



Cloud Security Can Be Made Simple

How ditno Used Spirent to Convince Security and Infrastructure Managers That Cloud Security Does not Have to Impact Performance

A Spirent Case Study



Background

You have complex systems and solutions to manage. It includes an extensive private cloud of virtual machines, a number of hardware servers and it also connects to public cloud services. You also have users and management breathing down your neck with concerns about data security, privacy and new waves of data protection legislation.

Then you hear about a company called ditno claiming “Security made simple” based on a single cloud-based framework that provides “single pane of glass” security management across public and private, internal and external clouds, and legacy resources.

It sounds too good to be true!

Exactly that was the problem faced by ditno sales. So, to address customer concerns about the ability of the solution to scale without adversely affecting server performance, they asked Matrium Technologies, a third-party supplier of testing solutions such as Spirent Avalanche Virtual to provide hard evidence that their solution delivered cloud security with minimal impact on CPU usage and transaction response time.

ditno’s security solution

Provides a continuous, pay-as-you-go security framework and logging capability across hosts, regardless of service provider, platform and operating system. This allows businesses to protect their data and improve network analysis while utilizing new technology services, enabling flexible customer services while increasing productivity.

As enterprises outsource hosting to the cloud, legacy security strategies no longer provide a matching level of flexibility and scalability. Cloud solutions replace the initial data center CAPEX with a more efficient pay-as-you-go OPEX model that scales expenses to match demand. Enterprise security, however, has been largely appliance or chassis based, requiring significant upfront capital equipment investment to meet possible future levels of demand.

This inflexibility of legacy security solutions erodes much of the potential cost-savings of migrating to the cloud.



Spirent Avalanche Virtual shows that ditno’s solution will secure hybrid clouds without adversely affecting server performance.



—Glen Messenger, ditno CIO

ditno has taken a radical new approach to this problem, creating a cloud-based framework that provided security for any cloud—whether including public, private, internal, external, and/or legacy resources. The security architecture is based on two main elements:

ditno NetGuardian: A light-weight embedded agent, enabling robust, powerful and continuous security controls regardless of major operating systems and location.

ditno Glass: Ditno Glass is a single security management portal that enables operators to perform repeatable, elastic and flexible deployments of security policies to each NetGuardian instance.

As Glen Messenger explains: “You can think of it as a delivery mechanism to roll out security across the cloud as needed, beginning with Layer 4 firewall security, then adding web security with advanced web application control and Inspection.”

“By providing a cloud-based security solution,” said Messenger, “we addressed the disconnect between the flexibility of cloud hosting and the hardware, and budget, demands of legacy security.”

The challenge

Some potential customers were concerned that the NetGuardian embedded agent would have an adverse effect on server performance and end-user quality of experience (QoE). To address those concerns and conclusively demonstrate the scalability and performance of their framework, ditno realised that they should provide independent test results from a reliable, third-party tester. This would depend upon the use of a test solution capable of emulating realistic test cases in a virtual environment.

According to Messenger, “the test tool needed to be flexible and scalable enough to simulate real-life scenarios, including dynamic loads and a range of connection and content types, while emulating realistic user behavior.”

ditno approached Matrium Technologies Australia's leading supplier of network test solutions with over 20 years' experience in the field. Matrium recommended testing using Spirent Avalanche Virtual—an "all-in-one" cloud test solution designed to test and measure the Performance, Availability, Security and Scale (PASS) of virtualized network infrastructure and applications deployed in the cloud. In particular, Avalanche Virtual's ability to be hosted in the cloud for testing provides compatibility with virtual environments such as XEN, Citrix, KVM and QEMU.

As a security test platform, Avalanche Virtual tests the robustness and resilience of a system under any combination of encrypted traffic, state-of-the-art cyber-attacks plus realistic user behaviour based on details such as a specific browser, authentication, task, timing, content validation etc., to interact with actual deployed applications. Among the features ditno needed to test was the system's scalability—they distributed up to 8 million logs in about an hour.

