

**BUYER'S GUIDE**



# File Integrity Monitoring (FIM)

## 8 Key Considerations



# Table of Contents

---

<b>1. Executive Summary</b> .....	<b>3</b>
<b>2. Introduction - What is FIM and why is it important?</b> .....	<b>4</b>
<b>3. What should you look for in an effective FIM solution?</b> .....	<b>6</b>
a) Surveillance must be Real-time and context-rich	
b) Monitoring must be cross-platform/application/device for any heterogeneous enterprise estate	
c) The 'I' in FIM is the most important element	
d) Must provide forensic detail while muting change noise	
e) Must integrate with SIEMs and SOCs to provide critical assistance during any root cause analysis	
f) Must support the complete GRC spectrum from DISA STIG through NIST 800, NERC, PCI and not stop until SOX	
g) Must be able to scale in a linear manner from 10 devices to 1M+	
h) Change Control must leverage ITSM Planned Change/RFC data	
<b>4. What should be monitored?</b> .....	<b>18</b>
<b>5. Change Tracker from NNT – Not just any old FIM</b> .....	<b>19</b>
a) Platforms/Devices/Containers Covered	
b) Configuration Settings and Attributes	
c) Change Tracker Management Console	
<b>6. SecureOps™ Feature set</b> .....	<b>23</b>
<b>7. Conclusion</b> .....	<b>24</b>



## EXECUTIVE SUMMARY

---

There is still no such thing as **'100%'** secure. Nobody can offer a guarantee to stop every Cyber Attack. Breaches keep coming, even for the world's largest and best resourced organizations.

**What's going wrong?** Despite increasing investments in IT Security year on year, annual incidences of data breaches are growing even faster with over 7.9 billion data records exposed between January and September 2019 - a 33% increase from the same period in 2018.

WannaCry in 2017, which hit over 230,000 victims in 150 countries within a matter of days, showed that we are all at risk of similar 'perfect storms' when a ubiquitous vulnerability is uncovered and exploited quickly before natural patching cycles can provide protection.

It's only a matter of time before the next malware pandemic strikes, but in the meantime, phishing attacks will continue to probe for any weakness.

The rules for Cybersecurity Professionals remain the same. Operate all security best practices, and don't cut corners on either vulnerability management or change control, critical to both maintaining security defenses and to isolating breach activity if and when it does happen.

# WHAT IS FIM AND WHY IS IT IMPORTANT?

**File Integrity Monitoring (FIM)** is an essential security control operated to expose any change to the integrity of system and configuration files. Maintaining integrity is key for two key reasons:



Changes to files could represent a malware infection and FIM provides a forensic-level Breach Detection mechanism to combat this.



With prevention better than cure, security defenses can only be maintained via a secure, 'hardened' configuration, so monitoring for any decay or drift of configuration states is vital.

Integrity Monitoring directly relates to the concept of Change Control. Any organization's '**Attack Surface**' is affected by changes made, chiefly to installed software and configuration settings. And from a security standpoint, change control is the only way to distinguish between legitimate IT activity, and a stealthy cyber-attack.

“ACCORDING TO THE 2019 VERIZON DATA BREACH INVESTIGATION REPORT, 56% OF BREACHES TAKE MONTHS OR LONGER TO DISCOVER.”



# WHAT SHOULD YOU LOOK FOR IN AN EFFECTIVE FIM SOLUTION:

---

Below are 8 essential considerations when selecting the right FIM solution

1. Surveillance must be Real-time and context-rich
2. Monitoring must be cross platform/application/device for any heterogeneous enterprise estate
3. The 'I' in FIM is the most important element
4. Must provide forensic detail while muting change noise. Files change, they are meant to change. Ensure your FIM solution is able to separate normal change from abnormal or unexpected
5. Must integrate with SIEMs and SOCs to provide critical assistance during any root cause analysis
6. Must support the complete GRC spectrum from DISA STIG through NIST 800, NERC, PCI and not stop until SOX
7. Must be able to scale in a linear manner from 10 devices to 1M+
8. Change Control must leverage ITSM Planned Change/ RFC data

# 1

## SURVEILLANCE MUST BE REAL-TIME AND CONTEXT-RICH

---



Immediate notification with enough supporting information to ensure the alert is useful and actionable. A notification that says **'File Changed'** in isolation for example provides no value whatsoever.

