The World's Leading SecureOps™ Solution - Rendered as a Service

Every change should be verified in line with the true intent of Change Control. Configuration drift or decay not only causes service delivery problems but may also increase an organization's attack surface. Furthermore, if changes are not controlled – analyzed, validated and approved - then breach activity, such as 'Zero Day Attacks', can simply hide in plain sight, with no means of detection.

NNT's SecureOps™-as-a-Service coupled with Change Tracker delivers peace of mind, compliance, security and operational control. By tying systems and business processes together to evolve data and events to actionable intelligence, the NNT SecureOps service option enables firms to mature and maintain cyber resilience, improving security operation's effectiveness from the average 60% to above 90%.

Best Practices of Change Control included:

- Secure Baseline, Vulnerability Analysis & Configuration Hardening
- Reduction of Change Noise
- NNT Intelligent Planned Change Operation
- NNT FAST Cloud
- NNT ITSM Integration
- Change Management Discipline

"Regardless of how much data an organization collects, it is always the decisions that the data empowers you to make that counts, SecureOps™-as-a-Service eases the burden of Change Control to ensure that data can always be properly protected and brought to a compliant state."

Mark Kerrison, GM of NNT

Stage 1

In Stage 1, the service will help an organization to understand the largely unpredictable element of change noise and prepare its change control best practice approach accordingly, and this stage will enable you to run change control as an efficient operation.

Stage 2

Stage 2 introduces the invaluable component of a Change Control strategy, the closed-loop, intelligent control of all changes and its innate power to automatically analyze and evaluate that activity. This stage ensures changes are validated as being implemented accurately, and only as approved.

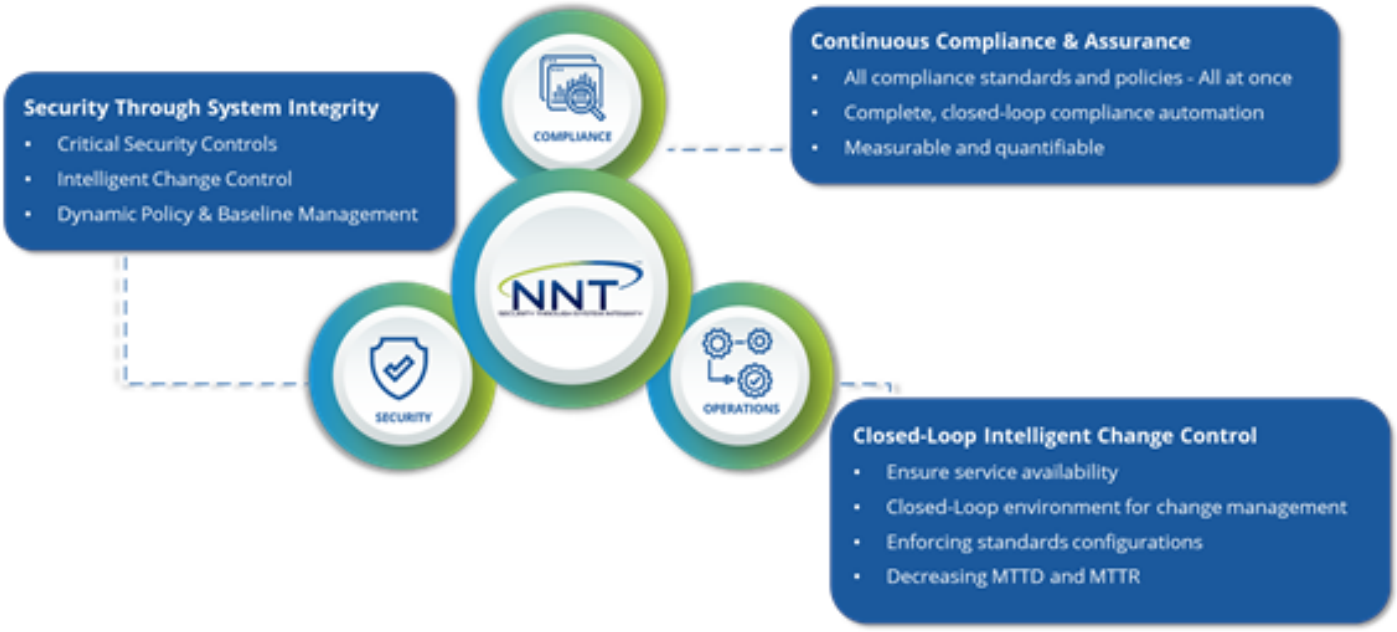
YOUR MONITORING REQUIREMENTS AND CHANGE NOISE

Change noise is just another term for change activity – the more configuration elements you monitor, the greater the level of change activity you will have reported. System and File integrity monitoring is most beneficial when applied to elements that should not change regularly – no changes, everything is as it should be.

