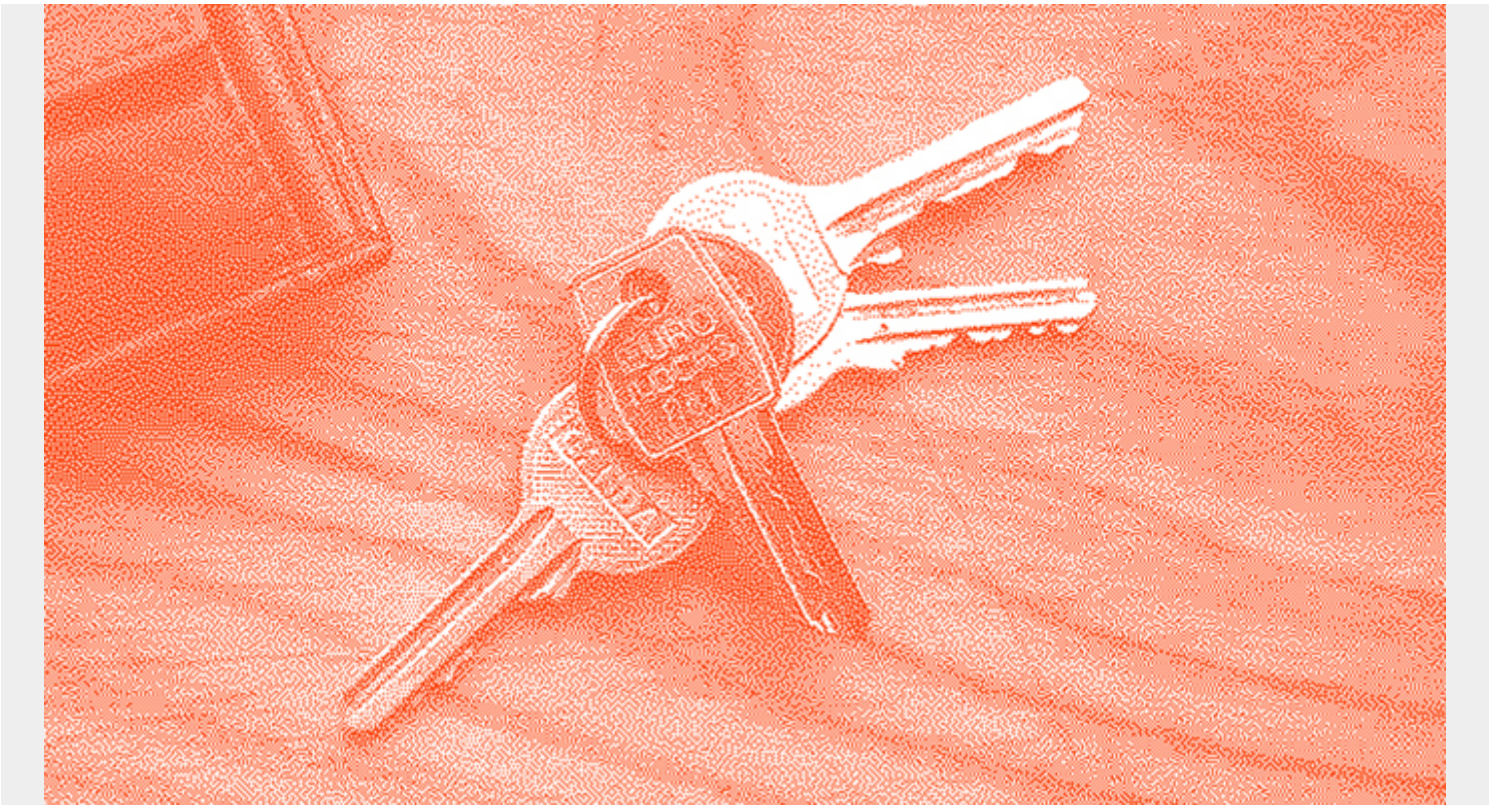
NATIONAL BANK OF CANADA BOOSTS SECURITY WITH IMPROVED VULNERABILITY MANAGEMENT



In this Run and Reinvent podcast, I chat with David Beaulieu, leader of IT infrastructure services integration and VP of IT operations and performance for National Bank of Canada, about how the bank manages its security vulnerabilities and server automation practice. Below is a condensed transcript of our conversation.