In fact, many so called FIM tools will actually compound the issue by simply monitoring file activity, which will generate an enormous amount of change noise, making the task of identifying malicious activity even harder. You would almost be better off with no FIM solution at all.

The critical element here, is the ability to determine which file activity is known, expected and harmless compared to that which is potentially dangerous or disruptive.

Make sure that any solution implemented doesn't just report file changes, but incorporates forensic and behavioral analytics with essential integrations with other trusted source information, such as the ability to determine whether or not the change was part of a planned change, matches an approved change manifest or is whitelisted and recognized as good.

## 2

# MONITORING MUST BE COMPREHENSIVE FOR ANY HETEROGENEOUS ENTERPRISE ESTATE

---



Today's enterprise networks will often comprise a vast range of assets, from the latest cloud and container-mobilized applications, through to legacy applications based on end-of-life platforms and everything in between.

While business-critical services will naturally register as the highest priority for protection, many attack vectors exploit users and user workstations to instigate an attack. Once a vantage point within the enterprise has been established, deeper and more damaging attacks can be staged.

The logical conclusion is that all IT assets need to be both protected from attacks and monitored in case of a breach. Make sure that your Integrity Monitoring solution can cover all contemporary and legacy platforms, and be extended to cover user Workstations and network devices too.

### 3

## THE 'I' IN FIM IS THE MOST IMPORTANT ELEMENT

---



Many so-called FIM solutions ignore the most critical element, which is the integrity of the file. Make sure the solution you choose can reliably and intelligently separate regular, normal file change from irregular threats to the integrity of the file.

This is where Change Control comes into play, and why it is not the same as Change Management. While Change Management focuses on the justification and planning of any changes, Change Control majors on the verification and approval of actual changes made.

Without Change Control, you won't know if changes you wanted were correctly implemented. And from a security standpoint, you have no way of distinguishing between legitimate IT activity, and a stealthy cyber-attack. This is why, according to the Verizon Data Breach Investigation Report 2019, 56% of breaches take months to discover.

It's important to ensure your FIM solution is able to separate normal changes from abnormal or unexpected changes.

# 4

## MUST PROVIDE FORENSIC DETAIL WHILE MUTING CHANGE NOISE

---



Files change all the time, for example log files or database datastore files. Other files, for example, core system files or drivers, will only change occasionally when new versions are installed.

Even then, things aren't quite so simple. Changes to configuration settings may be intentionally made and for solid business reasons, but this may also have side effects and result in weakened security. Trojan malware which replaces and impersonates genuine system files will look and feel almost identical to a regular patch being applied.

One of the traditional issues with any security monitoring technology is the false positive, also known as alert fatigue or change noise.

In a large estate with a lot of change, trying to detect tiny levels of stealthy breach activity that is trying to remain hidden is impossible unless change noise is efficiently managed.

The most effective contemporary FIM solutions leverage automatic analysis of file changes to go beyond the simplistic 'here's another change to investigate' method. One approach is to use threat intelligence in the form of file reputation which can be referenced as a **'Trusted File Whitelist.'**

The overwhelming majority of file changes in a secure IT estate will be attributed to regular patching, for example, Windows Updates.

Given that your IT estate is inherently secure and subject to change control and other security best practices, >99.99% of changes recorded will be 'safe'. Not always expected or operationally desirable, but at least files have been provided by the manufacturer and not a hacker.

With the threat of Zero Day malware increasing daily, viruses not yet blacklisted by the AV and Sandbox vendors will still be isolated from 'known safe' files present in the whitelist.



Make sure you get the most comprehensive file whitelist capability to minimize change noise and false positives.

