DeveloperDays
Network Services Orchestrator

Network Security and Automated Healing

Using NSO Compliance Service Pack

Giri Venugopal
Eswaramoorthy Ramasamy
24-June-2020

Agenda

1. The Problem Statement
2. Network Security – Current trend
3. Real time Threats
4. Pillars of Network Security
5. Automated Healing using NSO
6. Demo
7. FAQ’s

Problem Statement

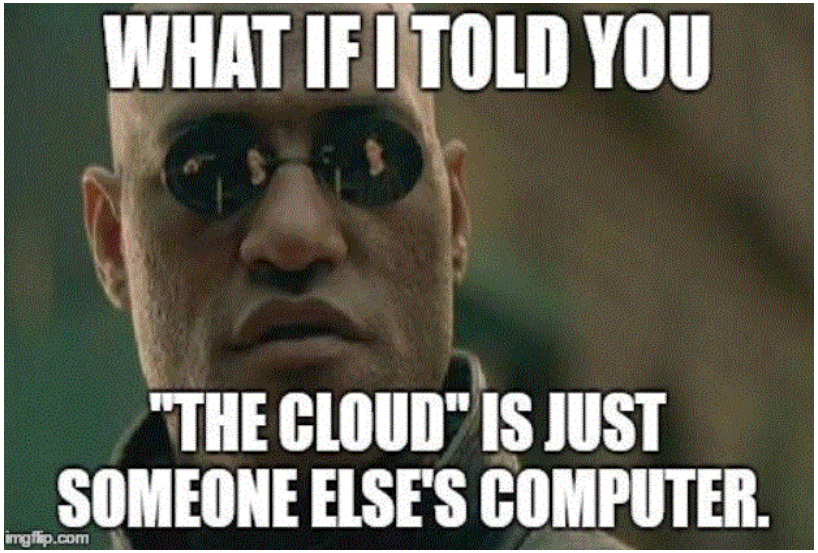
What are we trying to solve???

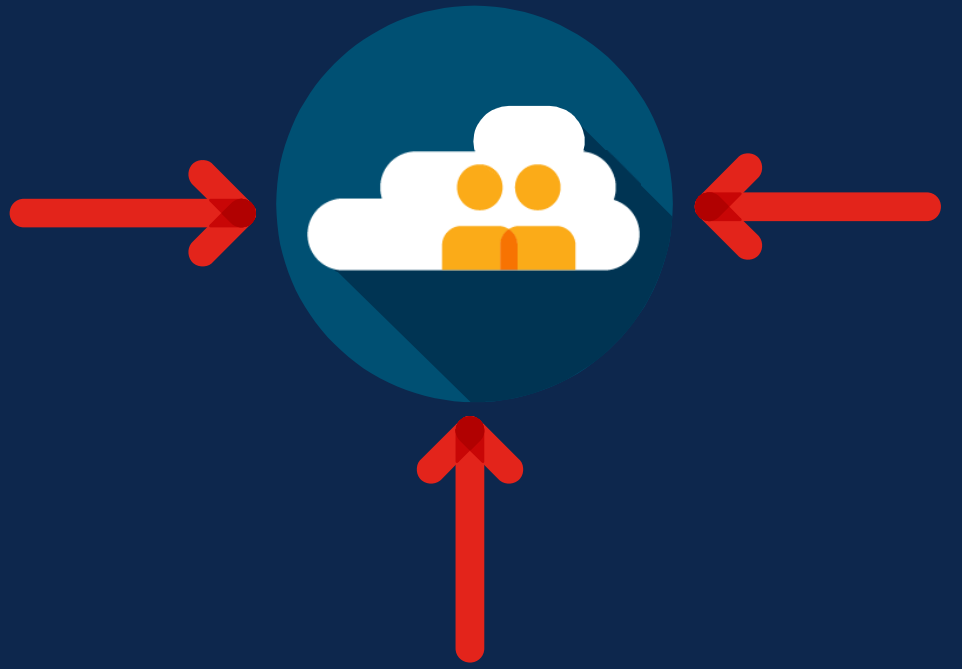
Mitigate unauthorized access of data

- Data is distributed everywhere
- Need for data protection is now more than ever
- Cloud providers offer certain level of security
- New encryption techniques are always neutralized by new vulnerabilities
- Data is always at risk
- The term "*100% secure*" is always an understatement

