Threat Intelligence & Closed-Loop Intelligent Change Control

Enhancing the Value of FIM for Breach Detection

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

Precis

> *"perform critical file comparisons at least weekly"*

The visibility of configuration changes provided by File Integrity Monitoring may provide a great solution for breach detection and security governance, but in the past this has come at a price.

Changes need to be reviewed and approved and to do this properly has always been a labour-intensive task. By combining Threat Intelligence with FIM, a knowledgebase of ***'known safe'*** files can be leveraged to improve the accuracy and speed of change review.

But if this knowledge is then leveraged to power contemporary Intelligent Change Control technology, the resourcing savings are multiplied. With the constantly-improving expertise being fed back to automatically review other occurrences of the same change patterns estate-wide, change control and breach detection processes are straightforward to operate even on large-scale Enterprise IT estates.

The Pros and Cons of File Integrity Monitoring: Change Noise

FIM technology has always been a key component of any information security strategy. FIM is the only technology that can both audit and score configuration settings to mitigate vulnerabilities, but also detect any system file changes too. This gives FIM an added advantage over the blacklist approach of AV: AV is always blind to Zero-day trojan malware and equally ineffective in detecting cunning APT incursions.

PCI Security Standards Council

PCI DSS Requirements	Testing Procedures	Guidance
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. *Note: For change-detection purposes*	**11.5.a** Verify the use of a change-detection mechanism within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files	Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected. If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls

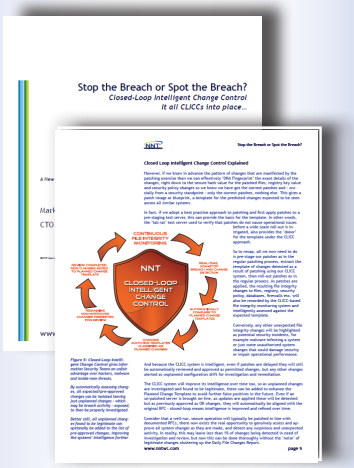
"perform critical file comparisons at least weekly."

But there is a problem. Having complete visibility of system configuration integrity changes introduces an unwanted side-effect: FIM Change Noise. And it can become ***D E A F E N I N G ! ! !***

Detecting subtle breach activity requires forensic-level clarity on all system activity: a new system file or an existing one being changed, a new service being created, new network ports being used, and so on.

You are going to need to set the zoom to max and crank the volume up to 10 to detect breach activity that is designed to be covert.

However, this also means that any other system activity is going to be amplified too: the change noise produced by patches, updates, software installs, new users, new devices can quickly become overwhelming.



Abstract

Within any IT estate, the only constant is change.

Change Control has always been a key security best practice. With every change made to IT systems comes a risk of a weakening of security defenses, not to mention operational problems, through misconfigurations.

Changes also create 'noise' that makes it more difficult to detect a breach when a cyber attack succeeds.

With Change Control notoriously difficult to operate, especially at the forensic level of detail needed for security governance, a new approach is needed that gives the level of analysis necessary for breach detection.

But how can this be provided without overloading already stretched IT Departments with yet more procedures to follow and alerts to review?

This white paper explores the need for file integrity monitoring-based change control and proposes a new approach to streamlining the review of security incidents and planned changes through automated, intelligent analysis.

Intelligent Change Control: Review Once, Approve Forever

Fortunately, this is where NNT Change Tracker Gen 7 introduces a revolutionary new approach to dealing with Change Noise: Closed-Loop Intelligent Change Control (documented in the previous whitepaper 'Stop the Breach or Spot the Breach? Closed-Loop Intelligent Change Control. It all CLICCs into place…')

> ***Quick recap:*** CLICC reconciles the security benefits of forensic change control with the detailed workload necessary to review changes. When legitimate patches have been deployed, the inventory of changes made on one server will be the same as for all other similar servers. By monitoring the filesystem of a host, firewall or POS system, any changes to configuration files or system files can be detected and highlighted for review.

In short – review changes on one server, once only, to produce an Intelligent Planned Change template. Using this template, all other changes across the estate – both past and future changes – will be automatically reviewed and approved on any other server, even if there are hundreds or thousands of devices all with hundreds of changes on each.

This alone has transformed the effectiveness and ease of use for FIM as a breach detection solution.

Change Detected! But is it Safe?

So Intelligent Change Control can substantially cut down the need to review all FIM changes on all devices, but there is still that initial review of first-time changes needed.

This has always been a slightly daunting business, regardless of whether you have used Tripwire® or NNT Change Tracker. At best, it is a straightforward but time-consuming procedure, identifying changes and approving them. At other times, deciphering whether unexpected change activity is really 'safe/OK' versus 'unexpected/breach activity' can require CSI-levels of forensic investigative process.

Fortunately, there is even more good news in this area: Change Tracker Gen 7 has got your back on this one, too.