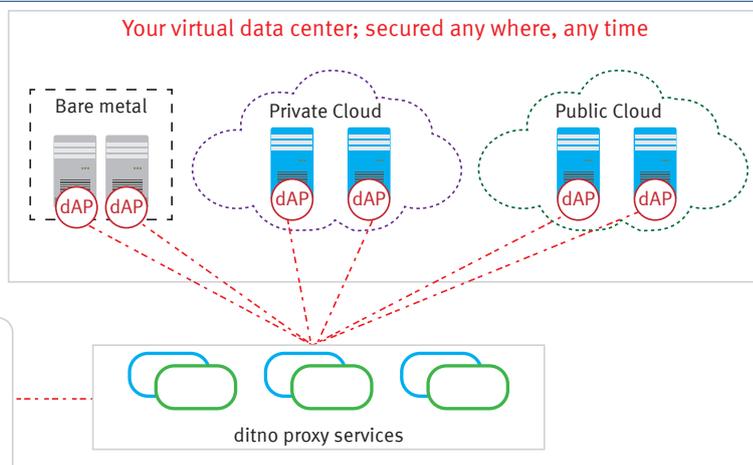
The solution

By late 2013, Matrium Technologies had performed rigorous third-party testing of the ditno solution using Spirent Avalanche Virtual. The Spirent system then generated a detailed test report that ditno can now use to demonstrate to doubting buyers that the solution really does deliver security across the cloud without impacting performance.

Avalanche Virtual provided the power of a physical appliance to emulate realistic user behaviour at any scale across a wide range of protocols, and the virtual component allowed the end-to-end test to terminate at the virtual-machine level on the servers, which was exactly the point of concern.

"The tests were run in a public cloud environment, which was perfect because that's where our development and deployment are done" said Glen.

The testing had other benefits for ditno. During the test, the transparency and flexibility of the Spirent test solution enabled the testers to pinpoint performance issues so that ditno was able to make code improvements on their solution before release. This is a vital and often overlooked aspect of network testing—more than just a necessary burden on development, testing becomes a highly efficient means to identify problems and resolve them, and much more cost-effective than addressing bug fixes weeks later when a customer discovers them.



Using multiple profiles, ditno was able to perform regression testing with the click of a button as new code versions were released, and this established test methodology has become a key part of ditno's development cycle. As Andy Walker, CEO explains, "The speed at which new releases come out now, calls for an agile response. With Avalanche in a cloud environment we can now do a regression test in a couple of hours that would have taken weeks in the past. Without leaving the premises we can massively scale tests in any location—the customer data center, Amazon in the US, a cloud service in China or anywhere."

A third benefit, according to Walker is that "our customers can now run their own tests after deployment, using Avalanche as an easy means to monitor performance and make sure that they are getting the full benefit of cloud-based security with minimal impact on memory consumption, CPU time, performance, and end-user QoE."

Conclusion

"Our solution is unique, and to convince the customer, we needed to do large scale tests across multiple service providers, multiple locations and multiple operating systems at the same time. We hurled massive amounts of traffic—not random bits, but realistic user traffic—and serious cyber-attacks, at each system, and then get an immediate report on performance results. That was the only way to meet the need for agile development and rapid response while providing proof of what our solution can achieve" Walker added.

Thanks to Avalanche Virtual's flexible and comprehensive test capabilities ditno had not only accelerated their solution development by identifying potential problems before they "hit the fan," they had also got objective proof of their solution's capabilities. The added benefit of being able to recommend a monitoring and test regime for their customers, using Avalanche Virtual provided on-going assurance of their cloud security and performance.

AUSTRALIA: 1 300 889 888 | sales@matrium.com.au

INTERNATIONAL: +61 2 8851 6900 | sales@matrium.com.au

www.matrium.com.au

© 2014 Matrium is ANZ's leading provider of high-end communications testing, monitoring and network security solutions. With more than 20 years of experience, Matrium delivers the industry's most innovative products and services to service providers, solutions suppliers and enterprises in the region. Rev. A 03/14

