Guardian

Configuration Drift in On-Premise Environments

Why Change Management, Configuration Management, and Drift Management Still Matter

Executive Summary

On-premise infrastructures remain the backbone of many enterprises, delivering control and predictability. Yet even in these environments, configuration drift poses a silent risk. When systems deviate from their approved state, security, compliance, and operational stability are compromised. While traditional infrastructures have long relied on rigorous **change management**, many organisations underestimate the need for **continuous drift detection** and governance. This paper explores why configuration and **drift management** in on-premise environments is essential, the challenges introduced by scale and complexity, and how automation and governance can restore order.

Introduction

On-premise IT environments promise stability and control. In reality, they often deliver complexity at the cost of agility. Unlike cloud platforms, these environments are static—but they are not immune to drift. In Barclays CIO Survey 2025 **86% of CIOs** said they were going to repatriate workloads from the cloud to on-prem and with IDC (Dec 2024 survey) finding that **48% of companies** using cloud are looking to bring workloads back, the on-premise IT vs cloud game is far from won. Manual interventions, emergency fixes, and inconsistent processes create deviations from the 'golden configuration.' Industry research underscores the urgency: despite mature ITIL-based processes, **70% of outages** in traditional environments stem from **configuration errors** (Uptime Institute, 2023). Without robust configuration and drift management, organisations risk turning their data centers into opaque, ungovernable estates—where compliance gaps, security vulnerabilities, and operational instability thrive.

The Problem: Drift and Its Consequences

Configuration Drift in on-premise environments often stems from gaps in process and governance. Manual changes during incident response or urgent fixes frequently bypass formal approval workflows, introducing inconsistencies. Out-of-policy changes, those not submitted through the **Change Management process**—compound the problem, creating blind spots for IT teams. Legacy automation scripts and conflicting tooling add another layer of complexity, making it difficult to maintain a single source of truth.

The Hidden Consequences

The impact of drift extends far beyond technical inconvenience. Misconfigured permissions or unpatched systems expose organisations to security breaches, while undocumented changes create compliance gaps that can lead to regulatory penalties. Operational stability suffers too—industry data shows that **70%** of network failures originate from configuration errors (Uptime Institute, 2023). These failures translate into financial losses, whether through downtime costs or inefficient resource utilisation caused by misaligned configurations.

Why It Matters Now

As hybrid adoption accelerates, the risk of drift is magnified across diverse environments. Without proactive detection and governance, organisations risk turning their estates into opaque, unmanageable infrastructures—where vulnerabilities thrive and compliance becomes a moving target.

Why Change Management Still Matters

Some argue that mature ITIL processes make drift management redundant. The truth? They make it more critical. Every change—whether updating firewall rules or modifying storage configurations—carries risk. ITIL principles remain relevant, but they must evolve. In on-premise environments, change enablement means automated, policy-driven governance that minimizes human error while enforcing compliance at speed.

The Solution: Governance and Automation

To tame the chaos, organisations need three pillars:

Infrastructure as Code (IaC):
Treat configurations as version-controlled artifacts. Even in on-premise environments, IaC ensures a single source of truth and reproducibility.

Continuous Drift Detection:
Tools like **Guardian by Cloudhouse** provide visibility into deviations from the 'golden build.' Integration with ITSM platforms ensures remediation aligns with governance. .

Adaptive and progressive Change Management/Enablement:
Policies and processes that support agility without sacrificing compliance.

