Why Enterprise Applications Compliance Sucks

– and what to do about it

A brief overview of the challenges of managing enterprise applications compliance- the costs, consequence, and solutions.

Enterprises, as you already know, are complex beasts and naturally, their applications are complex too. For example, enterprise communications (EC) systems. These products from Avaya, Cisco, and Microsoft's Skype for Business are the mainstay for telephony, conferencing, video, and collaboration for globally distributed enterprises.

For a moment, imagine that you are the CIO of a large enterprise. Now increased competition means that IT, as usual, is expected to "do more with less". At the same time, because the company is also acquiring new customers, you are being asked to roll out more services across the country, all on the same WAN, without adding bandwidth. After studying the options, you decide to switch over to more compressive, adaptive voice and video codecs.

But here is the challenge: How are you going to ensure that existing converged networking and VOIP gear adheres to the new policy? How will you ensure that the policy of using compressive adaptive codecs instead of the default static, large-bandwidth ones continues to be enforced? How do we know that the entire globe has moved to the new corporate standard? When an administrator forgets to follow the policy checklist, the servers will continue to use the older, more bandwidth-hungry codecs – how will you identify and fix this problem?

The enterprise applications compliance problem is non-trivial.

The cost of policy non-compliance

There is very little comprehensive data on the cost of policy non-compliance in enterprise communications applications, but some numbers are indicative.

- The cost of telecom fraud due to PBX hacking was more than $7 billion in 2015.[1]
- Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration[2]
- The cost of non-compliance is, on average, three times the cost of compliance, as per a study conducted by Ponemon Institute and Tripwire. ($3.5 million for compliance versus $9.4 million for non-compliance)[3]

[1] http://cfca.org/fraudlosssurvey/2015.pdf
[2] http://www.gartner.com/newsroom/id/2753017
[3] http://www.slideshare.net/Tripwire/true-cost-of-compliance

- In 2009, misconfigured PBXes across the US led to $55 million in phone charges because the PBXes were hacked by a single gang, and the misconfiguration was, simply, not changing default passwords.[4]

The problem in Enterprise Applications Compliance

Every year, companies devote vast amounts of effort to ensuring that they comply with standards like HIPAA, SOX, ISO, PCI and so on. Most realize that standardization, especially on the IT front, is beneficial; they usually go beyond basic compliance and embrace standards whole-heartedly. They use products like Qualys, which simplify enforcing compliance of the IT policy across the network.

On the applications front however, things are not so easy. IT managers face multiple challenges here:

1. Unlike IT, there are no government-mandated or even industry-suggested standards.
2. Organic growth in the number of applications, many of them developed inhouse, means that policies are difficult to evolve.
3. Unlike in IT, there are no tools that verify policy compliance

As a result, organizations end up with two solutions:

1. Engage auditors to manually check the applications and generate compliance reports.

   The problems with this approach are obvious:

   - Manual checks imply that the servers are randomly sampled. With random sampling checks, there is no guarantee of any comprehensiveness, which means that issues like policy non-adherence might still exist.
   - Security and access to these systems can be a problem. For example, in enterprise communications, with stores of call logs and recorded data, giving auditors admin rights is a point of worry.
   - Compliance reports need to be acted on, but how to you ensure that the policy is continually being adhered to. Continuing management and enforcement of a policy is always going to be a bigger operational challenge than its first implementation.
2. Leave the application alone and just check its OS and data stores. Use IT policy compliance systems to ensure IT compliance of the servers, but not the applications themselves.
   This leaves a big part of the infrastructure open to security holes, misconfigurations, and policy non-compliance.

In short, the challenges are:

- Lack of industry or government-mandated standards for adherence
- Lack of Automation to check the Policies
- Scale increases complexity
- Lack of formal organizational policies to adhere to
- And failure to address these challenges increases the risks of:

[4] http://voices.washingtonpost.com/securityfix/2009/06/default_passwords_led_to_55_mi.html

- System instability due to misconfiguration, leading to issues like customer backlash and unhappiness
- Regulatory backlash, by failure to adhere to government regulations
- Revenue loss, through hacking and abuse