“ THE BEST SOLUTIONS IN THE MARKET PROVIDE FILE REPUTATION DATA FOR OVER 9 BILLION FILES FROM OVER 650 PUBLISHERS. ”

# 5

## MUST INTEGRATE WITH SIEMS AND SOCS TO PROVIDE CRITICAL ASSISTANCE DURING ANY ROUTE CAUSE ANALYSIS



Your change control solution will need to feed into your SOC, typically by logging events to an intelligent SIEM system such as Splunk, IBM QRadar or Microfocus ArcSight. Operation of a SOC has a number of key objectives:



To detect and respond to threats, keeping the information held on systems and networks secure



To increase resilience by learning about the changing threat landscape (both malicious and non-malicious, internal and external)



To derive business intelligence about user behaviors in order to shape and prioritize the development of technologies



**“ BUT ACCORDING TO RESEARCH FROM THE PONEMON INSTITUTE 2019, MORE THAN HALF OF SECURITY PROFESSIONALS RATE THEIR SOC AS ‘INEFFECTIVE’, DUE TO TOO MANY FALSE POSITIVES AND THE SOC JUST BEING TOO COMPLEX. ”**

So, another key selection criteria for the FIM solution is to ensure that logged events are delivered in an Industry Standard Common Event Format. Without this, SIEM solution effectiveness is blunted due to its inability to properly interpret event intelligence.

Make sure there are Certified Apps, Add-Ons and integrations with leading SIEM systems to minimize spurious events and maximize the value of FIM data.

## MUST SUPPORT THE COMPLETE GRC SPECTRUM FROM DISA STIG THROUGH NIST 800, NERC, PCI AND NOT STOP UNTIL SOX



The default configuration settings for most platforms, applications and devices are optimized for ease of use and deployment, not security. Open services and ports, unnecessary software, old vulnerabilities - all can be exploited in their default state.

For this reason, organizations must maintain documented, security configuration standards for all authorized operating systems and software.

As a foundational security control, System or Configuration Hardening is a priority best practice in every GRC mandate. However, none are fully prescriptive and all place varying degrees of emphasis on the various facets of configuration, **for example** NERC CIP is very clear on the need to manage Open Ports and Services, while the PCI DSS focuses more on the need to minimize function and especially system services.

Therefore, another priority when selecting a FIM system is to ensure Compliance Standard-specific reports are available and included without additional charge. Many organizations end up needing to demonstrate compliance with a range of standards, so it is wise to verify coverage is comprehensive.

## MUST BE ABLE TO SCALE IN A LINEAR MANNER FROM 10 DEVICES TO 1M+



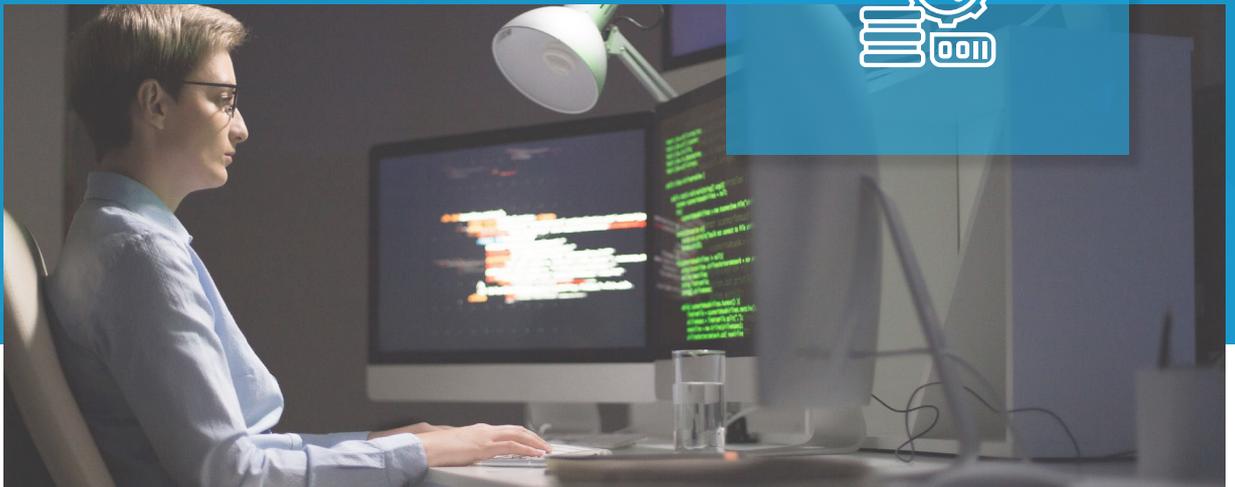
As change control solutions have been extended to incorporate some or all of the 'must have' features outlined in this guide, scale then becomes more difficult and expensive to deliver.

