CYBERSECURITY
CENTER *of* EXCELLENCE
A joint initiative of DSCI & Government of Telangana

CLOUD RAXAK
CLOUD SECURITY COMPLIANCE

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

GOVERNMENT OF TELANGANA

Proactive Security Configuration Management:

THE KEY TO CYBERSECURITY

WHITE PAPER 2019

CONTENT

01

The complexity of managing security configurations in the cloud:

How cloud and Software-Defined Data Center (SDDC) increase the complexity of managing security and how even the most security-conscious customers can face security failures.

02

Reducing security risk while managing DevSecOps:

Why the goals of improving security, reducing the cost of management and enabling enterprise agility through Development, Security, and Operations (DevSecOps) are not conflicting objectives.

03

Comprehensive, Consistent and Continuous Management of Security Configurations:

Why security in cloud and SDDC must be Comprehensive, Consistent and Continuous.

04

Secure-by-design, Deploy-as-designed, Run-as-deployed:

How enterprises can reduce friction in the DevSecOps process by breaking the process of managing security into 3 phases - Design-for-security, Deploy-as-designed, Run-as-designed.

INTRODUCTION

Rapid digitalisation across all facets of the industry right from financial transactions to command and control has shifted computing operations to the cloud. This paradigm shift is enabled by adoption of technology such as smartphones and Internet of Things along with an ever-increasing demand for real-time data. Cloud Architecture allows flexible scaling of infrastructure on a timescale that matches the dynamics of the underlying traffic with change in customer usage and demands. Cloud Architecture also enables rapid development and operational deployment cycles (DevOps) demanded by rapidly evolving needs.

Adoption of cloud-based architectures are increasing awareness regarding the critical need of effective and secure management. The industry needs to adopt effective techniques and procedures that can handle the complexities of moving to the cloud in order to meet the ever-increasing regulatory requirements for privacy and data localization along with the need to protect every company's intellectual property. These technology capabilities must not only be capable of dealing with the stringent demands of the cloud but also be cost-effective to maintain the cost-benefit ratios that allow modern DevOps to be effective.

Recent high-profile breaches have highlighted the importance of one key aspect of security: proactive automated management of security configurations. Moving to cloud and software-defined infrastructures have enabled a tremendous increase in scale, and complex, highly dynamic infrastructures.

Digital transformation & dynamic infrastructure have increased the need to ensure secure configuration. Business as usual (BAU) manual processes no longer work, and application programmers (who are generally not trained security professionals) lack the skills to manage these configurations on their own. As a result, misconfigured IT assets (X-force references) have been identified as the cause behind 4x jumps in breaches in 2018.

Gartner[1] states that although cloud services offer high levels of automation and user self-service, nearly all cloud attacks are the result of customer misconfiguration, mismanagement and mistakes.

Taking these aspects into consideration, the IT community must adopt automated, consistent, comprehensive and continuous configuration management of all security controls as a primary building block of any forward-looking IT architecture.

The four key issues customers face while managing security configurations in the cloud are:

1. Scale: As organisations transform their infrastructure from traditional IT to private clouds, public clouds and now to containerisation, there is a need to securely manage the cloud assets that have increased by up to 4 orders of magnitude. Each individual asset has hundreds of security configurations.

2. Dynamics: In the past, average lifespans of on-prem assets used to average 3 - 5 years. Average lifespans of cloud assets range from a few minutes to a few weeks. Manual processes developed in the on-prem era are too expensive as they cannot be scaled or amortised over large numbers of short-lived assets.

3. Skills: With cloud architecture, the control over servers is devolved to developers from centralized IT teams. When developers lack requisite security expertise, the organisation’s security policy and CISO’s guidelines may not be implemented accurately. This may make the process nimble yet highly vulnerable.