What we think about Cloud data security…

But the reality is…





So the truth is…

- Automation comes at a price
- Data Security – becoming a liability as cloud providers are becoming more vulnerable
- With rapidly evolving technologies, security always has to keep up.
- Along with technology, security threats are also evolving
- Data is never *“100% secure”*

It all starts with the network…

- Intrusions can come from external sources or from within (can be unintentional)
- Hackers & Network attackers prey on *Human sentiments & weaknesses*
- Techniques like *Phishing* are evolving to steal credentials & pose as legitimate users to hack into the network.
- Reports show about **30%** of phishing emails are opened by employees and **15%** of targets go on to click the link or open the attachment.
- Multi-level firewall framework & robust FW policies can help mitigate external breaches .

Real time Threats & Vulnerabilities

Common threats & vulnerabilities

- Non-compliant Device configurations
- Human Error
- Firewall / Policy changes that are not reverted back
- Phishing
- Distributed Denial of service (DDoS)
- Botnets
- Cryptojacking (crypto-currency)
- SQL-Injection / Cross-site scripting (XSS)
- Reversal of elevated access

What can we do to secure the network?

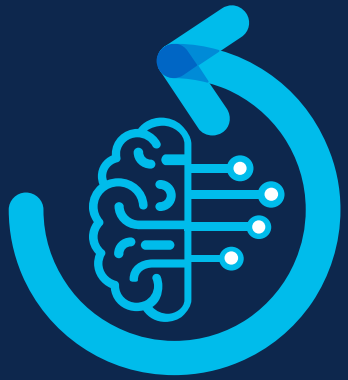
- Tightening Network Security is key to preventing potential data breaches.
- No foolproof solution that can provide100% guarantee against attacks

Best practices & mitigation techniques:

- Using Multi-level Firewall policies & ACL rules for different levels (App, DB, etc)
- Staying on top of security patches & Software updates
- Enforce setting strong password policies
- Running Compliance checks periodically
- Enforce Multifactor-Authentication (MFA)
- Regularly running Penetration Tests

Pillars of Network Security

- **Protection**: Configure networks as securely as possible
- **Detection**: Identify when the configuration has changed or when there is a problem
- **Reaction:** In case of a problem, detect early, respond quickly and return to safety as soon as possible