Most solutions will still handle device counts in the range of 0 – 8,000 but once in the 10,000+ device bracket the demand for expensive hardware resources becomes significant. Moving into the 20K + device range will then push some systems to breaking point, unable to process and analyze these higher levels of events. Tiered architectures and distributed consoles are sometimes employed as workarounds but can become restrictive.

Whether you are looking to cover large numbers of devices, or you anticipate needing to handle high volumes of events and reports, make sure you have a clear picture of how scalability is achieved and at what cost, both in terms of hardware resource and software requirements, for example Oracle or MS SQL licenses.

## CHANGE CONTROL MUST LEVERAGE ITSM PLANNED CHANGE/RFC DATA

---



Traditional change management takes the position that there shouldn't be any change to an IT system without a proper business justification.

**'If it ain't broke, don't fix it'** – and if there isn't a tangible benefit to outweigh the natural risk of any IT system change then the change shouldn't be progressed. Security requires even more stringent checks and balances on changes being made for **two key reasons**.

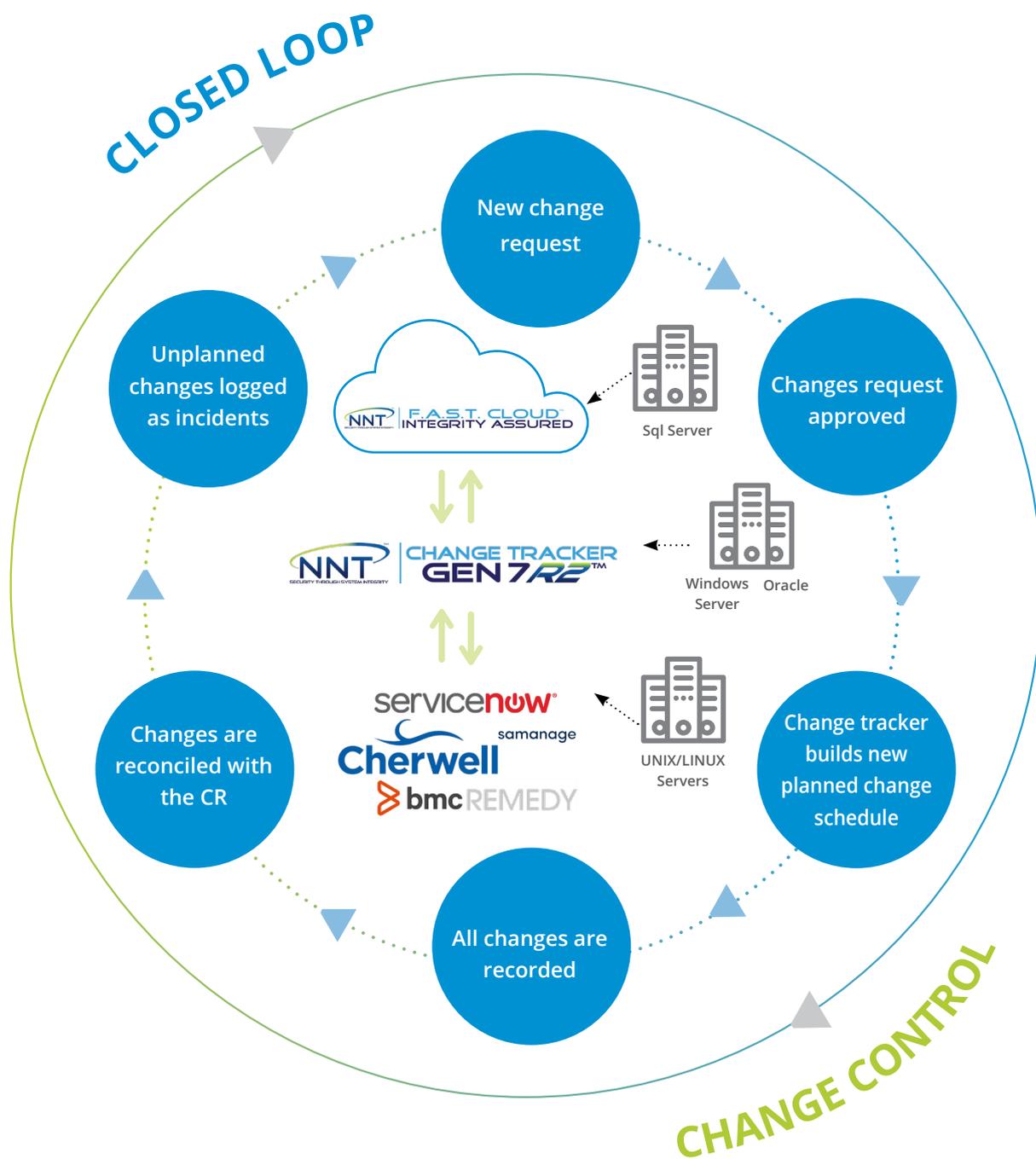
**One is that changes to configuration settings** – be it installation of software, new ports being opened and any change to system and configuration files – may adversely affect the attack surface of a system. The more functionality a system has enabled, the more opportunity there is for misuse or abuse, and it's the route of all exploitable vulnerabilities.