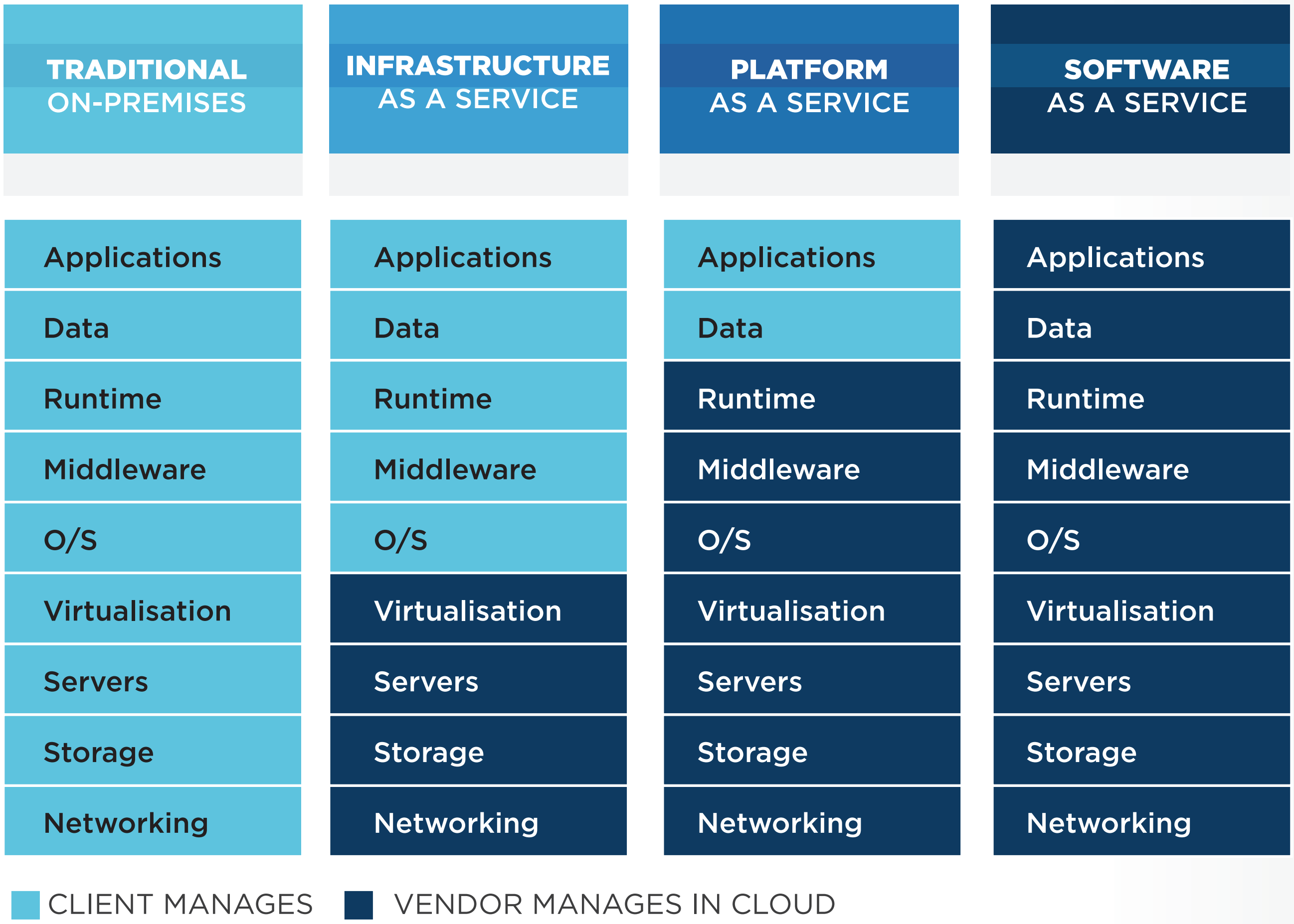
4. Diversity: As cloud usage proliferates, most organisations discover that their IT environment becomes significantly heterogeneous and fragmented. Some assets remain in the traditional on-premise environments; others migrate to different hosted data centres or commercial cloud environments. Each environment has its constraints, operational modes, tools, and APIs that must be mastered to gain a handle on company-wide security.

The complexity of cloud configuration has increased over the past few years as organisations migrate most of their on-prem infrastructure to the cloud. Organisations are also opting for a multi cloud approach to reduce over reliance on a single cloud provider. Infrastructure offered by cloud service providers is also becoming dynamic to meet demands of the businesses which are more end user centric. Companies are opting for a hybrid approach which makes the management of infrastructure a bit more complex. This makes it difficult to define and manage a single configuration across the entire enterprise. With the increase in sophistication of attacks on cloud environment, the number of security measures and protocols have also increased.

01 The complexity of managing security configurations in the cloud

Organisations need to manage a very large number of security configurations with vast security features provided on the cloud. For reasons that we will explore in this section, customers have not been able to keep up with this complexity using BAU processes.

Figure 1 graphically depicts the security configuration management problem in the cloud. In the shared responsibility model[2], the cloud provider manages the cloud, but the customer is responsible for managing their assets within the cloud.



