthorized changes will be investigated
- Individuals responsible for unauthorized changes will be held accountable to management and their peers. This includes publicly identifying the culprits after a major incident and may also include formal disciplinary action.

The message must be clear that the only acceptable number of unauthorized changes is zero. And this message must be reflected and reinforced by policies, procedures, and the actions of IT management.

Implementing Change Auditing as an Effective Change Control

Tripwire Enterprise change auditing solutions play an integral role in world-class IT organizations. Tripwire Enterprise delivers visibility into the entire IT infrastructure, immediately detecting changes to system baseline configurations and file systems — for servers, desktops, network devices, databases, directory servers, and more.

With Tripwire Enterprise, you can establish three critical change control capabilities:

1. **Detection:** Tripwire solutions detect infrastructure change independent of who made the change or how it was made. By separating change detection from the people and technologies that initiate change, Tripwire provides an independent detective control for all automated and manual changes across the entire service stack.
2. **Reconciliation:** By accessing information in leading change management tools, Tripwire solutions enable rapid reconciliation to quickly determine which changes were authorized and which weren't.
3. **Reporting:** Through independent, verifiable audit logs of all actual change activity, Tripwire reports document compliance and enables change management policy enforcement and accountability.

In addition to detecting service-affecting change, Tripwire software enables you to enforce change management processes and assign accountability for change. When a change is detected that cannot be reconciled with authorized work orders, management can identify who made the change and initiate appropriate consequences.

Business Benefits	IT Benefits
IT is able to focus on business needs instead of constant firefighting.	Rather than spending an inordinate amount of time on support, IT can work on new projects and technology.
Increased service availability means that the business can achieve its goals.	The business has a higher regard for IT as availability increases and changes fail far less often.
Production infrastructure risks are reduced and managed, facilitating regulatory compliance.	When a problem does occur, rather than a mad scramble to determine what changed, the service desk and incident management teams have factual data available, which improves their ability to respond.
Changes can be counted on rather than feared.	Budget previously spent on unplanned work can be invested in activities that move the IT organization forward, such as training, process improvement, and preventive maintenance.

Detection and enforcement capabilities can help deter ad hoc changes and are critical components in a successful culture of change.

Once processes are established and enforced, management can manage operations and make decisions based on documented facts. With credible data, an IT audit trail, and histories of change over time, the IT organization becomes a credible force in measuring improvements and aligning IT improvements and metrics to overall enterprise objectives.

Visible Ops Phase One: Stabilize the Patient

IT groups usually operate at capacity with high stress levels. Therefore, the first project phase of Visible Ops is designed to reduce the amount of unplanned work that contributes to a high-stress environment by addressing the problems that stem from insufficient or un-enforced change management processes. This phase begins by identifying the hosts and applications that will be in the project scope and their relevant associated change management processes.

Electrify the Fence

With management support for the goal of "zero unauthorized change," the IT organization can quickly generate high value by "electrifying the fence" — that is, by implementing defined maintenance windows and enforcing them, by reconciling all authorized changes to work orders, validating that the changes were made correctly and completely, and reporting the results. Getting to this state, however, will require intermediate steps.

First, by interviewing staff and reviewing service desk logs, we begin to identify the initial CIs to monitor. These should be the systems that generate the most problems and those which are the most valuable to the organization.

Next, document existing change management processes. If no formal change management processes exist, determine which ITIL best practices you intend to implement and ensure the IT organization is mature enough to implement new, formalized processes. At the same time, consider any other constraints that may be present. The change management process must identify roles, responsibilities, proper segregation of duties, change windows, and other appropriate controls present. At a minimum, the newly defined change management process must have:

- A request for change (RFC) form that can be tracked from initial request through implementation
- A standard change model that governs each CI
- An emergency change model that governs each CI

An IT organization cannot leap from having no change management processes directly to a rigorous model without the proper process maturity and discipline in place, supported by a culture of change. Two elements must exist for effective change over time:

1. **Tripwire Enterprise must be monitoring key elements of each CI, not the entire CI.** For example, on a Windows system, certain key elements in the Windows system32 folder and registry entries along with specific files in application directories should probably be monitored. CIs have various configuration elements that change constantly during the course of normal operations. Monitoring non-key elements will result in a high volume of non-important data that consumes time and resources to review. Instead, monitoring must be tailored to what matters and what is initially feasible. Otherwise, the resulting data overload will cause the operators to miss true changes and lose faith in the system.
2. **There must be effective access controls and segregation of duties.** Excessive permissions and shared accounts should be removed. This includes limiting access to administrator functionality and a core set of authorized individuals who can promote code into production and/or change systems. Otherwise, it will be extremely difficult to correlate individuals or roles with detected changes. Once the permission model is established, Tripwire Enterprise can be used to monitor and report changes to permissions on user groups, files, registry entries, and Active Directory/LDAP objects.