**The second reason is simple in that, if you don't know when safe, legitimate changes are being made, how would you ever know that a system had been breached?**

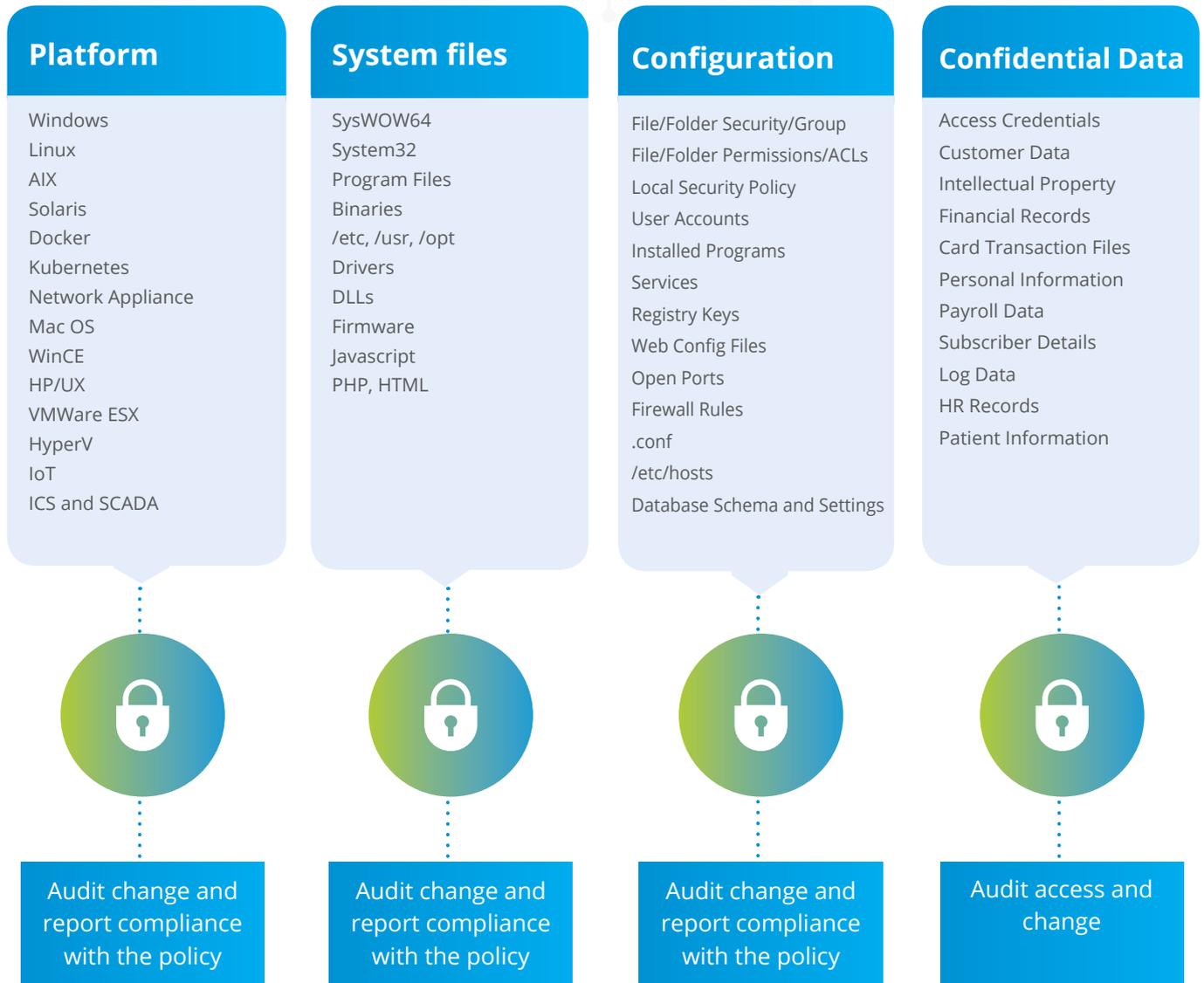
One innovative way to distinguish between good changes and bad changes is to correlate observed changes with the Planned Change schedule. If there are changes planned and approved in the ITSM system then this can be leveraged as a factor in determining that changes are expected.