TRADITIONAL ON-PREMISES	INFRASTRUCTURE AS A SERVICE	PLATFORM AS A SERVICE	SOFTWARE AS A SERVICE
🟦 Applications	🟦 Applications	🟦 Applications	⬛ Applications
🟦 Data	🟦 Data	🟦 Data	⬛ Data
🟦 Runtime	🟦 Runtime	⬛ Runtime	⬛ Runtime
🟦 Middleware	🟦 Middleware	⬛ Middleware	⬛ Middleware
🟦 O/S	🟦 O/S	⬛ O/S	⬛ O/S
🟦 Virtualisation	⬛ Virtualisation	⬛ Virtualisation	⬛ Virtualisation
🟦 Servers	⬛ Servers	⬛ Servers	⬛ Servers
🟦 Storage	⬛ Storage	⬛ Storage	⬛ Storage
🟦 Networking	⬛ Networking	⬛ Networking	⬛ Networking

🟦 CLIENT MANAGES ⬛ VENDOR MANAGES IN CLOUD

Figure 1: The Security Configuration Management Challenge

Even with the evolution of IT from traditional on-prem infrastructure to the cloud, customers still have to manage the configuration of large portions of the technology stack. This is often referred to as the ‘shared responsibility’ model. Each of these stack layers have hundreds of security related parameters that must collectively and correctly work together to achieve the desired organisational security posture.

The security cycle pits guidance from the CISO into the budget-constraints of the operations teams. The development cycle pits the desires of the non-security-aware developers and manual operations thereby creating a drift in the security posture. Business cycles present conflicting needs among the CEO's need for speed, the CISO's need for security, the CIO's need for efficiency, and the developer's needs for a constantly changing baseline. These factors lead to complexity that is hard to manage through traditional processes.

Figure 2 shows how the security cycle gets pitted against the business cycle and the development cycle. Traditional processes for managing security configurations present the enterprise with a tough choice - whether to cut the cost of managing security configurations and increase risk to hobble enterprise agility; or ignore security or limit it to the available budget and take on unquantified risks. Nevertheless, one effective approach to reduce residual risk, cut costs and enable enterprise agility is through automation, as given below:

01 Security configuration checking and setting is automated or made automatable via APIs.

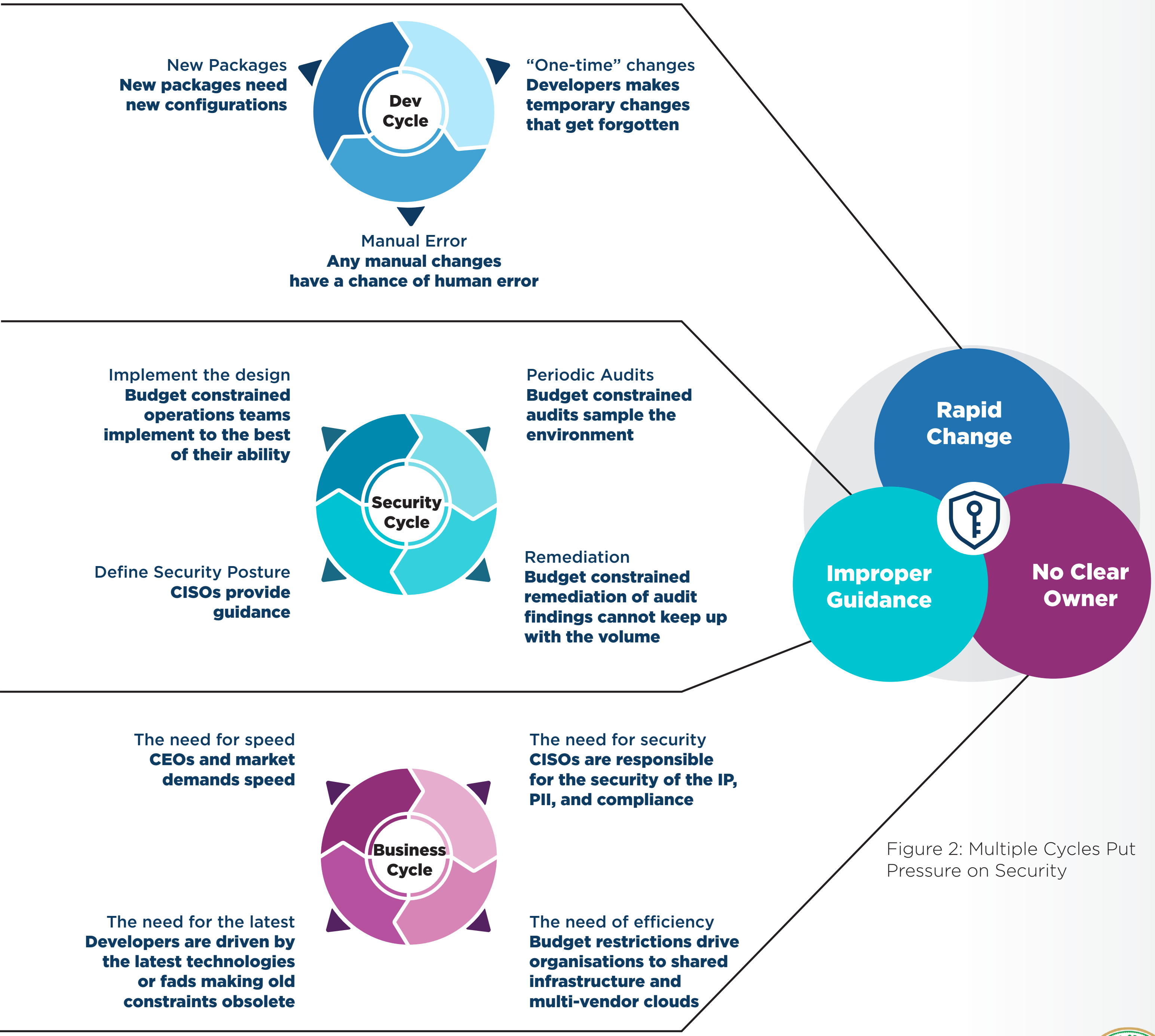
02 Automation removes responsibility from development and operations at deploy and run time and moves it to the design stage where it can be done comprehensively and consistently.

