CONTINUOUS COMPLIANCE AT NIU SOLUTIONS

Niu Solutions offers IT managed services specializing in regulated industries such as retail, financial services and banking. Founded in 2000, Niu is a UK-based company operating with data centers in the UK and US as well as on the public cloud. In this article, Jon Williams, CTO at Niu, talks about InSpec, Chef and the beauty of automation.

Many of Niu's clients are what Jon calls "high velocity." He says, "By high velocity, I don't necessarily mean that they need to deliver things quickly, though actually they often do. It's more that they're going through rapid changes, perhaps because they've divested from another company or they're a startup or because of internal challenges. For whatever reason, these companies have strategic changes going on in their organization.

"Most of them also tend to be in highly regulated industries, such as banking. We come in and help them, not just with the infrastructure side of things, but with mapping their regulatory requirements to the infrastructure we provide them and to the applications that sit on top. We work very heavily with ISVs to build out platforms that are repeatable for their client base."

ADDRESSING THE CHALLENGES OF HIGH VELOCITY BUSINESS

High velocity companies turn to Niu to help them move quickly to capture opportunity while limiting regulatory and operational risks. To meet those needs efficiently and avoid unplanned work, Niu employs repeatable patterns and processes. As Jon describes, "We effectively try and build out a template of the world and deliver that again and again. But humans will make mistakes and once they're in the system, they get missed." Gary Bright, an infrastructure developer at Niu, was tasked with finding a way to eliminate those mistakes, as well as the inefficiency and risk they create. Jon says, "He told me he'd found the answers to our prayers and that was InSpec."[1]

[1] To learn more about how Niu uses InSpec and has tied it into their DevOps transformation, listen to Gary's ChefConf 2017 presentation, "Kick starting our DevOps Transition with Chef Compliance." https://youtu.be/YhZajGM-fQY

COMPLIANCE AS A FIRST STEP

To drive greater efficiency and eliminate risk, Niu started by applying InSpec to support a three-tiered approach to compliance checking. The first tier is regulatory compliance, including conformance to standards such as PCI Security Standards and CIS. Jon describes what auditing was like before and after InSpec. "Audits tend to be a leap of faith. You work your systems and follow your processes throughout your yearly cycle and you hope you win. All of it is kind of like an exam in the sense that you do all your revisions and you do all your work and you hope that you get good results at the end of it.

"With InSpec, you have a real-time view of how you're performing. When you come to that audit exam you already know if you're passing or not. In fact, the event of the audit is a simple step of printing the output."

The second tier is compliance against best practices. The accumulated knowledge of how to create base infrastructures or client applications are mapped into compliance checks. All the best practices that Niu and their ISVs know are encoded to make sure that the systems are consistently in the correct state. The result is that the number of issues decrease and overall compliance increases.

"With InSpec, you have a real-time view of how you're performing. When you come to that audit exam you already know if you're passing or not. In fact, the event of the audit is a simple step of printing the output."

Jon Williams, CTO, Niu Solutions

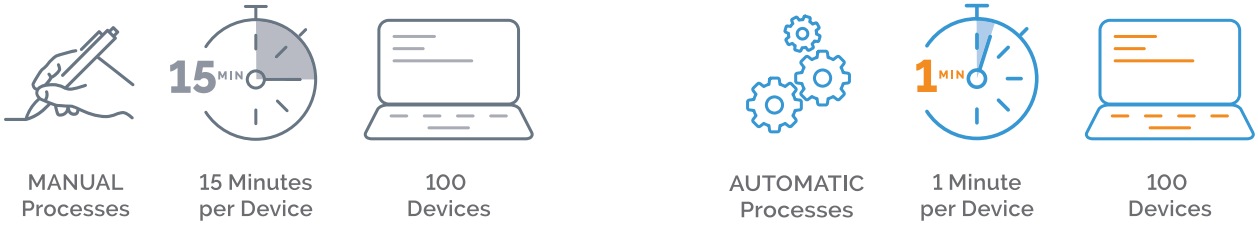
The third tier is to incorporate lessons learned as they arise. Jon gives an example. "We might have an outage on a system and find that it's a configuration issue that's not part of our standard compliance checking. We can write that compliance check and then run it across our entire estate so we'll know straightaway if there are any other risks."

Jon says, "There's a huge potential to reduce unplanned work. That's a key benefit and a great place for companies that are adopting InSpec to start. Too often, other approaches are basically seen as punitive. You end up creating a whole queue of work for the operational team that they're then responsible for fixing. They see the process as calling out every mistake they've ever made and giving them more work.

"With InSpec, life is better. If they've experienced an outage, they've already gone through the pain of the client calls and the late hours. We can turn around and say, 'Good news. Before you experience another outage, we can tell you that there are four other systems that have the same issue. Here's the fix.' Now, all the operational teams are coming to the likes of Gary and others in our organization and asking them to write controls for issues they find."

CAPTURING MEASURABLE OUTCOMES

Niu conducted experiments to discover how much time they saved with InSpec. In one, they used firewall compliance as their test case, giving an engineer the task of checking devices manually and seeing how long it took. They then performed the same checks with InSpec. Based on those results, Niu found they could reduce the time taken to conduct compliance checks by 93%. This saves Niu nearly three person-days of work for every 100 devices checked.