Time to introduce a further innovation in Gen 7, one that brings instant confidence and authoritative corroboration that changes really are safe: Threat Intelligence.

But before we get into the new world of Threat Intelligence and FIM, how has this level of confidence in 'safe changes' been provided in the past?

> *"Since any new patch may have undesirable side-effects in terms of adversely affecting service delivery, it makes sense to test the patch on a trial basis before deploying to the entire Production Estate"*

Patch Lab-Rat: No Animals were Harmed During this Patch Roll-Out

Using a 'patch lab-rat' or pre-staging system is a security best practice that can be employed to provide surety between the cause and effect of patches or updates.

In summary, an isolated test system can be patched under highly controlled circumstances with the impact recorded, and is a widely-advocated practice not just to help with change control. Since any new patch may have undesirable side-effects in terms of adversely affecting service delivery, it makes sense to test the patch on a trial basis before deploying to the entire Production Estate.

In fact, Change Tracker Gen 7 already provides a standard facility to record changes from a test system and automatically build an Intelligent Planned Change template using those changes detected. The controlled environment of the test system provides the guarantee that the changes recorded are directly attributable to the patching and nothing else, a conclusion that can't be made with the same level of certainty when using events observed from live production systems.

The only problem with this is just that it requires more planning and organization prior to deployment and not everyone has got the resources or procedural maturity to always work in this manner.

The latest NNT option to help with this is to leverage Threat Intelligence, and more specifically, File Whitelisting repositories.

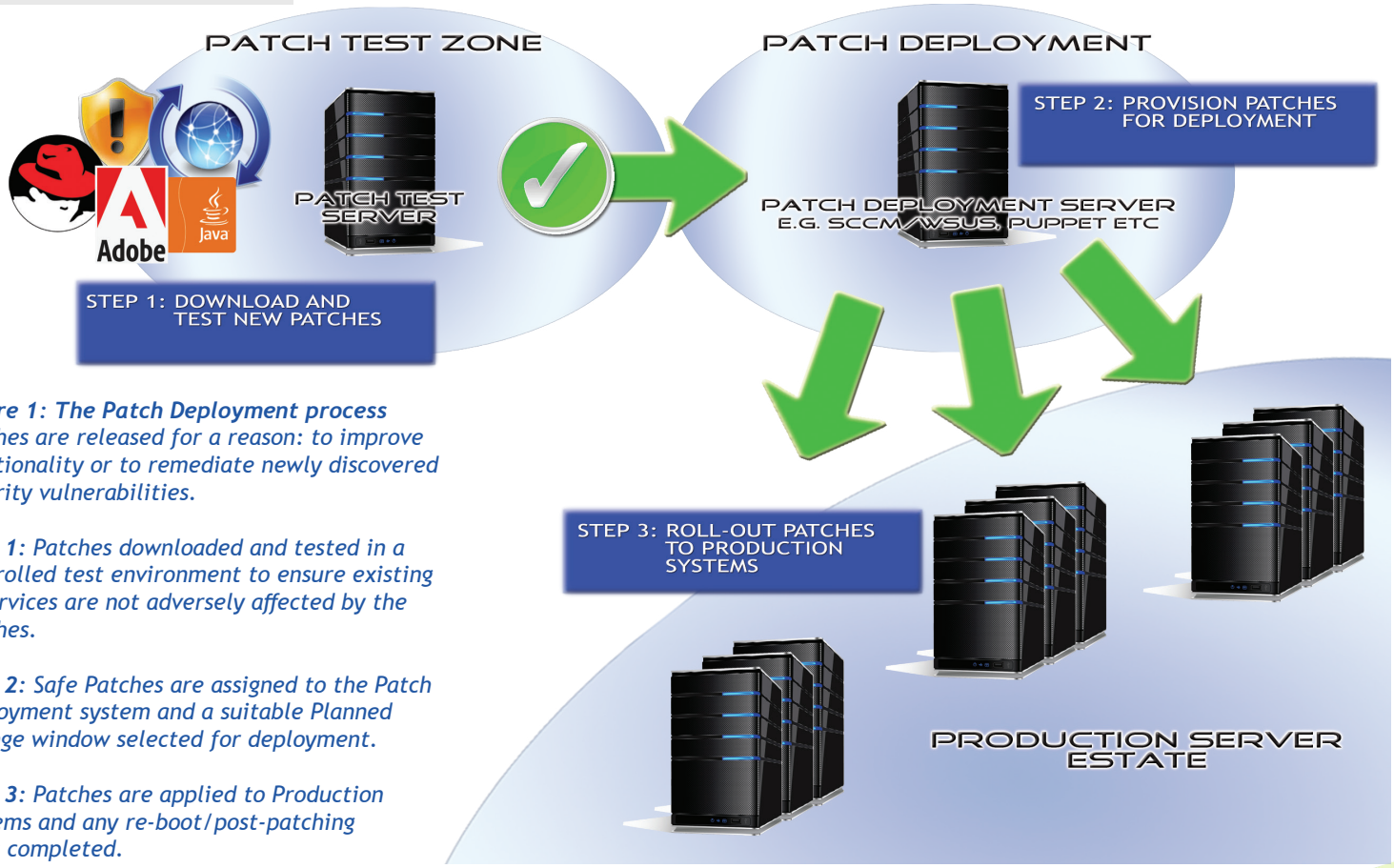


Figure 1: The Patch Deployment process
Patches are released for a reason: to improve functionality or to remediate newly discovered security vulnerabilities.