03 Automation reduces the cost of deploy and run phases.

04 The process can be better defined to remove friction between Dev, Sec, and Ops.

02 Reducing residual risk while enabling DevSecOps

With the wide adoption of DevOps, it has become imperative for organizations to include security in their DevOps processes. Enterprises measure the effectiveness of their security and compliance management program along 3 axes - cost of management, residual risk, and supporting enterprise agility through DevOps. Effectiveness of their programs is determined by the cost saved through effectively managing security and compliance, ensuring prevention of loss of money and reputation and enabling the company to make money through agile business processes.



New Packages
New packages need new configurations

"One-time" changes
Developers makes temporary changes that get forgotten

Manual Error
Any manual changes have a chance of human error

Implement the design
Budget constrained operations teams implement to the best of their ability

Periodic Audits
Budget constrained audits sample the environment

Define Security Posture
CISOs provide guidance

Remediation
Budget constrained remediation of audit findings cannot keep up with the volume

The need for speed
CEOs and market demands speed

The need for security
CISOs are responsible for the security of the IP, PII, and compliance

The need for the latest
Developers are driven by the latest technologies or fads making old constraints obsolete

The need of efficiency
Budget restrictions drive organisations to shared infrastructure and multi-vendor clouds

Figure 2: Multiple Cycles Put Pressure on Security

BAU processes would cause an extreme increase in cost if we adopt the 3 C's. Figure 3, however, shows that automating the management of security configurations enables an organisation to cut residual risk through adopting the 3 C's, while also reducing costs.