Tripwire Enterprise effectively reinforces cultural change and helps enforcement of any change management policy. When the IT organization is aware that changes are audited and data is being collected, reviewed, and acted upon, individuals are significantly less likely to circumvent the defined change management processes.

To foster the incremental implementation of change management, let's consider three distinct stages of adoption that organizations can use. Based on years of experience building change control processes, we have found that the following incremental steps are effective measures toward controlling change and demonstrating visible and measurable wins:

1. **Enforce change windows.** This is easy to enforce and immediately creates a more stable operational environment, making it a powerful step. Begin by defining change windows for critical services and then implement the policy that changes can only be made within those windows.

   Enforcement is easy because any change made outside the change window is by definition an unauthorized change. Since all changes carry a degree of inherent risk, limiting them to certain periods of time increases stability during the periods outside the change window, and thereby reduces overall risk to operations. Furthermore, when changes inside the change window do fail, stakeholders will be better able to quickly associate resultant issues with the scheduled and detected changes.

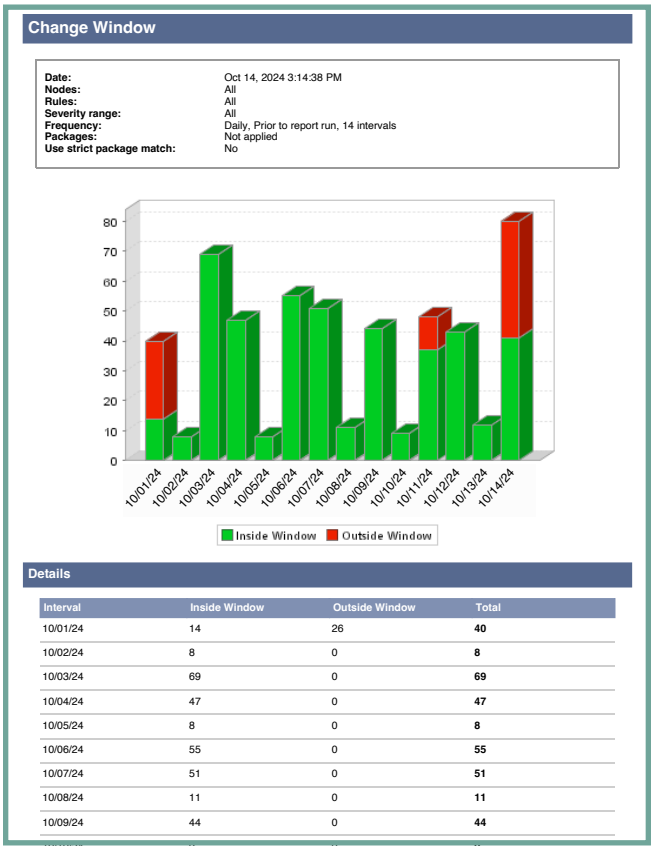
   Tripwire Enterprise provides a Change Windows Report to identify changes inside and outside of planned change windows. This can help determine compliance with the change window policy.

2. **Validate what changed within the windows.** In other words, now we need to ensure that the changes were duly authorized. This can be accomplished by using Tripwire Enterprise's intelligent promotion actions to uncover any unauthorized changes. This stage also validates that authorized work was completed successfully.

   To assist with the reconciliation process, the Change Process Compliance report can be used to review changes that can and cannot be mapped to an authorized RFC.

   Another useful report is Frequently Changed Nodes, which identifies the CIs that most frequently change. As the rate of change increases, so does the organization's risk level (see Figure 2). Thus, it is wise to monitor nodes with high rates of change to ensure that changes are properly managed and risks to the organization are reduced.

3. **Automate.** Create an automation link to other business tools using tailored integrations incorporating Tripwire's rich application-programming interface (API).