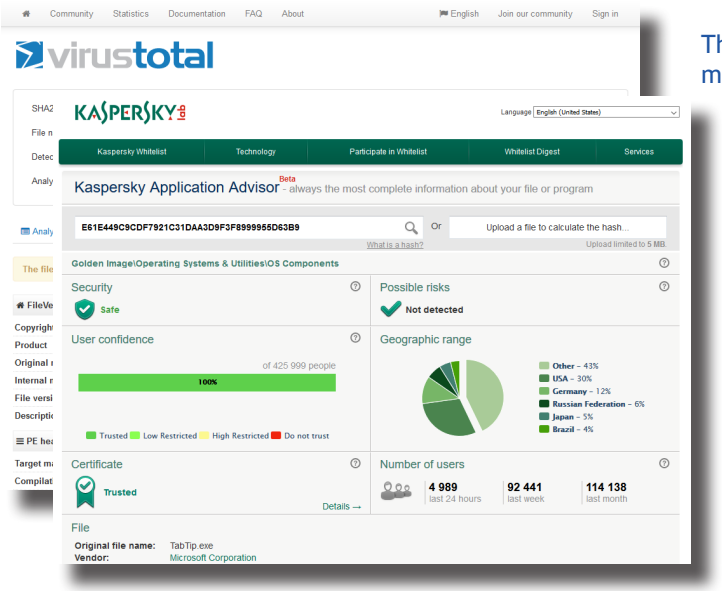
***Step 1**: Patches downloaded and tested in a controlled test environment to ensure existing IT services are not adversely affected by the patches.*

***Step 2**: Safe Patches are assigned to the Patch Deployment system and a suitable Planned Change window selected for deployment.*

***Step 3**: Patches are applied to Production Systems and any re-boot/post-patching work completed.*

The File Whitelist: Right Solution, Wrong Application...

A File Whitelist is based on a completely opposite line of thinking to the approach taken by AV systems. Signature-based AV scanners are designed to look for known-bad files. The logic is that any file not on the blacklist is OK/safe.



The fatal flaw with this approach is that too many newly originated malware variants – aka Zero Day malware – can be active in the wild for weeks or even months before they are identified and added to the blacklist. During this Zero Day period they remain covert and invisible to the AV system, free to infect and wreak havoc.

No surprise then that the Whitelisting approach assumes any file is bad unless it is specifically on the whitelist. This provides a safety-first approach but ultimately is still a flawed solution to providing absolute surety of security. The same issues that blunt the blacklists' effectiveness – the list is always out of date and behind the curve - also limit the effectiveness of a whitelist. The best cloud-based whitelist repositories available today are built collaboratively with leading software developers, leading to claims of 95% + coverage of all commercial software components being included in the whitelist, although of course this still leaves blindspots.

But what if we are actually using the whitelist in the wrong way? Accepting that AV systems, whitelists and blacklists do not provide a 100% guarantee of threat protection is why FIM is so valuable as a breach detection and change control solution. If instead we were to instead embrace both technologies and operate them in a combined solution wouldn't this give us the best of both worlds?

The FIM solution provides the clear visibility of all configuration changes, not just file changes, and is the ideal tool for reviewing and approving changes as detected. The intelligence of the FIM solution is always being improved to in its awareness of required exclusions and is able to cope with any applications, even unique, bespoke systems developed in-house.

But even an intelligent FIM solution can be significantly enhanced by leveraging the encyclopaedic knowledge inherent in a whitelist repository. As changes are reported for review, the whitelist repository can provide the expert insight required to understand the file heritage and get a positive assurance that the file is 'known safe'.

It gets better: Using Change Tracker Gen 7, any gaps in the whitelist knowledge are plugged using Intelligent Change Control, with Gen 7 continually improving its own whitelist of known-good change patterns and behaviours. Not only can the whitelist be queried manually when assessing the validity of a particular file, but can alternatively be used to automatically check each and every file change as it is detected.

Due to the nature of IT estates typically monitored for FIM being inherently securely operated, with tight access and change control in place, the overwhelming majority of changes detected should be planned, intended changes. Therefore, using Threat Intelligence in this automated mode, any filechanges that either do not match a Change Tracker Intelligent Planned Change template, or do not check out as known safe on the whitelist, will be extremely rare and as such, will always be highlighted as critical security events.