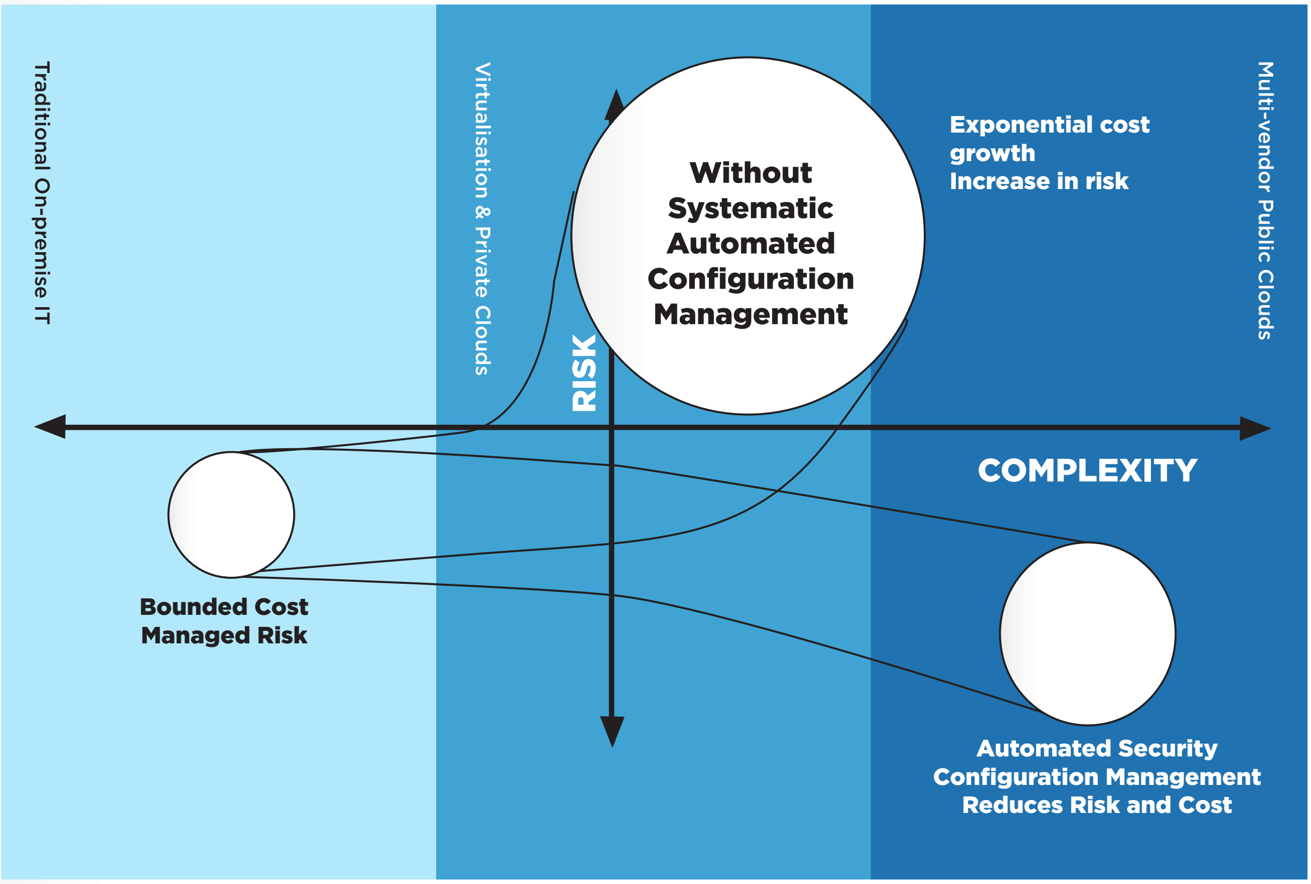
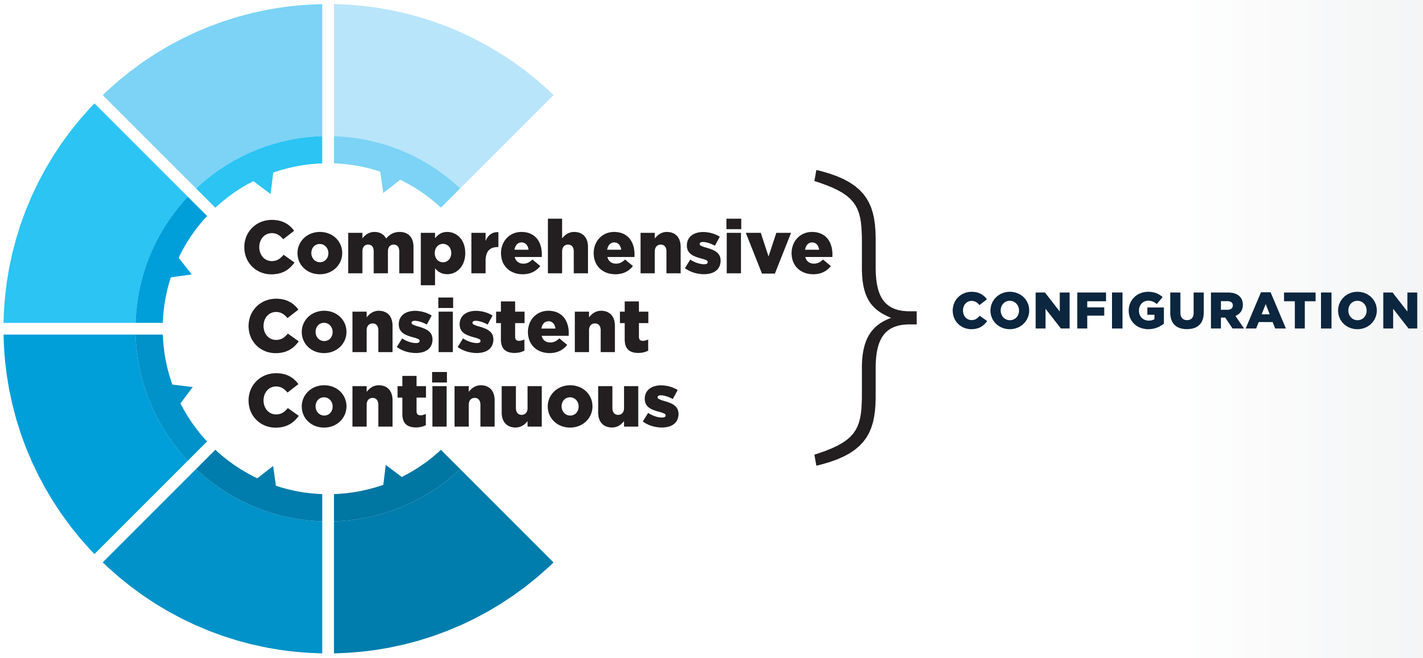