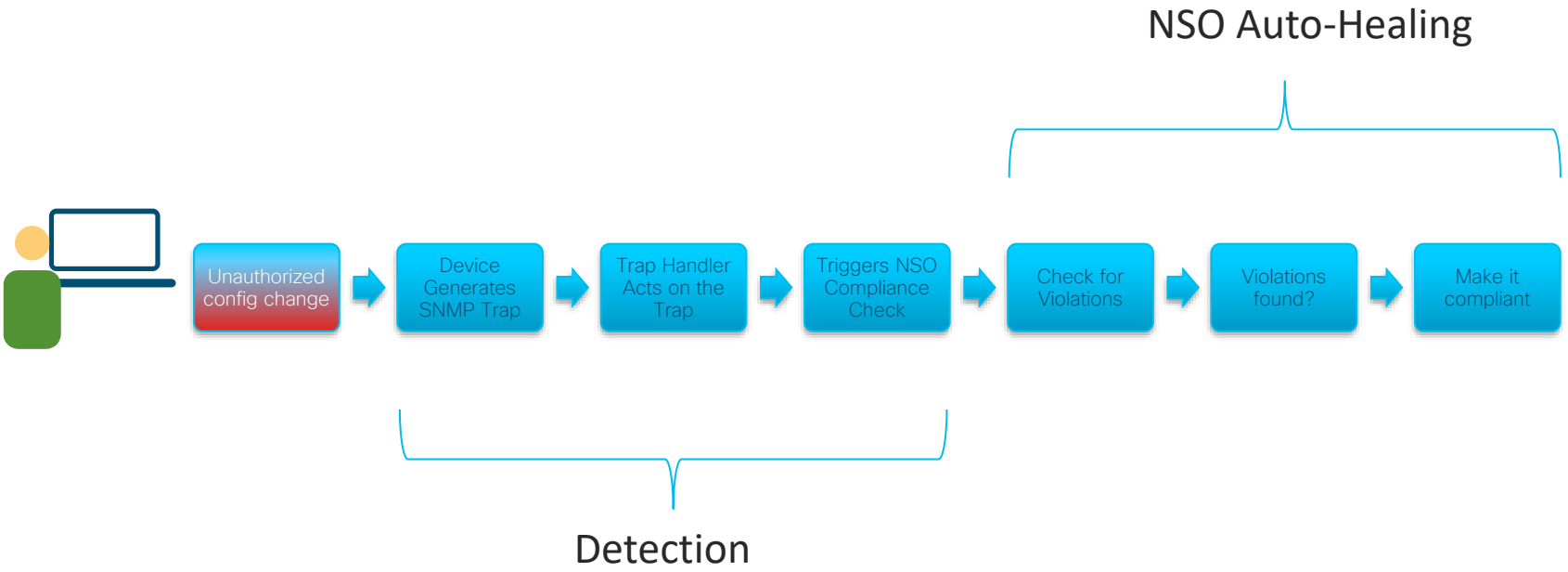


Automated Healing using NSO

What are we doing?

1. Monitor device for un-authorized config changes or tampering
2. Generate SNMP traps and invoke Trap-handler
3. Trap-handler will invoke Config Compliance Service Pack
4. On-Demand Configuration Audit to check config-compliance
5. Make devices compliant with/without Admin approval
6. Config Diff Report with Pre/Post Checks

Automated healing: *High-level Use case overview*



Solution Components

- Network Services Orchestrator
- Compliance Service Pack
- SNMPTRAPD – Trap Listener & Handler
- OSS/BSS(BPA)
- Network Devices – Configured to send traps on config change