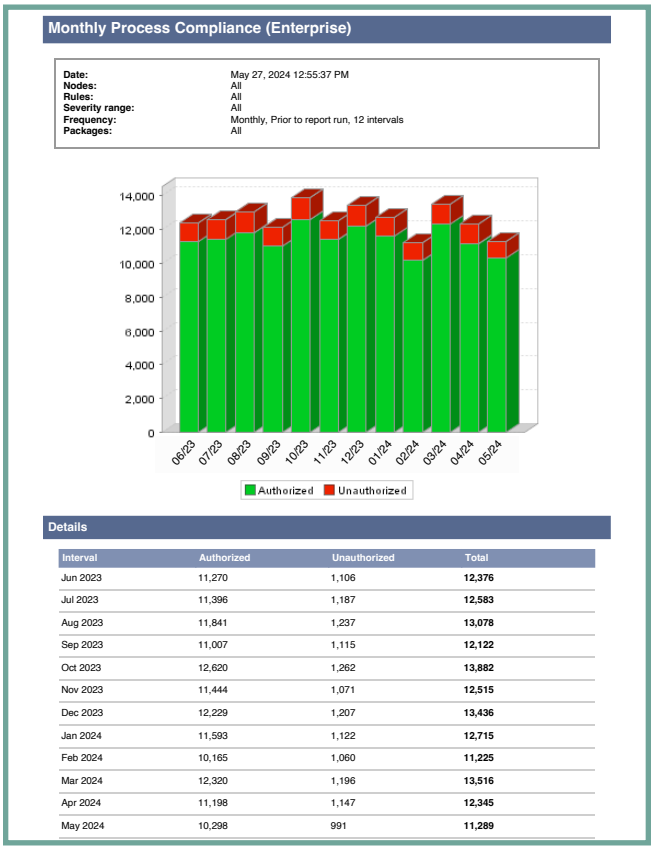
Change Window

Date: Oct 14, 2024 3:14:38 PM
Nodes: All
Rules: All
Severity range: All
Frequency: Daily, Prior to report run, 14 intervals
Packages: Not applied
Use strict package match: No

Details

Interval	Inside Window	Outside Window	Total
10/01/24	14	26	**40**
10/02/24	8	0	**8**
10/03/24	69	0	**69**
10/04/24	47	0	**47**
10/05/24	8	0	**8**
10/06/24	55	0	**55**
10/07/24	51	0	**51**
10/08/24	11	0	**11**
10/09/24	44	0	**44**

Fig. 3. Change Window Report



Monthly Process Compliance (Enterprise)

Date: May 27, 2024 12:55:37 PM
Nodes: All
Rules: All
Severity range: All
Frequency: Monthly, Prior to report run, 12 intervals
Packages: All

Details

Interval	Authorized	Unauthorized	Total
Jun 2023	11,270	1,106	**12,376**
Jul 2023	11,396	1,187	**12,583**
Aug 2023	11,841	1,237	**13,078**
Sep 2023	11,007	1,115	**12,122**
Oct 2023	12,620	1,262	**13,882**
Nov 2023	11,444	1,071	**12,515**
Dec 2023	12,229	1,207	**13,436**
Jan 2024	11,593	1,122	**12,715**
Feb 2024	10,165	1,060	**11,225**
Mar 2024	12,320	1,196	**13,516**
Apr 2024	11,198	1,147	**12,345**
May 2024	10,298	991	**11,289**

Fig. 4. Change Process Compliance Report

Modify First Response

"What changed?" should be the first question asked whenever an incident occurs. And if Mean Time to Repair (MTTR) metrics typically run high, this indicates that this question (and "Who did it?) cannot be answered easily. Integrating Tripwire Enterprise change detection data with incident and problem management processes will dramatically reduce MTTR by rapidly providing the answers to those questions.

One way to provide access to incident data is to grant read-only permissions to incident and problem management teams. They can manually query Tripwire Enterprise using the Changed Elements Report, and then quickly identify differences between expected baselines and detected production builds.