ITSM Integrations

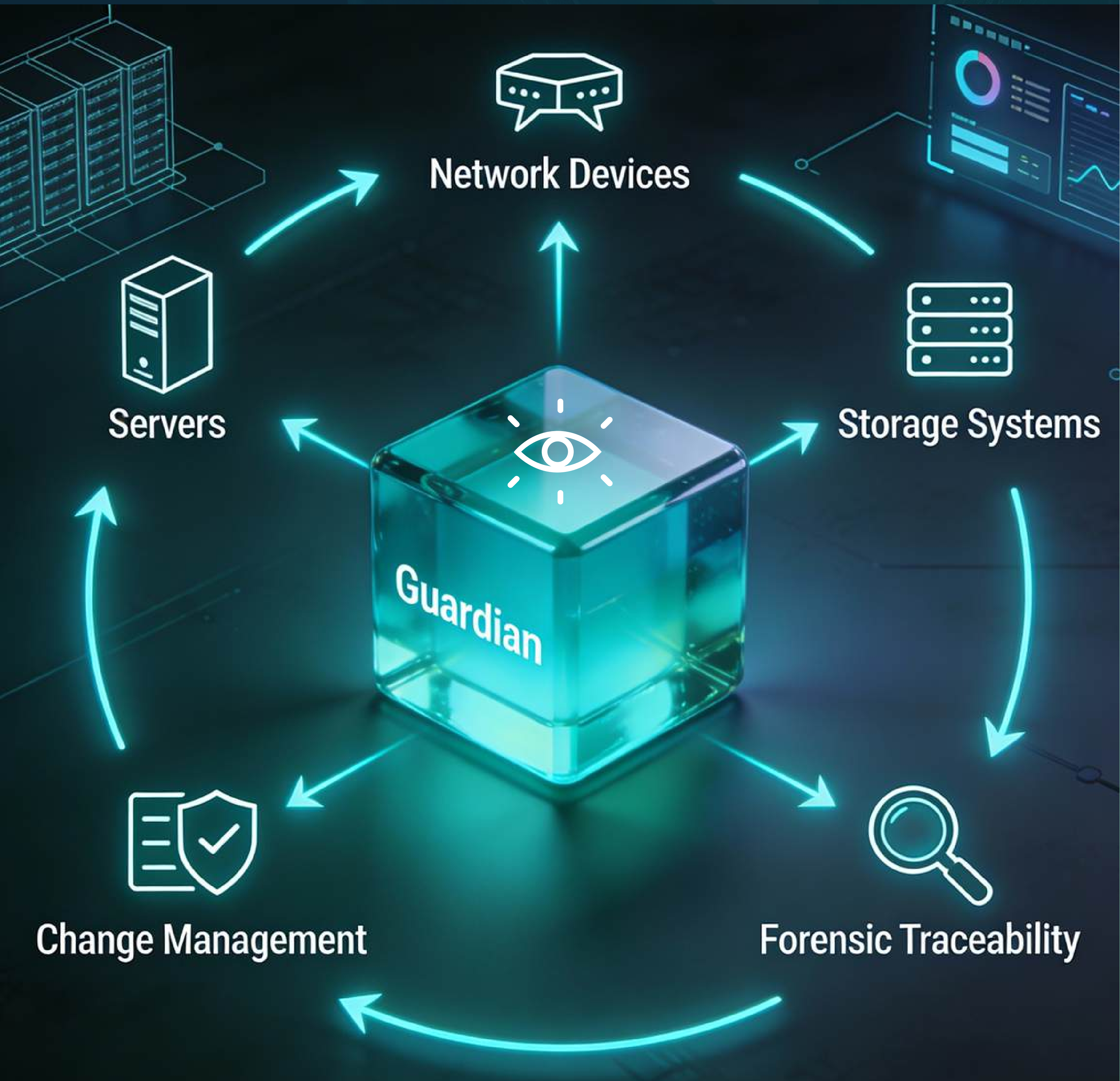
servicenow freshservice bmc ivanti

Tool Comparison:
Which Approach Fits Your Estate?

Capability	Guardian	Microsoft Desired State Cofiguration (DSC)	Ansible
Primary Purpose	Unified drift management across hybrid/on-prem	Desired State Configuration for Windows	Configuration automation
Resource Inventory	Interrogates servers and network devices	Windows nodes	Linux/Unix nodes
Configuration History	Full forensic traceability	Partial via logs	Version-controlled playbooks
Compliance Evaluation	Continuous drift detection	Checks against DSC configs	Detects drift vs desired state
Remediation	Auto Change Reconciliation	Apply DSC configs	Apply playbooks
Integration	ServiceNow, FrehService, Ivanti, BMC	Windows Admin Center	CI/CD pipelines
Reporting	Unified dashboard	Basic reporting	CLI/third-party dashboards

How does Guardian by Cloudhouse help?

Guardian provides insight into your on-premise estate, enabling Change Management and governance without adding complexity. It interrogates servers, network devices, and storage systems to ensure all elements are accounted for, then adds them into its management framework for detailed monitoring and forensic traceability. Guardian reconciles changes against approved processes, highlighting unauthorized modifications and failed deployments. Operating at scale, it brings transparency and control to environments that have historically been opaque.



Benefits of Doing It Right

- Security hardening by eliminating misconfigurations.
- Regulatory compliance through continuous enforcement.
- Operational resilience by reducing outages linked to undocumented changes.
- Cost optimisation by preventing resource sprawl.

Conclusion

On-premise environments are not immune to configuration drift. The principles of change enablement that safeguarded traditional infrastructures remain indispensable. By combining governance, automation, and proactive monitoring, IT leaders can transform operations from chaos to control, ensuring security, compliance, and operational excellence.

References
Uptime Institute (2023). Network Outage Analysis.
ITIL Foundation (2024). Best Practices for Change Management.
Cloudhouse (2024). Drift Management Tools Documentation.