After deployment of Change Tracker, the system will start to receive change events. Seeing zero changes unless there is an associated 'Planned Change Record'. Change Control means that change is controlled – it happens when expected, in the way it is required and is verified and validated.

This would include system and application program files and key configuration settings, especially those settings that harden security, but can be extended to any other dimension of configuration, including the installed software and patches, open network ports, processes and services and the entire filesystem and registry.

NNT Monitoring Policies allow fine-grain targeting of monitoring to specify precisely what and how changes are monitored, allowing you to cut-out changes you don't want to be alerted to and to highlight changes that really matter.



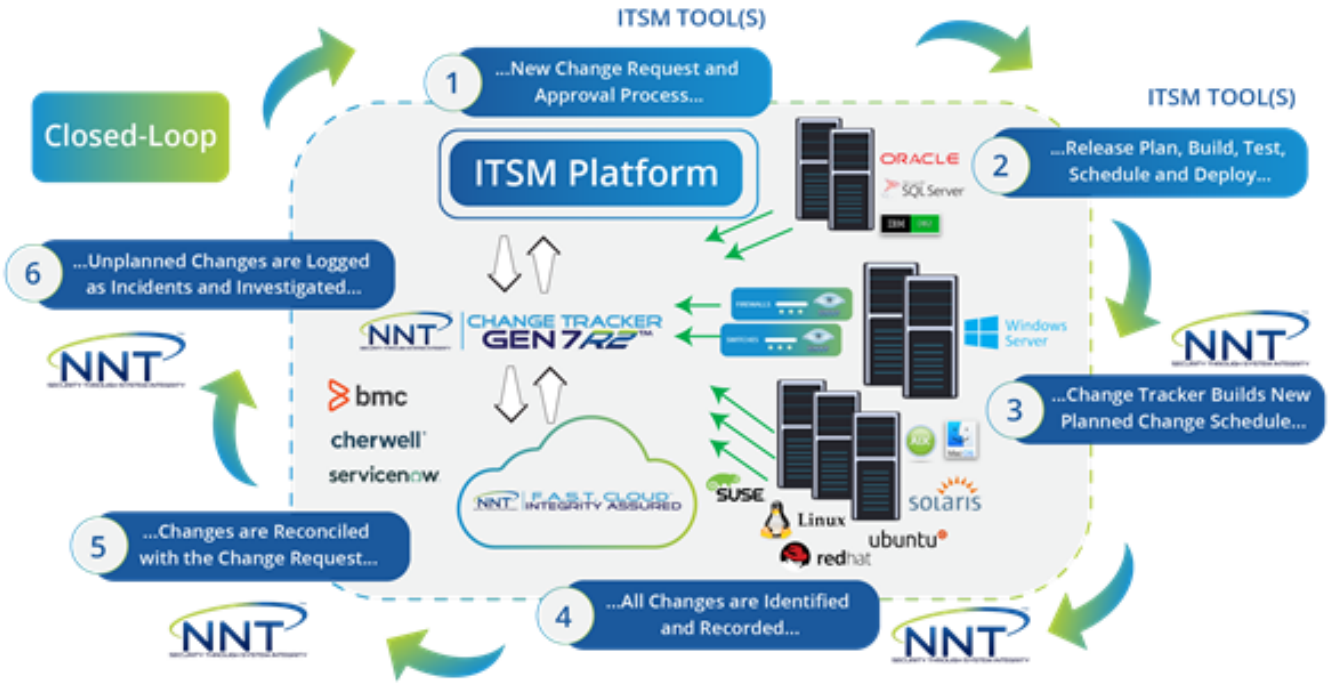
In order to reduce or eradicate any changes occurring that cannot be associated with a 'Forward Schedule of Changes', Stage 1 helps you to build in as much process as possible, which is to say develop a Change Tracker integrated process that sees no changes happen without a related preemptive planned change.

During this build phase, especially when Change Tracker is installed first time, it is usual to see some unexpected change events that fall outside of any anticipated change activity and is linked to the normal cycle of systems and applications.

SecureOps-as-a-Service, in Stage 1 is designed to support and guide you during this ramp-up.