WITHOUT INSPEC

3.125
WORK DAYS

93%
TIME REDUCTION

WITH INSPEC

100
MINUTES

There's another benefit of InSpec that Jon appreciates. He says, "The control is about the business problem and that makes things easier. I stole this idea from Nathen Harvey and used it at ChefConf last year. Nathen's point around the difference between easy and simple is that people say they want simple but what they really want is easy.

"With InSpec, you really can shift to the left. Anyone at any level of the organization can consume a control and assess their risk. What's going on behind the control can be incredibly complex but the result is very easy. It's just a yes/no answer. 'Is it compliant? Yes? Perfect, I'm happy. I don't need to know how you checked it.' Obviously, people do want to know how the controls work but at a business level, and InSpec helps us to stay with business conversations rather than technical ones."

Niu began by writing just a few controls and gradually built up their library. Now, Niu has approximately 1,000 controls available and they've seen huge reductions in the time it takes to perform compliance checks, in the amount of rework and in the amount of unplanned work. Niu feels that their process is mature enough that they will offer their own compliance as a service product built on Chef technology.

DETECT, THEN CORRECT – MOVING TOWARD CONTINUOUS AUTOMATION

As they became comfortable with compliance as code, Niu began to incorporate infrastructure automation with Chef into their process, both for configuration and to deploy compliance fixes. Jon felt that starting with InSpec gave them insight into how they should write their cookbooks. He says, "The two are linked. Writing controls helped us to define how things should be built. In fact, it gave us a template. If you're going to automate something, you should be very, very clear about what you're trying to automate.

"A typical case is that people say they want to automate building a server but that's an outcome. What needs to happen along that journey? Lots of people think only about deployment. You can deploy a cloud server in a few minutes, which is a great thing. What surprises people is that it's still a server. They still have to manage it if something goes wrong. They still have to patch it. Many people think it's automatically patched.

"Our approach to automation, certainly from a server point of view, has three steps: deployment, configuration and integration. Deployment comes first, naturally. That's when we build the server. Configuration happens once the build's done. We need to know what changes we're going to make and what the settings should be. Finally, there's integration, which is the toughest to achieve but has the highest value. That's where you make sure the system is plugged into your backups, your monitoring, your patching, your anti-virus. Integration is often done by different people but automation reduces the number of hands."

> **"What was amazing also was watching what the teams went through when an urgent patch was released. They saw that 60% of the manual work they previously had to complete, often resulting in lost nights of sleep or their weekends, was reduced to minutes.**

Jon Williams, CTO, Niu Solutions

RAISING EFFICIENCY, REDUCING RISK

On their journey to continuous automation, Niu is realizing outcomes with every step. As Jon describes, "One of our big wins is SQL. It used to take our SQL specialist a day to go through the full end-to-end set up. With Chef, we've reduced that to 12 minutes. Another example is managing disk space, one of our biggest headaches. For too long, we simply accepted this problem as the norm and told ourselves we didn't spend much time on it but, when we did an analysis, we found out differently. We were spending a huge amount of time on it."

Patching is another area Niu addressed with automation. Jon found that automated builds and InSpec made an enormous difference in the amount of work they had to do to make their servers safe. He says, "Literally, anything that went through an automated build had no issues, which is amazing and, actually, a revelation. Also, the InSpec coverage we have on the legacy infrastructure reduced greatly any legwork we had to do. We already had the basic control and only had to write a specific control just to double check that the patching was up to date. Very powerful.

"What was amazing also was watching what the teams went through when an urgent patch was released. They saw that 60% of the manual work they previously had to complete, often resulting in lost nights of sleep or their weekends, was reduced to minutes. This made it easy for the teams to see why creating these controls helped them, as it really hit home how important visibility and automated remediations are. You've got to be able to react to these situations. It's back to that point about the audit. You can't be in a position where something like this happens and you live in hope. Hope is not a strategy."

LOOKING TO THE FUTURE

Automation, particularly with InSpec, has helped Niu further their DevOps initiatives by encouraging more involvement from stakeholders. Jon says, "The lesson we learned is it's all about bringing people with you. You need a plan of what you're trying to achieve. What business problem are you trying to solve? Keep it really simple. You can run away with the tools and get very excited. The team was smashing out controls like nobody's business and we had to stop. It was more about going and speaking to the operations teams and the InfoSec teams and understanding their problems, what was burning up their time. You need to deliver something that will get their buy in, get them to understand that this is a good thing so that they tell you about their faults because it helps them. If you don't see those people as the customers you just create barriers, which is the opposite of what you're trying to achieve."

Reflecting on what Niu has accomplished so far, Jon sums up by saying, "InSpec gave us the headspace and the room to go on the automation journey. When you're managing legacy infrastructures, you're in a catch-22 around reducing unplanned work. You don't have time to figure out what the next step should be. Reducing unplanned work has given us that time. We can ask ourselves, 'We've taken control of our legacy. How do we build our future?'"