Demo–Auto healing networks

Auto Healing

No Human Intervention

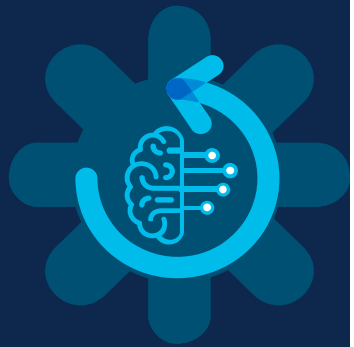
NSO

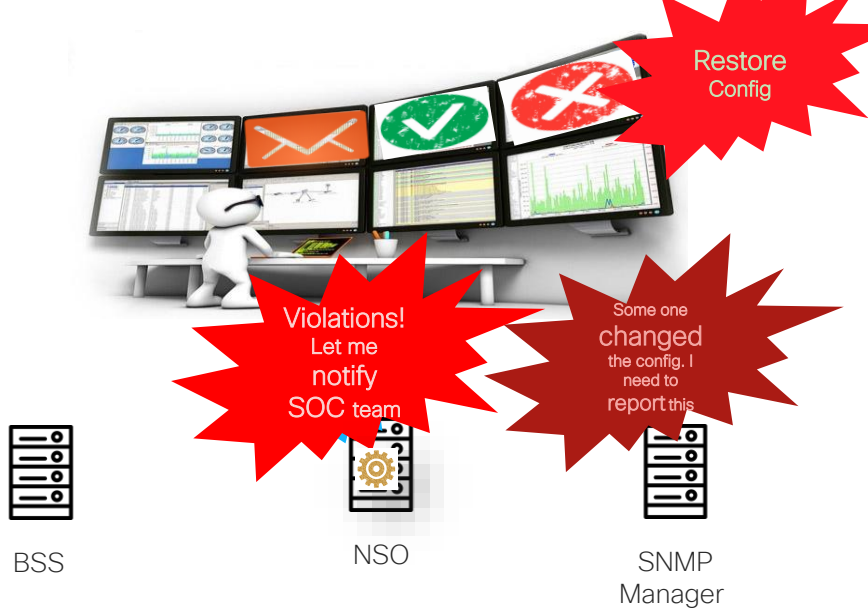
SNMP
Manager

Demo – Guided healing networks

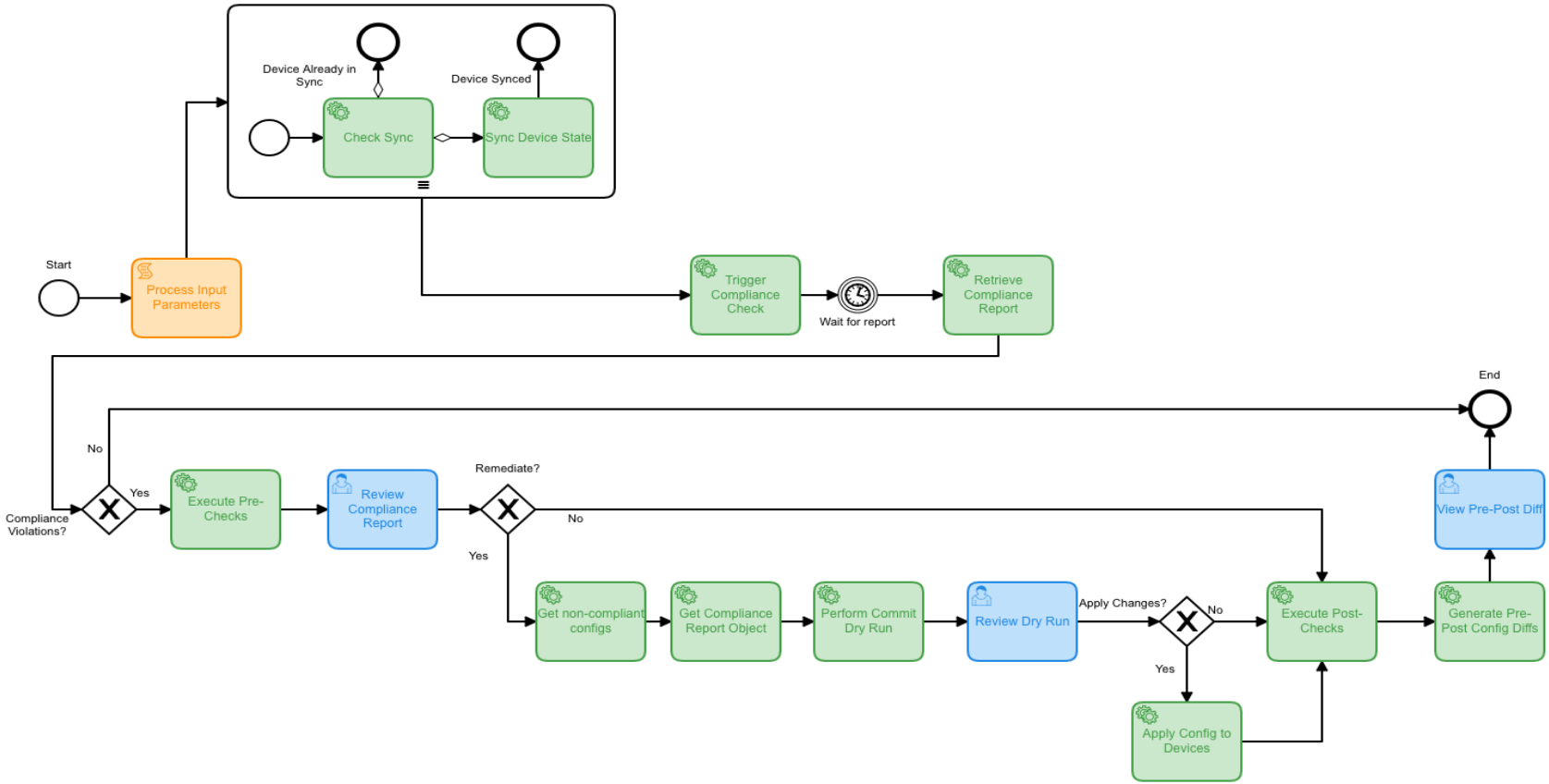
Guided Healing

With Human Guidance(Review & Approval)





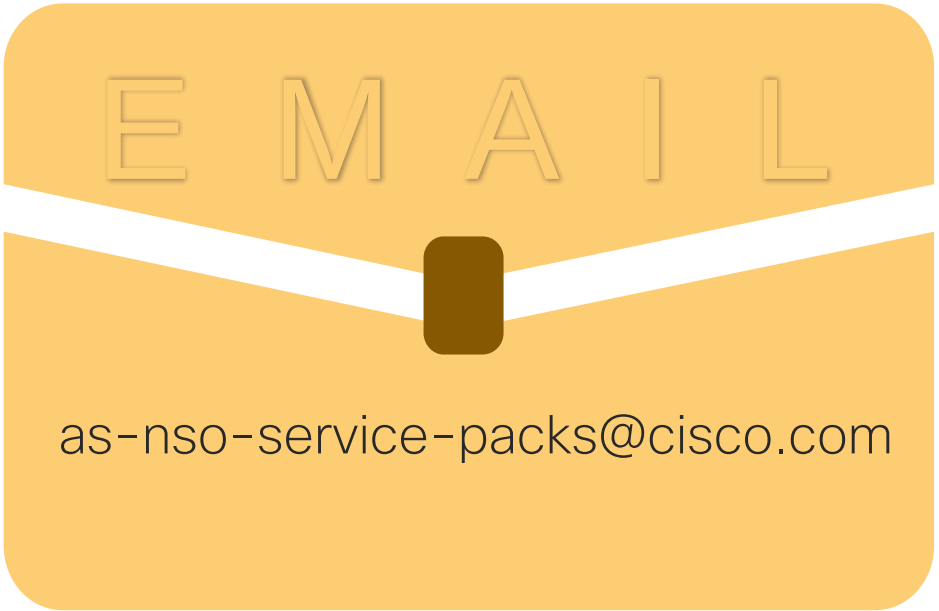
Guided-healing: High-level Workflow



FAQs

- How can we trigger compliance check when the device is configured for multiple trap types?
  - Trap Handler can be configured to call the compliance check only for config change traps
- When an undesired change on device triggers a trap, NSO pushes configs to make it compliant, which in turn triggers config change traps. Isn't this a Deadlock ?
  - No, compliance package first checks if there are any violations. Only if there is/are violation(s), the templates are applied
- Configuring a new feature which has 10-20 lines of config. It will trigger 10-20 traps for each configuration change. What will happen now ?
  - Though compliance check will be triggered for each trap and templates will be applied only in case of violations, it is recommended to incorporate co-relations feature in the net-snmp trap handler or any SNMP-Manager
- How to stop Auto Remediation/Healing for a device when change are intentional?(e.g. During a maintenance window)
  - Maintain a device list within trap handler which needs to be ignored from performing a compliance check. This list can be coming from Change management systems/ Inventory etc.

- Have more questions?
- Want to know more ?



Got Feedback?

http://cs.co/autoheal


CISCO