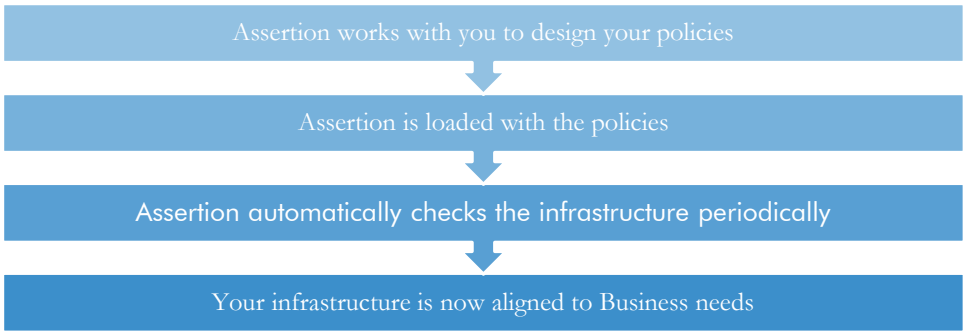
The Assertion approach

Assertion is a solution to the problem of enterprise applications compliance.

Assertion is a product that provides the capability to connect to different enterprise applications, including internally developed applications, and test them for compliance to organization policy. To do so, Assertion provides connectors to various applications.

Let's take the previously mentioned example of enterprise communications applications. To implement Assertion,

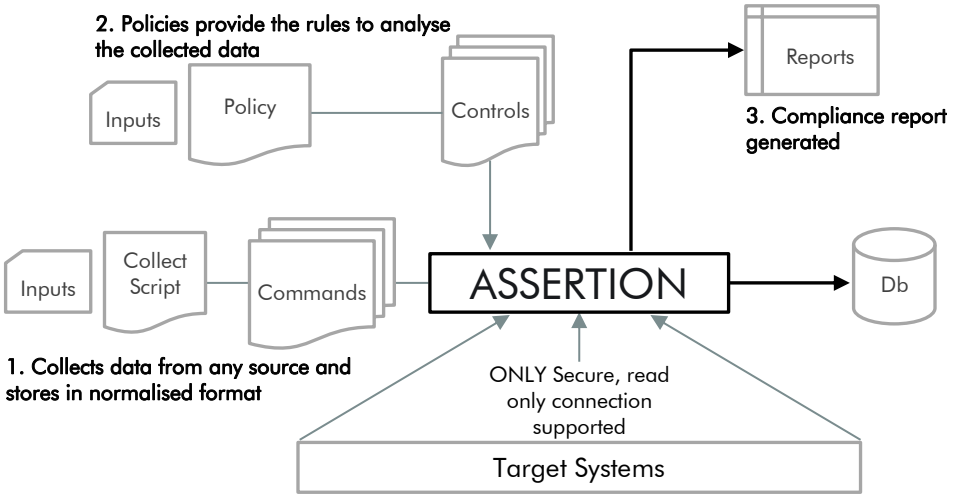
1. Consultants engage with your EC teams to define your organization's policy – this work often needs to be done from scratch as companies often do not have defined policies in place. If defined policies do exist, they are verified and improvements made, if needed. These policies are your record and are expected to be 'living' – going forward, every time you change any aspect of your EC policy, you can update these documents.
2. Assertion then uses these low-level policies to create standards.
3. The standards are then loaded into the Assertion server.
4. You can configure which servers need to be tested for policy compliance. On demand, Assertion connects to the servers and checks their compliance by testing them against the policies.
5. The results are logged and converted into graphical reports that are easy to track and understand.



Assertion, as an automation system, allows for comprehensive, accurate, and rapid checkup of all your EC systems. It also allows you to confirm that your policies have been implemented as required, and more importantly, continue to be enforced across the enterprise. Also, once configured, it helps you undertake periodic and regular compliance checks of the system. Adding or modifying your EC policy becomes easier – update the policy, create a new set of tests, load them into the server and you are good to go.

From a security perspective, the system requires limited access to the target systems – there is no agent to install, the access is read-only, and the load on the system is minimal. This makes it much safer to work with than a typical manual check – once set up, there is no human access or intervention needed at all.

Reports are customizable, sliced by time, location, error, and many other parameters to suit organization requirements and are also signed, so there is a clear guarantee against tampering. Adding support for a new product is simply a matter of writing a new connector, creating appropriate policies and loading them on the Assertion server.



Overall, Assertion provides a straightforward and much-needed resolution to a problem that has plagued large enterprises for quite some time.

Conclusion

The lack of an automated policy compliance tool for enterprise applications has been a problem for large enterprises – it has left them with significant exposure to security issues, losses due to misconfigurations, and to regulatory backlash. Without a policy compliance tool, application infrastructure managers have been forced to rely on solutions that are manual, half-baked, and non-comprehensive. Assertion fills a much-needed gap and can help large organizations significantly cut costs, close security gaps, and ensure policy implementation.