In the very best Change Control solutions, this is taken to an even further level in that the Change Manifest – the detailed blueprint of which changes are going to be made – can also be used to validate that changes have been implemented accurately, no more, no less.

If you are looking for the most effective Change Control solution, make sure that ITSM integration and Change Manifests can be used.



# WHAT SHOULD BE MONITORED?



# CHANGE TRACKER FROM NNT – NOT JUST ANY OLD FIM

---

NNT Change Tracker Gen 7 R2 includes context-based File Integrity Monitoring and File Whitelisting to assure all change activity is automatically analyzed and validated.

Complete and certified CIS and DISA STIG configuration hardening ensures all systems remain securely configured at all times. Combined with the most intelligent change control technology, Change Tracker Gen 7 R2 provides unparalleled change noise reduction along with the ultimate reassurance that the changes occurring within your production environment are consistent, safe and as required.

NNT Change Tracker Gen 7 R2 now features NNT's unique 'Mega Hub' technology, which provides a compartmentalized architecture with the ability to grow to millions of devices, delivering unrivalled scalability and reliability like no other FIM solution in the market.



# PLATFORMS / DEVICES / CONTAINERS COVERED

---

- Windows, all versions including Server 2019, 2016 and Windows 10, XP, 2003/R2, Windows 7, Windows 8/8.1, 2008R2, 2012/R2 (Core and GUI), Win CE
- Linux, all versions, including Ubuntu, SUSE, CentOS, RedHat, Debian, Oracle, FreeBSD and Apple MAC OS
- Unix, all versions including Solaris, HPUNIX, AIX, Tandem Non-Stop
- Virtualization and Container Servers, all versions including ESXi, Docker and Kubernetes
- Database Systems, including Oracle, SQL Server, DB2, PostgreSQL, My SQL
- Network Devices and Appliances, all types and manufacturers, including routers, switches and firewalls, from Cisco, Nortel, Palo Alto, Juniper, Fortinet and Checkpoint