Roger Hellman: Could you just tell us a little bit about your IT environment, so we get a feel for it?

David Beaulieu: Our environment, as most banks or most financial services, is composed of various technologies. Some are newer. Some are let's say older. We have a range of platforms which might include Windows, Linux, AIX, AS/400, mainframe, so we do really have big difference in technologies. And like everybody, we're interested by cloud. We have a small presence, but still trying to deliver faster solutions to our customers.

Roger: And how is your group organized?

David: We're a big organization. We have 23,000 employees. The main sectors, I do report to IT Operations, the Vice President of IT Operations. And I closely work with my colleagues in security, which they report to the Chief Information Security Officer. And both teams work very closely together to make sure that the risks are brought down to the minimum. And then as long as we deliver value, especially in the cloud, that will leverage the technology that allows us to see the blind spots and fix them as quickly as possible.

Roger: What were the challenges and the goals that you wanted to achieve that led you to adopt a TrueSight Server Automation and TrueSight Vulnerability Management?

David: Our environment is quite wide; different systems, different platforms, different environments, anywhere in the world. And we had challenges, like everybody. We had old systems. We had new systems. Some of them were manual. Some of them were automated.

And the key factor here is we were looking at speeding things up, making sure that when a hacker gets up and decides to attack that we would be ready at any time of the day to quickly detect and fix any vulnerability in the infrastructure.

Roger: Give us an idea of how things were done in these areas in the past, so the before picture, and then how things are being done now, so the after picture.

David: Oh boy, quite different. I have to dig deep back in how we were doing things before. But it involves a lot of manual process and a lot of manual steps, a lot of emails, a lot of downloads. Everything was manual. We had different systems. We had change management. We had the sys admins, depending on the platform. And then if you wanted to fix something that was not provided into a fix by a manufacturer, well, you were kind of in between two worlds. And what TrueSight Vulnerability Management made us do is everything that I just said, but in a better way. Automated. Change management. A to Z is now automated. We don't even create changes anymore. The system does.

The system opened the changes, deployed the patches, or the configuration. It closed the changes in the change management system, TSVM also gets its input from a detection system, so the TSVM knows when there's a vulnerability. It knows when it can patch. It knows when it can deploy. And it can all do that by itself.

Roger: Sounds like you're really taking advantage of the integration between these offerings.

David: Definitely. That was the key point for us. Doing like a change record in a system and chasing the approvers and the testers, it took time. They were questioning why are you doing this? Why now? Why not tomorrow? So, we had a lot of questions.

So, and then it took a lot of time for a lot of people. But the overall integration between TSVM and our other software is the key here to make sure that everybody's got a – their life is more easier, and they can concentrate on what brings value to the bank and to our customers.

Roger: Are any metrics that you could share with us about the improvements that you've seen from using these offerings?

David: Where before, it took us maybe let's say a couple weeks to deploy the patches with all the manual steps. Now, depending on the criticality, we can deploy within less than 24 hours. So, I don't see that happening in the old days.

Roger: Share with us the value you realized from these solutions, and how they've helped to improve, and maybe even transform your business?

Well, the life of my sys admins, they can look at TSVM on a Saturday morning with their coffee and making sure everything is green, and everything is running smoothly. It took a lot of effort. I have to mention that. It's not something that you're gonna buy and do next-next finish install. No, it takes time. You need to know your processes. You need to know your infrastructure. And, honestly, with big infrastructure, sometimes you run out into surprises, and then that's the value that TSVM

brought.

Roger: What other advice would you give people in a similar situation?

David: Automation is a big part. Don't be scared to automate, start up, and testing of your infrastructure, even if it's in the old age. I'm not talking OS/2 or Novell here, but with technology, I mean, some of the systems are fairly old, but you can still automate stuff. Obviously, if you do have only one server, maybe it's not worth it. But the automation is the way to go because creating something that everybody will be able to reuse and adapt will be the key success to maintaining infrastructure.