CLOSED-LOOP, INTELLIGENT CHANGE CONTROL

Once the base is established, the core component of a NNT's Change Control strategy, close-loop, intelligent change control, will automatically analyze and evaluate any change activity. It ensures that changes are validated as being implemented accurately, and only as approved. This provides a guarantee on service delivery quality and consistency while maintaining secure configuration standards at all times, and also better isolates unplanned, unexpected and unwanted changes to act as a sensitive breach detection control.



The **Four Dimensions** to Change Tracker's Intelligent Change Control are:

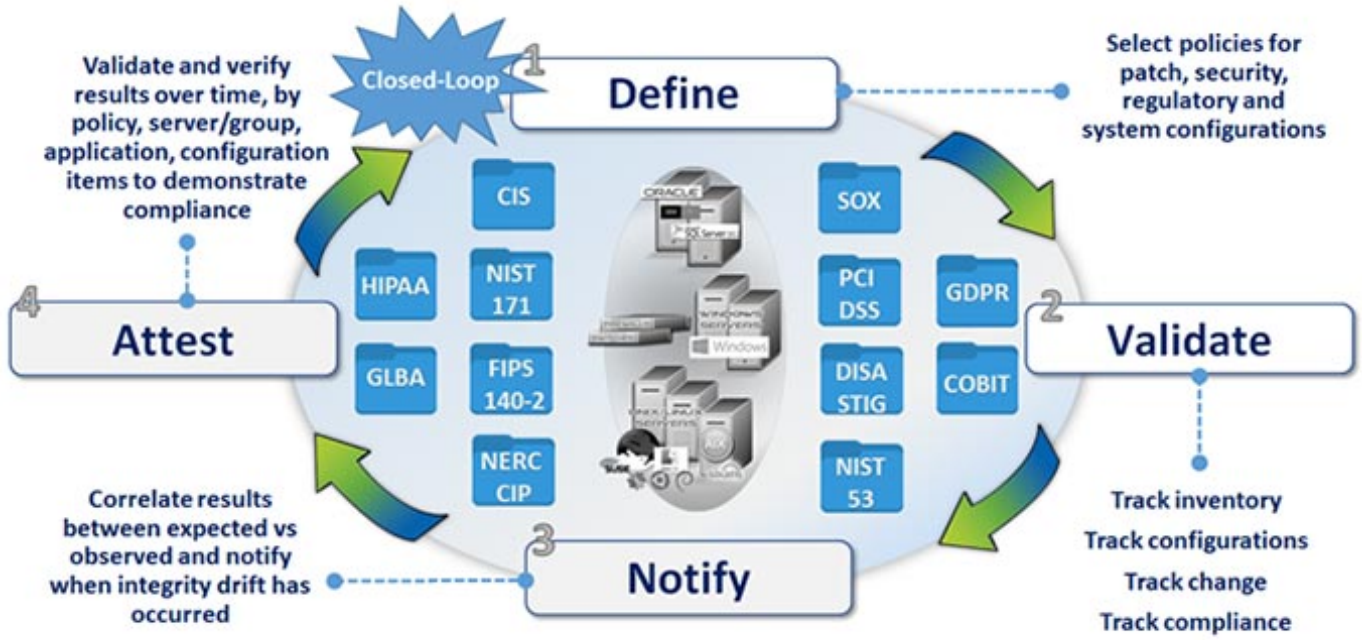
- **FAST Cloud Correlation:** Do all file changes have a confirmed 'good/safe' reputation score?
- **Change Manifest Correlation:** Are changes detected in line with approved system changes known to occur when the change is implemented?
- **Maintenance Window Correlation:** Are changes approved for these devices during this time period?
- **Pre-defined Rules Correlation:** Do changes meet pre-defined rules such as previously seen and accepted change or changes made under certain criteria such as approved users or change profile detail?

SecureOps-as-a-Service, in Stage 2, is maintaining and further improving your achieved Change Control posture, helps you to pro-actively manage any drift occuring. New or altered Compliance requiremens can be introduced with ease.

Of course, all this is part of NNT's SecureOps-as-a-Service, allowing you to delegate the set-up and operation of Closed-Loop, intelligent Change Control to NNT.

CONTINUOUS COMPLIANCE & ASSURANCE

Your additional benefit of SecureOps-as-a-Service: Continuous Compliance and Assurance achieved!
With Change Control implemented as an ongoing process of proactive risk management delivering predictable, transparent, and cost-effective results, your organisation will meet information security goals, maintain compliance and is assured that this status is monitored and maintained at all times.



US - (844) 898-8362,
UK - 01582 287310
info@nntws.com
www.newnettechnologies.com

Schedule a free consultation

Request a Demo