Traditional On-premise IT
Virtualisation & Private Clouds
Multi-vendor Public Clouds
Without Systematic Automated Configuration Management
Exponential cost growth
Increase in risk
RISK
COMPLEXITY
Bounded Cost
Managed Risk
Automated Security Configuration Management Reduces Risk and Cost

Figure 3: Managing Risk and Costs Through Automation

As IT infrastructures evolve from traditional on-premise architectures, through virtualization and private clouds, to fully hybrid multi-vendor public cloud architectures, the management processes must scale. Traditional manual or semi-automated process costs grow exponentially, both in cost and risk. Because of this, they hit a wall beyond which they can no longer handle the complexity of the architecture. Automated configuration management is the only way to reduce costs and risks together in a sustainable way.

03 Comprehensive, consistent and continuous management of security configurations

In section 2, we discussed how numerous controls are available in IT infrastructures (especially in the cloud) to safeguard the infrastructure. Using these controls comprehensively, consistently and continuously is critical as each of these 3 C's are important.



Comprehensive
Consistent
Continuous

CONFIGURATION

Comprehensive configuration means that all available controls are applied to all assets, regardless of whether they are in any cloud, in on-premise IT, or virtualised infrastructures. A recent high-profile exploit was caused because the company failed to do this at the design stage.

Consistent configurations must be maintained consistently across all different IT infrastructures used; like on-premise as well as the different cloud platforms.

Continuous configuration management means going beyond quarterly audits. The smaller the time interval between configuration checks, the lower the cumulative cyber risk. Developers and operations teams routinely bypass controls to get their job done but identifying these changes and correcting them automatically is critical to risk reduction.

Consistent Automated Deployment:

The task of deployment usually falls to the operations team lead by the organisation CIO and is the phase with the biggest hurdles. In conventional practice, the CIO's operations team tends to fall short at translating the CISO's guidelines into practice in a cost-effective manner. Performing this phase correctly is the only way to ensure that the 'as-deployed' infrastructure is the same as the 'as-designed' intent.

Continuous Automated Run-time Management:

This phase is responsible for ensuring that the infrastructure does not drift from its configuration at the time of deployment. In a conventional process, run-time management consisted of tight process controls that IT and operations team placed on change management, and quarterly or semi-annual audits that sampled the environment to document drift. This aspect becomes challenging when it comes to modern cloud-based environment due to the four issues described earlier (Scale, Dynamics, Skills, and Diversity). IBM X-Force study shows that these challenges lead to configuration drift which in turn becomes the easiest avenue for attackers to exploit. Therefore, it is necessary to eliminate drift in the run time to ensure that 'as-running' is same as 'as-deployed'.

Quarterly scanning and manual remediation at the scale and dynamic nature of cloud are too slow, expensive and increase risk. Automated scanning and remediation are the only ways to keep cost and security risk bounded. Unfortunately, remediating drift automatically requires specialised security and operations skills and therefore a dedicated development team. It should not be made the responsibility of application programmers. In 2017, a large outsourcing company was breached because they failed to continuously check for drift in security configurations, and then remediate these findings. Several security configurations were reset during a transition of a key application from test to production and were not identified until much later. This exposed a significant trove of highly confidential data to the internet, and consequently, was exploited.

Therefore, automated cost-effective tools for ensuring 'as-running' is the same as 'as-designed' and 'as deployed' configuration, is key to reducing the risk.

04 Secure-by-design, deploy-as-designed, run-as-deployed

Several recent high-profile breaches were caused due to security misconfigurations. However, it is not the fault of the application programmers alone if security breaks down; the process of defining a comprehensive security posture and applying it consistently and continuously is orthogonal to their main task of meeting functional requirements. This entire process should be frictionless for all parties involved.

