

How Assertion saved us \$10 million

Un-trackable Risk

The Chief Information Security Officer (CISO) of this large multinational bank had a problem on his hands. They had been subject to toll-fraud, and ended up paying call charges of \$10 million to their service provider in their major business unit in Africa. It was a shocking and unacceptable financial loss to the Enterprise. While the financial loss was one aspect of the problem, what bothered him was that it took them months to identify, assess and remediate the issue.

“We had a good GRC practice in place - a firm, version-controlled, policy setting mechanism, market-leading compliance tools that verified the controls on all the systems and network devices, and robust risk management to track all the findings and manage them to conclusion. Yet, how did this happen?”

Our existing systems couldn't identify or track the fraud, breaking the complete risk management cycle.”

To their compliance teams, the communications network and the associated risks were a black box with minimal visibility and understanding. All their existing tools only identified the OS and network vulnerability issues, but not the application level

issues. This made ensuring the enforcement of their enterprise-wide policy a huge challenge.

“We had Telephony Solutions from Industry leaders like Avaya, Cisco and Microsoft at various locations across the globe, in a huge network of devices and applications. We realised with a shock that all the data that we needed to track this fraud was being provided by the Service Provider, and our internal systems were just not geared to collect or analyse the call records and routing configurations from our communications network.”

The global increase in the number of Telephony-based Fraud and Compliance Issues, and the complete lack of insight into the status of compliance for these devices put the enterprise at a significant regulatory, financial and security risk.

“Managing compliance for this network was challenging, since not only were there a large number of interconnected applications for managing calls, call recordings, messaging, sessions, trunks, unified communications etc., we also needed to get sufficient expertise for all these products within our compliance teams. It was clear that we needed to change the way we were approaching these risks.”

“We needed a tool that would go beyond the platforms and the databases, and study the application level configuration and report on findings.”

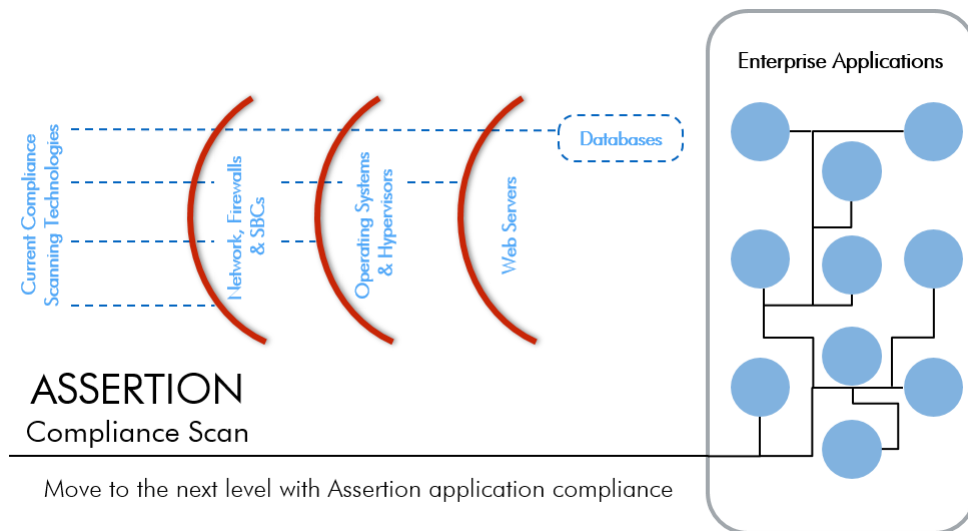
Understanding the Communication Manager

The governance and the risk tiers in any GRC ecosystem are reliant on the compliance tier being able to detect and assess any shortfalls by scanning the controls. The compliance tier is seeing the emergence of new tools that are taking the technology to the next plane.

“What can I do to ensure all my call recordings across the world are backed up as required by enterprise policies? How do I ensure proper CDRs in the right format are collected everywhere? We

needed a tool that would go beyond the platforms and the databases, and study the application level configuration and report on findings.”

Assertion was chosen to manage Compliance for this customer's Communication Infrastructure. A single window into the compliance status of all their communications equipment across the world, with regular and timely scans made the life of the compliance teams much easier.



Adaptability of Assertion

The generic Assertion core platform, with product specific connectors can connect to most communications applications and create a consistent, verifiable data map from the configuration information on these applications like the Avaya Communication Manager, Avaya Call Recorder etc.

These data maps are then used to check for compliance with the organisation's policy.

"We were impressed with the adaptability of the system. We enforced our fully customised policies and controls, on these applications.

The initial scans recognised compliance issues across the board, and we realised what a significant amount of risk was hidden from us all this time."

Costs and Benefits

"The Cost benefits are multifold. While I don't have to worry about expertise in all the different communications products within our compliance teams, we also get to perform the scans on a more frequent basis."

As an additional benefit their sanctioned country policy became a breeze to enforce. Regulators had levied coercive fines over the years for policy violations involving sanctioned countries.

"The question was how can I ensure all our Avaya Communication Managers and Cisco Call Managers in the Middle-East, Africa, APAC, and EMEA can't route calls to a sanctioned country? With Assertion scanning these applications, it was just a matter of adding one more custom control!

In purely dollar terms, I am confident Assertion has saved us \$10million and more."

Published by: ASSERTION | All rights reserved. © 2017 | Publications Date: May 2017