Phase One Completion Indicators

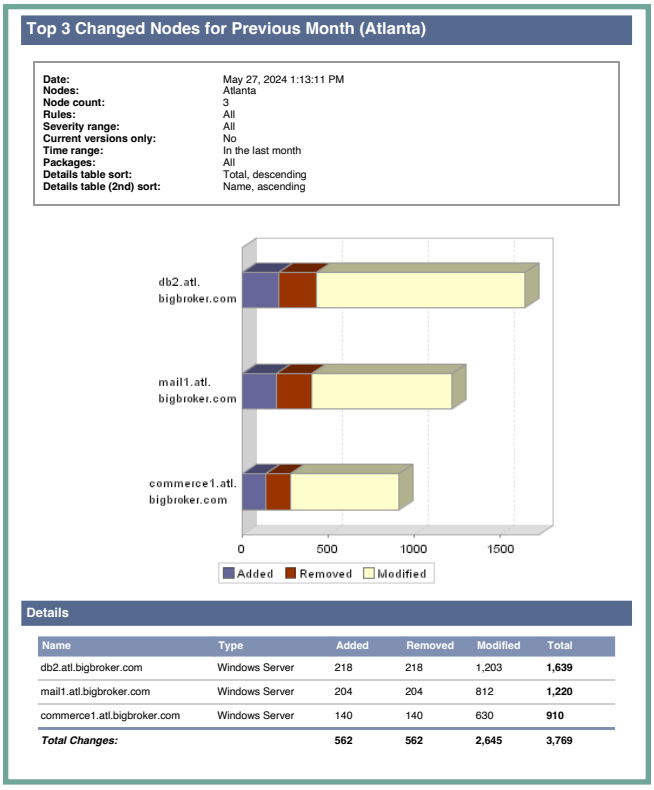
Phase one, "Stabilize the Patient," is vital because it results in a stable infrastructure that supports follow-on phases. These metrics will indicate when an IT organization has successfully completed Phase one:

- Unplanned work is reduced to 25 percent of operating expenses or less. Some organizations with high levels of process maturity have driven unplanned work as low as 5 percent.
- A change success rate of 70 percent or more. Achieving higher rates requires a detective control to enforce change management processes. Disciplined, high-performing organizations achieve change success rates reaching 99 percent.
- Low number of unauthorized changes (ideally zero).

Unless changes are managed, the production environment will not be stable enough to conduct a meaningful inventory, create repeatable builds, or successfully introduce desired changes.

Visible Ops Phase Two: Catch & Release and Find Fragile Artifacts

The next step is to identify CIs, particularly those that generate high amounts of unplanned work. This is achieved by inventorying existing production builds. Senior staff should perform inventory in order to transfer configuration details from their heads into a configuration management database.



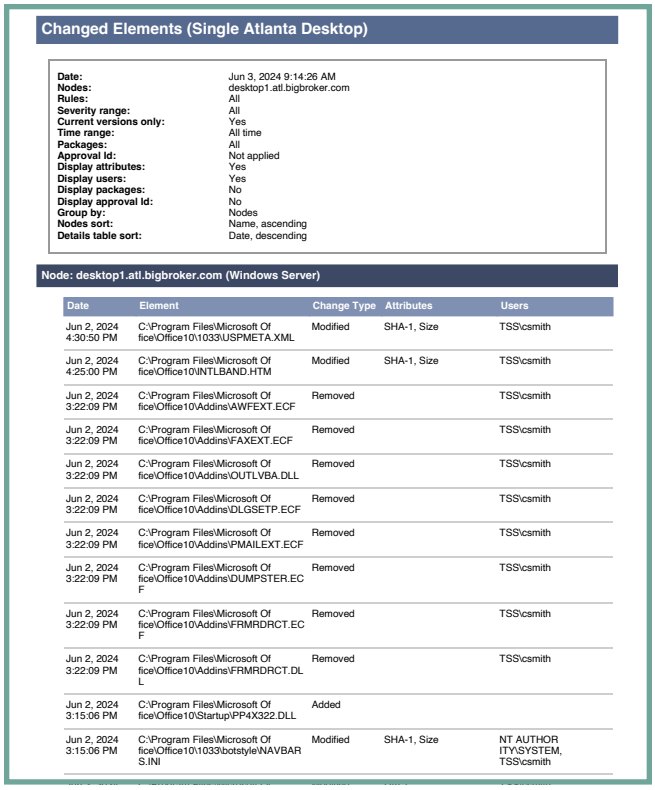
Top 3 Changed Nodes for Previous Month (Atlanta)

