



A CUSTOMER-CENTRIC GLOBAL NETWORK

Network security continues to be a very serious issue for the industry in general as cyberattacks affect networks and services. What is NTT Communications doing to protect its network – the Global IP Network – and its customers' networks?

We're doing a lot of things on a number of different levels. From our own network perspective, we've built the network to be resilient and also meet the most stringent standards so it is protected if it is attacked deliberately or errors occur in routing from our customers or peers, to make sure it doesn't impact our customers in a negative way. Our network is based upon industry standards and we make sure we're applying them in the best possible way – things like BGP tools and RPKI are key parts that we've adopted for a while.

Beyond that, we offer our customers a suite of services and tools for network security. These include mitigation of DDoS attacks, and free tools like black hole filtering. We will continue to develop our product range to enhance our offering, whilst giving our customers the choice of services which best suits their needs.

How does NTT Com evolve its offering to tackle the ever-changing nature and size of DDoS attacks?

There is a bit of cat-and-mouse to tackling new threats. Beyond making the architecture of our network resilient, there is a number of steps we take. Volume is not the only issue – there is also packet-per-second volumes and these can be much more damaging for particular services. At that point, the infrastructure itself doesn't help a lot – you need to look at being able to deploy more advanced tools and capabilities around access control risks, scrubbing of traffic, and redirecting or terminating traffic on the edge to make sure those kind of attacks don't take down customer specific services or environments. It is an ever-evolving situation and I don't think we'll see that change any time soon. Generally speaking, attackers will continue to get better at what they do and find new avenues to pursue attacks, but we'll continue to develop ways to address those attacks.

NTT Com offers one of the most comprehensive set of BGP Communities in the industry. Why is transparency on routing policies and BGP communities in particular important for your customers? What's the benefit for them?

We think transparency is important for a number of reasons. The internet is a network of networks and it utilises a series of industry standard RFC-based BGP announcement sets allowing configurations and for traffic to travel round the world. For this to all work, you need to have transparency and there also needs to be a commensurate level of trust.

At its core, that's how the internet functions, so if it breaks, or if someone tries to attack somebody, you need transparency. That's why we've been a big proponent of things like Resource Public Key Infrastructure (RPKI) for a while. We've done a lot of work – along with a number of our peers – to propagate that. Those kinds of things protect the internet to make sure it works the way it needs to.

For our customers on a global level we provide a lot of flexibility.



I'd certainly put us among the top carriers regarding flexibility for our customers to use BGP communities in allowing policies as they connect to us in different parts of the world. This allows them to do a number of things in regards to how they route their traffic and how the traffic they send to us, dependant on geography, will route to other networks in the ways they define, as opposed to how we define it. We try to pass that transparency on to our customers so they can leverage the network in the best possible way.

A lot of our competitors offer quite a bit less visibility to their customers. I'm not sure why but it serves as a differentiator for our network with other tier 1 operators.

Focusing now on innovation and automation, NTT Com was one of the first carriers to develop and implement software-defined networking, or SDN, in its global network. What are the results that the company has seen by adding automation to network management?

I feel like SDN and automation has been part of our DNA as an organisation for so long, I'm not sure I could imagine it without the automation. It is part of who we are. Automation reduces errors that can occur down to human-error by creating rules that are part of that software package, and that is a huge benefit. It also saves a tonne of time for our staff, allowing us to do things much more efficiently, much more effectively, and that has benefits in terms of operating expense for us as well.

Where it has taken us in the last year or two – because we've been working on automation for over 15 years – is in providing us the ability to be highly efficient when scheduling network maintenance. Also things like upgrading routers or uploading new code, or making a transition in infrastructure from 10G cards to 100G cards for example, can be done in a much shorter amount of time. Customers see these as very positive things as they reduce disruption and keep service speed and the status quo. That's on a global scale so it's a big advantage for us.