Transforming configuration management into a three-step process that spans design, deployment, and run-time management helps reduce friction, thereby reducing the residual risk.

Comprehensive Frictionless Design:

In the design phase, it is the role of the security team including the organisation's CISO to define the security posture that meets regulatory and corporate requirements. The goal is not just to provide guidance or minimum specifications, it is to ensure that the comprehensive set of controls needed to maintain the organisation's security posture are defined. Ideally, all variables that are present in a configuration (ranging from server settings, network parameters, storage controls, and such) are discussed, defined, and documented. The output of this design should be in a machine-readable form so that it can be automatically deployed and enforced. This is one of the best ways to ensure that the applications are 'secure-by-design'.

It is critical to simplify the process of designing the security posture. Designing the security posture comprehensively to consider standards, regulations and best practices consistently across multiple clouds and on-prem is a challenging task. Even highly security-conscious companies have recently failed to include all the necessary configurations in the security posture for their organisations.

In one recent incident there were three sets of missing security configurations: Server security configurations, WAF configurations to prevent SSRF access to the metadata server, and metadata server permissions which were lax. Like most organisations, even this enterprise accepted risks to move the business faster. This desire for velocity drives the devolution of control from expert IT teams to developers and lines of business. While the developers are skilled at using the capabilities of the cloud, they cannot be expected to master all the rapidly changing controls that cloud providers provide. Asking application programmers alone to design and implement security configurations on the cloud is not wise because security is an adjacent skill for them. Thus, each organisation should focus on using appropriate tools that can remove the 'friction' that security introduces into DevOps.

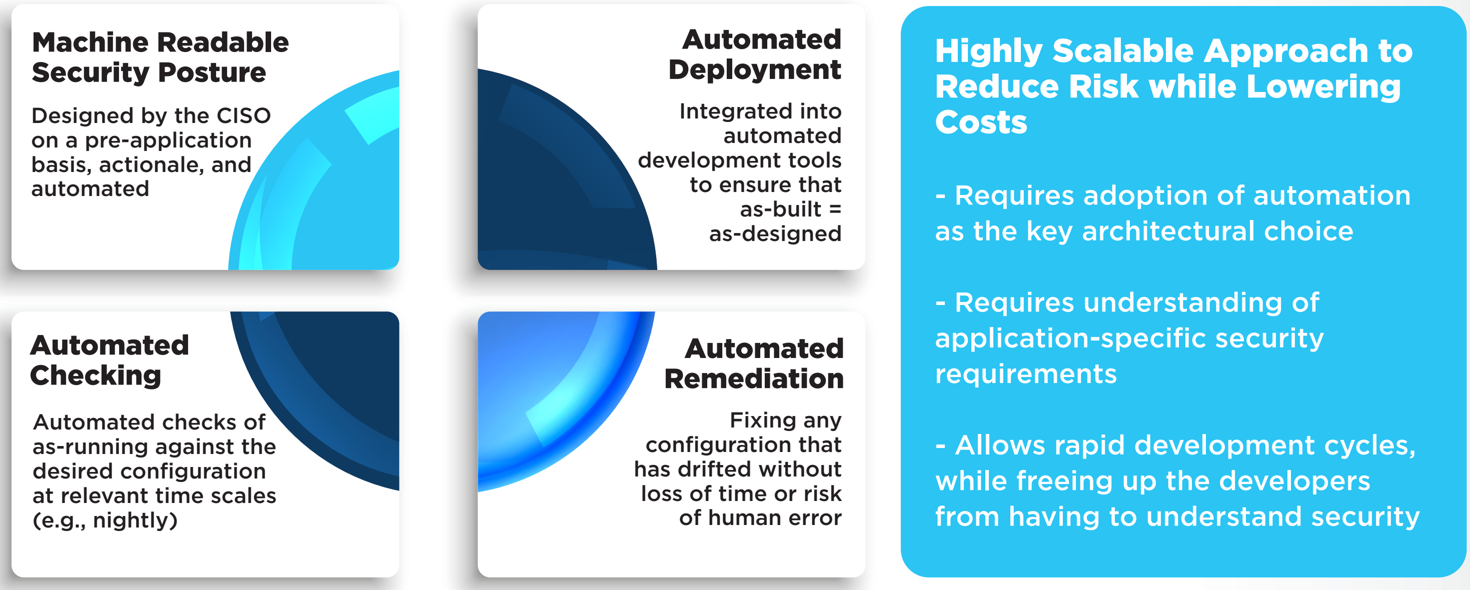
CONCLUSION

It is evident that traditional labour-intensive processes managing security configurations do not work well in the cloud. The increase in scale, the dynamic nature of the infrastructure, hybrid and multi-cloud, and the lack of security management skills in the DevOps community dramatically increase the cost of management and the residual risk associated with traditional processes. Automation can reduce the residual risk by up to 90% and the cost of management by over 85%.

