ServiceNow & NNT Integration Solution Brief

MANAGING BY FACT NOT FICTION

> The industry average for Mean-Time-To-Detect (MTTD) for both expected and unexpected changes is 190 days.

NNT's Change Tracker Gen7 MTTD is measured in seconds.

> 80% of unplanned outages are due to the lack of change management process and controls.

NNT can enable and enforce a closed-loop intelligent change management process.

> 91% of all security breaches can be auto-detected when release, change and configuration management controls are implemented.

NNT's SecureOps approach incorporates a best practices methodology to achieve the desired results.

How can you accurately ensure that intended changes were delivered as requested and approved?

NNT's Closed-Loop Intelligent Change Control

NNT has integrated its award-winning Change Tracker ™ Gen7 with ServiceNow's leading service management framework to enable a closed-loop environment for change management. Approved and authorized changes issued by ServiceNow can be validated by NNT Change Tracker Gen7, with a full audit trail of what actually changed and reconciled with the Change Request(s).

By leveraging NNT's Closed Loop Intelligent Change Control Technology, repeated or recurring change patterns can be captured and identified as either harmless or potentially harmful as well, discriminating pre-approved changes from unexpected and unwanted changes. Pre-approved changes may also be forensically profiled ahead of time in order to spot any deviations that may indicate 'insider threats'. This approach drastically improves the ability to spot potential breaches by reducing the "change noise" and exposing insider and zero-day malware activity. This approach also helps enable SecureOps.

SecureOps

SecureOps is NNT's approach to addressing issues and problems that are applicable and common to both security and IT operations. It is also, where specific controls overlap to support the defined business objectives from two different perspectives of security and operations, which in itself has a unifying best practice effect on both disciplines.

This common perspective encompasses foundational requirements and includes visibility and knowledge of:

> A clear understanding of what you have
> Making sure what you have is fit for purpose
> Monitoring changes to prevent integrity drift from known and trusted states
> Incorporating a best practices approach to managing changes

Human Factor

Human error has long since been held as the biggest source of unplanned downtime – mistakes are made and systems end-up misconfigured, not just affecting service delivery, but also leaving the organization more susceptible to various attack vulnerabilities. With an emphasis on the approval and review process prior to changes being made, unwanted changes can be exposed for remediation and integrity of IT systems reinstated.

Transform your Change Control Capabilities with our ServiceNow Integration

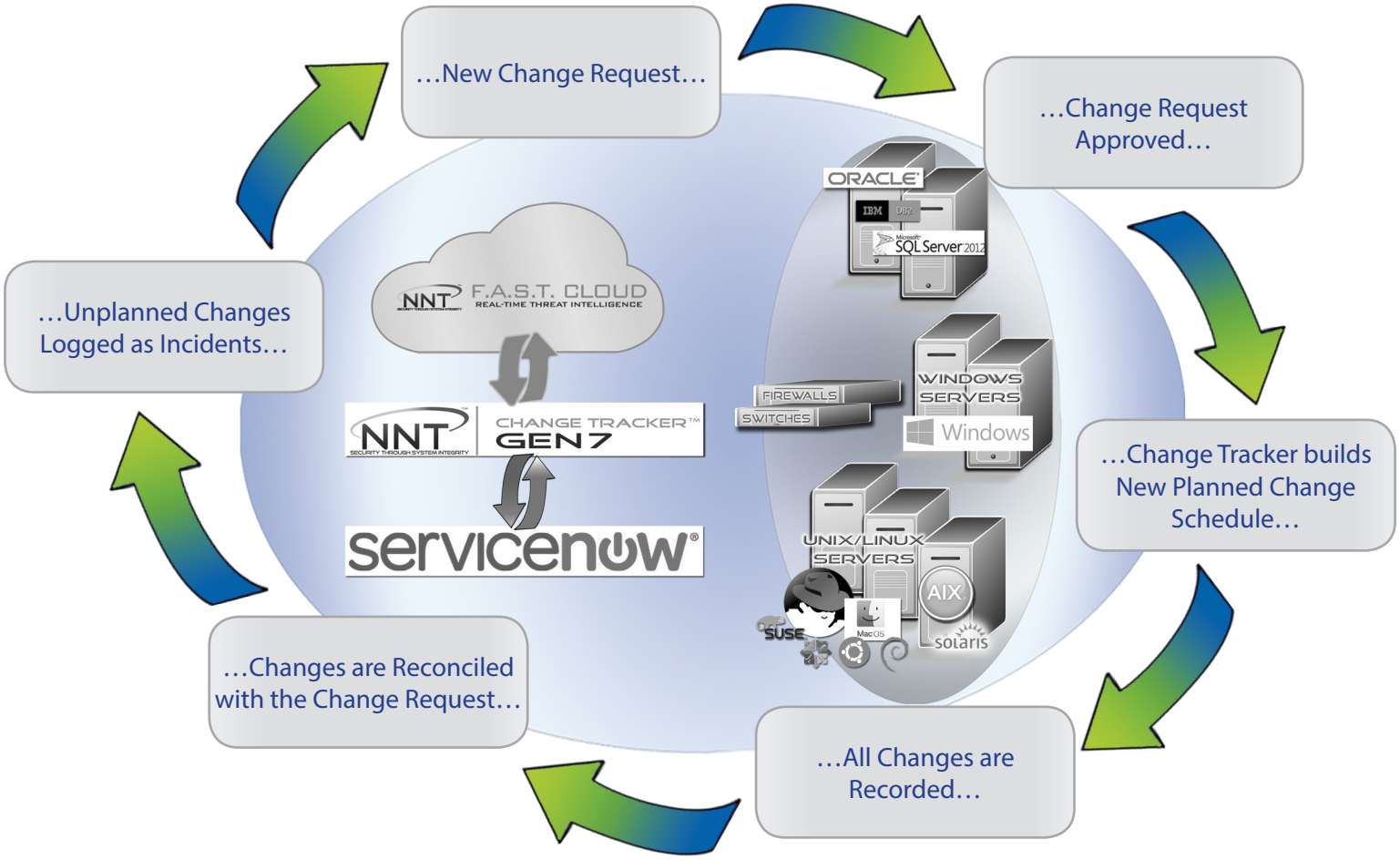
> Automatically validate approved changes with a full audit trail of what actually changed provided.

> Isolate pre-approved changes from unexpected and genuinely suspicious changes by re-using recurring change patterns.

> Significantly reduce overwhelming change noise to clearly expose insider and zero-day malware activity.

ServiceNow & NNT Integration Solution Brief

What does a closed-loop intelligent change control process look like?



Change Tracker™ puts a spotlight on all changes made. Changes made during a prescribed planned change window get validated against the expected change profile - any exceptions, such as misconfigurations or additional non-scoped changes are exposed for review and remediation where required. All unplanned changes are also recorded in full – Who made the change, with before and after exposure of changes clearly reported. These are prioritized as ServiceNow incidents where the unknown or unwanted changes will be automatically analyzed using NNT's white-list cloud service called F.A.S.T. Cloud.

In reality, in a well-run secure IT environment, most unplanned changes will be emergency changes or unexpected changes such as automatic software updates. They may not be dangerous changes or malicious activity, but as non-approved changes, they must be reviewed. The beauty of this approach is that it ensures that any suspicious and potentially dangerous unexpected changes are clearly highlighted and categorized as critical.

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.

W: www.newnettechnologies.com E: info@nntws.com