Date:	May 27, 2024 1:13:11 PM
Nodes:	Atlanta
Node count:	3
Rules:	All
Severity range:	All
Current versions only:	No
Time range:	In the last month
Packages:	All
Details table sort:	Total, descending
Details table (2nd) sort:	Name, ascending

Details

Name	Type	Added	Removed	Modified	Total
db2.atl.bigbroker.com	Windows Server	218	218	1,203	**1,639**
mail1.atl.bigbroker.com	Windows Server	204	204	812	**1,220**
commerce1.atl.bigbroker.com	Windows Server	140	140	630	**910**
Total Changes:		**562**	**562**	**2,645**	**3,769**

Fig. 5. Frequently Changed Nodes Report



Changed Elements (Single Atlanta Desktop)

Date:	Jun 3, 2024 9:14:26 AM
Nodes:	desktop1.atl.bigbroker.com
Rules:	All
Severity range:	All
Current versions only:	Yes
Time range:	All time
Packages:	All
Approval Id:	Not applied
Display attributes:	Yes
Display users:	Yes
Display packages:	No
Display approval Id:	No
Group by:	Nodes
Nodes sort:	Name, ascending
Details table sort:	Date, descending

Node: desktop1.atl.bigbroker.com (Windows Server)

Date	Element	Change Type	Attributes	Users
Jun 2, 2024 4:30:50 PM	C:\Program Files\Microsoft Office\Office10\1033\USPMETA.XML	Modified	SHA-1, Size	TSS\csmith
Jun 2, 2024 4:25:00 PM	C:\Program Files\Microsoft Office\Office10\INTLBAND.HTM	Modified	SHA-1, Size	TSS\csmith
Jun 2, 2024 3:22:09 PM	C:\Program Files\Microsoft Office\Office10\Addins\AWFEXT.ECF	Removed		TSS\csmith
Jun 2, 2024 3:22:09 PM	C:\Program Files\Microsoft Office\Office10\Addins\FAXEXT.ECF	Removed		TSS\csmith
Jun 2, 2024 3:22:09 PM	C:\Program Files\Microsoft Office\Office10\Addins\OUTLVBA.DLL	Removed		TSS\csmith
Jun 2, 2024 3:22:09 PM	C:\Program Files\Microsoft Office\Office10\Addins\DLGSETP.ECF	Removed		TSS\csmith
Jun 2, 2024 3:22:09 PM	C:\Program Files\Microsoft Office\Office10\Addins\PMAILEXT.ECF	Removed		TSS\csmith
Jun 2, 2024 3:22:09 PM	C:\Program Files\Microsoft Office\Office10\Addins\DUMPSTER.ECF	Removed		TSS\csmith
Jun 2, 2024 3:22:09 PM	C:\Program Files\Microsoft Office\Office10\Addins\FRMRDRCT.ECF	Removed		TSS\csmith
Jun 2, 2024 3:22:09 PM	C:\Program Files\Microsoft Office\Office10\Addins\FRMRDRCT.DLL	Removed		TSS\csmith
Jun 2, 2024 3:15:06 PM	C:\Program Files\Microsoft Office\Office10\Startup\PP4X322.DLL	Added		
Jun 2, 2024 3:15:06 PM	C:\Program Files\Microsoft Office\Office10\1033\botstyle\NAVBARS.INI	Modified	SHA-1, Size	NT AUTHORITY\SYSTEM, TSS\csmith

Fig. 6. Changed Elements Report

Catch & Release

During the inventory of production builds, all configuration data and relationships must be entered into the change management database and, current builds should be entered in a production Definitive Software Library (DSL) through an amnesty program. The Tripwire Enterprise database stores current build data as a baseline, enabling the software to detect changes to key attributes. If changes are unauthorized, the affected system can be returned to its baseline through the stored build.

Find Fragile Artifacts

An important part of change management is identifying failed changes — those that cannot be implemented according to the formal plan in the allotted period of time. If a change fails or causes incidents later on, then the change identifier should be related to the incident ID to facilitate tracking and identification.

A fragile artifact is a CI with abnormally high levels of downtime, integrity breaches, or security compromises when changes are attempted. They may also exhibit sporadic, elusive availability problems causing frequent Service Level Agreement (SLA) issues. If a given CI has a high rate of change and availability problems, then it should be considered a fragile artifact.