# CONFIGURATION SETTINGS AND ATTRIBUTES

---

- Files, file contents, file attributes and folder structures
- File secure hash value, to give a unique DNA Fingerprint for each file, essential to detect Trojan malware
- Choice of Hash Algorithm, SHA256, SHA384, SHA512 (and SHA1 and MD5)
- Running processes (checked against blacklists and whitelists)
- Windows registry keys and values
- Installed applications and patches
- Local and domain user accounts
- Services' start-up and running states
- Windows audit and security policy settings
- Configuration settings for audit and security policy
- Command line process output, for example a netstat query
- Open network ports, both UDP and TCP scanned externally on a scheduled basis
- Enforces CIS Benchmark Checklists for vulnerability mitigation
- Username and Process used to make file changes
- Include/Exclude file and path match filters, with wildcards and regular expression matches, plus controllable recursion depth
- Include/Exclude registry hive and value match filters, with wildcards and regular expression matches, plus controllable recursion depth

# CHANGE TRACKER MANAGEMENT CONSOLE

---

- Powerful REST API for full integration with 3rd Party applications, all Change Tracker UX operations can be driven externally via API
- Fully customizable Dashboard, with choice of widgets and multiple tabs for alternative Dashboard layouts
- 'Single-Page Application' design gives a contemporary, super-responsive Change Tracker experience
- Wizard Guides, guided setup for common admin operations
- Universal Query/Report controls, consistently available, enables reports to be built 'off the page'
- Reports Center – build and schedule any reports, with graphically-rich content, including all new Executive Report showing overall security of your estate
- 'Expert Event Analysis' sections for reports, with events automatically pre-analyzed to show 'noisiest' devices, paths, registry settings and any other monitored configuration attributes to aid decision making in your Change Control Program
- Report production now performance optimized, even large volume event reports are generated on a streamed basis to minimize impact on Hub server resources
- Report properties can be tailored – include a hyperlinked Table of Contents, Event Details table and Query Parameters, together with as many/few event attributes as required
- Group & Device/Date & Time filter and selection control panel, selections persist for any page accessed, panel can be hidden when not in use to give a 'full screen' display of the Dashboard

- User-defined auto-refresh settings for all pages
- Device page with condensed Event Stream and Configuration panels facilitate a comprehensive 'at a glance' overview of all Device information
- Planned Change page with full range of filters to provide clear access to your planned changes, overlaid with new Query/Report controls to provide direct access to Planned Change event reports
- Componentized Planned Changes, allowing easy re-use of schedules and/or rulesets, driven by a new Planned Change Wizard for easy, guided schedule and rule set-up
- 'FAST list' planned change rule option, ensures only file changes you select as permitted, allows a user-defined list of approved file changes to be operated – like a personal FAST Cloud!
- Full updated new web controls for improved user experience

## SECUREOPS™ FEATURE SET

---

- Unique to NNT and the world's most powerful Change Noise Reduction technology, F.A.S.T. Cloud provides a comprehensive File Whitelist, comprising over 9 BILLION file reputation scores to provide a clear 'Is this file know-safe or otherwise?'
- ITSM Integration, synchronizes Planned Change RFCs from ServiceNow, Cherwell, Remedy and any other leading ITSM systems, ensures changes detected are reconciled with Planned Change schedules to isolate unplanned, unexpected change

## CONCLUSION

---

NNT's Change Tracker Gen 7 R2 is simply recognized as the most effective and feature-rich FIM solution on the market today since it is the only solution that combines inbuilt self-learning intelligence to determine the validity of activity with the world's largest file whitelisting service. The authenticity of activity combined with the ability to hook into your current change management process, harvesting vital detail associated with expected changes is what sets Change Tracker Gen 7 R2 apart from alternative products.

The result is a precision system that will sift through the mass of legitimate file changes and only alert you to those that may be potentially harmful. NNT puts the 'I' back in FIM.

"NNT's Change Tracker product architecture, the rich feature set and ability to implement the closed-loop change cycle has been very effective in securing our IT operations. Rather than use a lot of different security tools to perform the functions we need, we use Change Tracker. Overall, we're very pleased with how Change Tracker supports our digital transformation goals while protecting our clients' data and assets from the latest cyber threats."



David Smithers  
CIO, IDB Bank