Figure 4 shows a proven approach to managing risk and complexity. The most forward-looking organisations adopt these practices to reduce this risk and to cut the cost of management:

• Create and share comprehensive guidance derived from international standards, regulations, and best practices. This guidance must be established between the CISO, Operations team, and the development team to enable them to cooperate and quickly come up with ‘executable’ application-specific profiles.

• Automate the application of these profiles to the infrastructure. This enables consistent application of these comprehensive profiles to hybrid IT infrastructures (across all public and private clouds, and on-prem elements), continuously over the entire infrastructure lifecycle.



Machine Readable Security Posture

Designed by the CISO on a pre-application basis, actionale, and automated

Automated Deployment

Integrated into automated development tools to ensure that as-built = as-designed

Automated Checking

Automated checks of as-running against the desired configuration at relevant time scales (e.g., nightly)

Automated Remediation

Fixing any configuration that has drifted without loss of time or risk of human error

Highly Scalable Approach to Reduce Risk while Lowering Costs

- Requires adoption of automation as the key architectural choice

- Requires understanding of application-specific security requirements

- Allows rapid development cycles, while freeing up the developers from having to understand security

Figure 4: Proven Approach to Managing Risk and Complexity

It has been identified that systematic application of these principles can lead to a significant reduction in both the residual risk to the organization and the cost of managing the infrastructure by freeing up resources that can focus on other valuable opportunities.

Adoption of fully automated security configuration management is imperative for all emerging architectures. This is particularly important to industries and organisations migrating or planning to migrate from traditional IT infrastructures to the cloud. Failure to adopt these approaches will leave organisations vulnerable to extremely large and potentially unconstrained financial risk from security breaches or loss of reputation due to compromised confidentiality of data or exponential impact to their operational costs.

About Cybersecurity Center of Excellence

The Cybersecurity Center of Excellence (CoE) is a joint initiative of the Government of Telangana and Data Security Council of India (DSCI) to accelerate the cybersecurity momentum and create a conducive cybersecurity ecosystem that nurtures innovation, entrepreneurship and capability building. CoE works with all industry organisations, government agencies, academia and R&D centers and user groups and collaborates with other industry bodies, incubators and accelerators to accomplish its mission. DSCI is a not-for-profit, industry body on data protection in India, set up by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI is the apex industry body for Cybersecurity in India.

https://tcoe.dsci.in

tcoe.hyd

tCoE_Hyd

cybersecurity-coe-telangana

dscivideo

About Cloud Raxak

Cloud Raxak is transforming security in the cloud and creating a business around Security-Compliance-As-A-Service. The company is founded on the premise that the ability to automatically and continuously check the configuration of compute assets in the cloud and fix the configurations as they drift from the desired state is the key to securely using cloud computing in highly regulated industries such as financial services and healthcare. Cloud Raxak's innovative and award-winning agent-less solution works uniformly across cloud providers such as AWS, Azure, GCE, and IBM, as well as across private cloud implementations such as VMWare or OpenStack. Cloud Raxak is based in Silicon Valley with development driven from Mumbai, India.

https://www.cloudraxak.com.

cloudraxak

@cloudraxak

cloud-raxak

References:

1- Gartner security configuration management:
https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2019/

2- Shared Responsibility
Modelhttps://aws.amazon.com/compliance/shared-responsibility-model/

Cybersecurity Center of Excellence
Manjeera Trinity Corporate,
12th Floor, Kukatpally,
Hyderabad, Telangana 500072

For any queries:
P: 040 40339650
E: marketing.tcoe@dsci.in

Cloud Raxak India Pvt. Ltd.

Suite No 05, GF, Copia Corporate Suites
Plot No 09, NHCC Jasola District Center,
New Delhi 110025

For any queries:
E: prasanna@cloudraxak.com

CYBERSECURITY
CENTER *of* EXCELLENCE

A joint initiative of DSCI & Government of Telangana

☎ 040 40339650
✉ marketing.tcoe@dsci.in
🌐 https://tcoe.dsci.in