To identify fragile CIs, staff should manually review availability logs and compare them to Tripwire Enterprise and service desk reports. In mature IT organizations, Tripwire Enterprise data can be collected using the API and merged with network monitoring and service desk availability data to enhance analysis. One Tripwire Enterprise report that helps identify fragile artifacts is the Frequently Changed Nodes report (see Fig 5).

Once fragile artifacts are identified, prioritize them by the amount unplanned work each generates. If possible, it is also helpful to determine how they became fragile in the first place — that is, what caused the problem? If cause can be established, you know how to avoid repeating the incident.

Production builds should be regularly compared to stored baselines to identify unauthorized changes that cause configuration drift. All changes should reconcile to documented work orders, or corrective action will be required.

The Reference Node Variance report can be used to compare production builds to baselines and to compare "identical" hosts where one exhibits problems and the other doesn't. Small, previously missed differences can be readily identified and remedied in the next version of the build.

Visible Ops Phase Three: Create a Repeatable Build Library

Phase three builds on a stable change and configuration management environment. Here, we standardize builds to reduce production variations. Once the pre-production environment mirrors production, builds can be developed and tested, and releases can be crafted. Changes to known baselines can be documented and presented to the Release Management team for review and approval. In turn, Release Management documents all of their releases and presents findings to Operations staff, who can then reconcile all changes detected after installation.

This review allows Release Management and Operations teams to verify production releases with supporting evidence for audits. Either team can use the Tripwire Reference Node Variance Report to identify system deviations and reference the build catalog for comparing pre-production to production systems.

Visible Ops Phase Four: Continuous Improvement

Phase four is an ongoing process that provides a framework for using change management process metrics to pinpoint areas for improvement and document the presence of effective IT controls.

The IT Process Institute (ITPI) performed a benchmarking survey that measured the value, effectiveness, and efficiency of security controls to determine which ones deliver a high return on investment. The survey assumed that the amount of unplanned work experienced by IT organizations was related to failed changes. The data led to the results documented in Fig. 2.

Reducing failed changes and/or MTTR should result in lower levels of unplanned work, and data proves that this is indeed true. Assuming that the number of production changes will be relatively constant, the challenges lie in reducing failed changes and the MTTR.

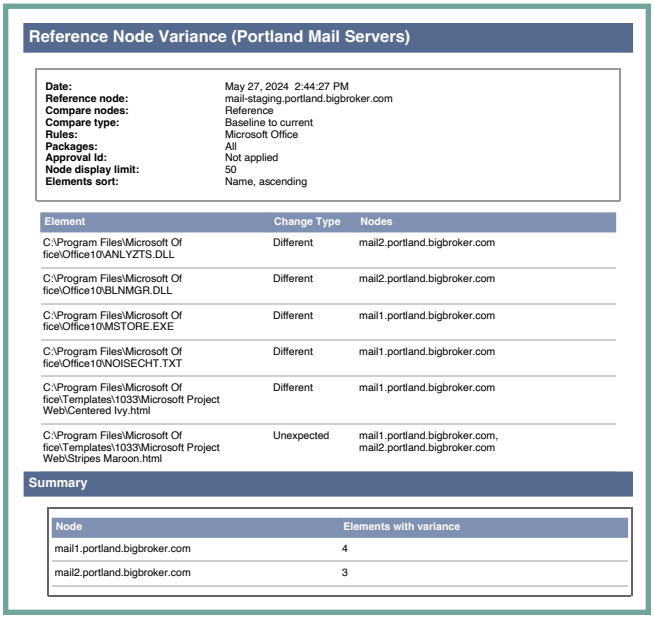
Tracking Process Compliance with Tripwire Enterprise

Tripwire Enterprise becomes a vital element of effective ongoing change and configuration management.

- Tripwire Enterprise Change Process Compliance and Change Window reports can track racking compliance with change management processes
- Frequently Changed Nodes reports can highlight volatile systems that may warrant further investigation.
- Tripwire reports are used to compare production builds to stored baselines and find variances for more accurate building and testing.
- Tripwire reports enable Release Management to match pre-production machines with production systems for accelerated development and testing.
- Tripwire Enterprise enables Operations staff to quickly know what changed, how it changed, and who changed it.

Improved Visibility Drives Improved IT Performance

The ITPI Visible Ops methodology is playing an important role in many world-class IT organizations as they work to improve processes and enforce a culture of change management. With Tripwire Enterprise as a fundamental change audit tool, these organizations are achieving their compliance, security, and service quality goals more quickly — and gaining high, positive visibility within their enterprises.



Reference Node Variance (Portland Mail Servers)

Date:	May 27, 2024 2:44:27 PM
Reference node:	mail-staging.portland.bigbroker.com
Compare nodes:	Reference
Compare type:	Baseline to current
Rules:	Microsoft Office
Packages:	All
Approval Id:	Not applied
Node display limit:	50
Elements sort:	Name, ascending

Element	Change Type	Nodes
C:\Program Files\Microsoft Office\Office10\ANLYZTS.DLL	Different	mail2.portland.bigbroker.com
C:\Program Files\Microsoft Office\Office10\BLNMGR.DLL	Different	mail2.portland.bigbroker.com
C:\Program Files\Microsoft Office\Office10\MSTORE.EXE	Different	mail1.portland.bigbroker.com
C:\Program Files\Microsoft Office\Office10\NOISECHT.TXT	Different	mail1.portland.bigbroker.com
C:\Program Files\Microsoft Office\Templates\1033\Microsoft Project Web\Centered Ivy.html	Different	mail1.portland.bigbroker.com
C:\Program Files\Microsoft Office\Templates\1033\Microsoft Project Web\Stripes Maroon.html	Unexpected	mail1.portland.bigbroker.com, mail2.portland.bigbroker.com

Summary

Node	Elements with variance
mail1.portland.bigbroker.com	4
mail2.portland.bigbroker.com	3

Fig. 7. Reference Node Variance Report

Visible Ops Phases and Tripwire Enterprise Reports

Summary of how Tripwire Enterprise can be used to assist in the implementation of the Visible Ops methodology.

Visible Ops Phase	Steps	Notes	Tripwire Enterprise Reports
Phase One: Stabilize the Patient	**1.** Electrify the Fence — Implement a change management process and a detective control	• Implement Tripwire Enterprise to monitor for compliance to the process. Leverage the Change Window and Change Process Compliance reports.	**Change Process Compliance** **Change Window**
	2. Configuration Item (CI) access permissions should be reviewed and reduced to the minimum possible.	• Tripwire Enterprise can monitor access permissions via access control lists, local registry entries, LDAP and active directory. Tripwire Enterprise can then alert when changes are detected.	**Changed Elements**
	3. Modify First Response — Provide incident and problem management teams with access to the detected change data.	• Grant read-only report access to individuals involved with incident and problem management. Use the Changed Element report.	**Changed Elements**
Phase Two: Catch & Release and Find Fragile Artifacts	**1.** CIs in scope have builds inventoried and recorded.	• Tripwire Enterprise can store a baseline for each CI in scope.	**Change Variance**
	2. Production systems should have their builds audited against stored baselines to guard against configuration drift.	• Tripwire Enterprise can routinely compare the production system to the stored baseline and highlight differences.	**Missing Elements** **Frequently Changed Elements**
		• The Frequently Changed Nodes report can be used to identify systems with high levels of change that may warrant investigation.	**Frequently Changed Nodes**
Phase Three: Create a Repeatable Build Library	**1.** Pre-production systems must mirror production systems for repeatable builds to be possible.	• Tripwire Enterprise can be used to audit all systems in question to verify that the builds match the expected stored baselines.	**Change Variance** **Changed Elements**
	2. Operations needs assurance that what they will install is properly documented and that what they have installed matches expectations.	• Tripwire Enterprise can be used to generate a change or release manifest to verify a release before acceptance and to verify the final implementation into production.	**Change Variance** **Changed Elements**
Phase Four: Continuous Improvement	**1.** Metrics need to be collected and used to identify areas for process improvement.	• Use Tripwire Enterprise's Change Process Compliance, Change Window and Frequently Changed Nodes reports to monitor the health of the change management process. Use the Changed Elements report to audit production builds against their relevant baselines.	**Change Process Compliance** **Change Window** **Changed Elements** **Frequently Changed Nodes**

Sources

1. https://www.lookfar.com/blog/2022/01/12/software-maintenance-understanding-and-estimating-costs/

2. https://www.cio.com/article/3487383/moderate-it-budget-increases-have-cios-shaping-2025-strategies-to-suit.html

3. https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/

FORTRA®

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(tw-gd-1224-r2-hm)