Securing intelligent networks: a guide for CISO and CIOs

93% say security is a ‘must have or should have’ for customers of SD-WAN technology; 97% say the same for network function virtualisation.

Paul Crichard,
Chief Security Technology Officer, BT

Paul is in charge of bringing together the technical capabilities around the BT technology stack and making sure they have a future, a development path and options for revolution as well as evolution.

He’s a Fellow of BCS and an advisor to a number of universities and expert Government panels for security.

He worked for nine years in UK Government, was Head of Cyber Research for Raytheon and Head of Incident Response for Vodafone Group.

Security must keep pace with evolving networks.

With networks evolving fast, it’s a good time to rethink your approach to security. A leading analyst who did some research for us recently[i] found that security is the C-suite’s top consideration when looking at network services. But networks are changing. New ‘internet native’ applications and services need more bandwidth, performance and flexibility.[ii] Luckily, new technologies like software-defined wide area networks (SD-WAN), network function virtualisation (NFV), hybrid WAN and application performance management (APM) can do all of this. But they’re shaking up the way we think about security, too.

Organisations are investing in new networking technologies to keep up with digital transformation and the unstoppable growth in data. They’re pushing their business traffic over public internet links and cellular networks. And that means taking it outside of their organisation’s boundaries. The traditional security perimeter is disappearing. More internet break-outs mean more points of entry for hackers. It’s complex. And it’s a vulnerable environment that’s difficult and vital to protect.

Although MPLS and Ethernet services still have an important part to play in the network landscape, because of new technologies they now need to be included in a wider network. One with a security strategy embedded in it. One that takes care of local internet breakout and cellular bandwidth provision.

Here’s a summary of the key security considerations in this hybrid network landscape. As well as some suggestions as to how some of the challenges can be overcome.

i CXO survey – Gartner July 2017 (BT GS sponsored survey)
ii SD-WAN Is Causing Disruption in the Enterprise WAN Edge – Gartner June 2016

A move to virtualised security

As network technology changes, the role of security technology needs to change with it.

It used to be simple to design a network. The focus of the security defences would be the hardware and software applications in the data centre. But as we move towards software controlling the network, we need to make sure it's able to control security as well.

The journey starts with the virtualisation of core network security devices, like firewalls. And it ends with the full connection and streamlining of security controls, defences and processes around events and responses.

Intelligent connectivity means it's more and more likely that data in your network will be hosted on virtualised technology. That means your network's security functions need to be virtualised, too. So they can flex with your network. The move to a virtualised environment should be smooth and seamless. Not forgetting speedy and automated. Service providers should make complex challenges, simple. That way, you'll be able to set up a range of security services, from basic service management through to full incident response and threat intelligence, quickly. To make a success of this full security technology and process life-cycle, you need the support of skilled practitioners. People who can set up your service, manage your system, and detect and respond to any threats.

In the same way that network technologies are changing, the roles of different security technologies are becoming more blurred. This makes it more of a challenge when it comes to providing clear direction and strategy. As networking and security strategies and operations come together, it creates the need for new skills within those teams. For the best chance of success your CISO and CIO teams need to align, quickly.

Securing a flexible, hybrid network

Let's take a look at a few different ways in which your network can evolve.

It's important to weigh up the risks versus the threats. That way, you'll be able to spot any new security considerations. And work out where traditional perimeter security controls are still useful.

Growing network traffic is prompting companies to adopt new network services – ones that can boost their core MPLS and Ethernet services. But bolting on extra services makes it hard to keep up the right level of security across them all. A bigger, diverse network adds a lot more complexity to the data, making it more of a challenge to spot unusual behaviour.

What you need from your network

- To be able to detect new threats quickly – using threat intelligence and horizon scanning to find and address threats before they can do serious harm. This includes providing clear and useful information to those who can respond.
- Secure, policy-based routing – you'll need to think about security end-to-end and use the right security measures. Make sure your controls are tailored for maturity, network pathways, application usage and data centre locations, but also give you clear and flexible options.
- Performance vs security – it's important that your security devices adapt and grow at the same rate as your network and computing power.
- New sources of data and response – new technologies bring a variety of new sources of data that can be used to detect and respond to threats. They do this by understanding the underlying log systems, amongst other things – for example, Amazon Web Services (AWS) can detect potential breaches in the fabric of the data centre and get round those threats using selective network blocking.

iii https://link.springer.com/article/10.1186/s13174-014-0015-z

Best defences for critical sites and data centres

When it comes to security defences, organisations tend to still focus on central gateways and access points.

Smaller branches connect through them to customers and web services. Security defences include network controls (firewalls through to proxy technologies), access management technologies (identity access management and privileged access management) and into data and application controls. These controls are built upon centralising the technology because of the implicit trust of MPLS/Ethernet links.

Moving to a new world of virtual routers, firewalls, isolation tools – and the creation of virtual links between all of these – is a big shift from the traditional networking model. So you may need to rethink some of these security areas:

- **Policy enforcement** – security policy should be weaved into the overall fabric of your network policy design. It plays a bit part in routing decisions, application usage and network behaviour.
- **Device authentication** – you need to make sure that the right devices are connecting to the right part of the environment.
- **Access governance** – it's important to limit who can access what. Identity control needs to work at a local and global level, and you need to be able to specify people's access based on their role and location. Think about using privileged access management for critical services administration. You can combine it with multi-factor authentication to get the maximum flexibility.
- **Compliance** – you should define policies, data locations and allowable data usage to make sure you're following compliance across different geographies and vertical markets.
- **Detection** – if you're going to spot any unusual behavior quickly, you need a clear view of all your assets – it will help you sustain your defences.

Securing branch networks

Flexible branch environments need in-built security that can flex with their network technology and applications. All while staying compliant with local and global regulations.

- **Local internet breakout** – there are some pretty strong arguments for local internet break-out. But it's not without risk. It has the potential to increase your attack surface, making individual branches more vulnerable to data theft or the bypassing of controls.
- **Compliance** – it is really important to comply with all the relevant regulations. For example, many branches could process credit card transactions but the cost of implementing PCI DSS regulations at each branch could outweigh the benefits. When that happens, the use of encryption, and a good understanding of each stage of the processing, can make sure the right systems process and store the right data.
- **Multi-layer end point modules** – having a mix of corporate and guest devices on a flexible network can bring security risks. So it must be properly managed and maintained. But it can bring opportunity too. It can give you further layers of defence and analysis for behaviour and anomaly detection.
- **Responsive hosted defences** – defences that were once based at data centres, working inline, now need to be applied flexibly. Done properly, they can create both detection and defensive layers without slowing down the user's applications.

iii https://link.springer.com/article/10.1186/s13174-014-0015-z

Conclusion

Keeping systems, devices, users and data secure when new networking technologies are at force, means re-looking at security from a number of different angles. Some familiar – others not so.

With the right approach, skills and services, it's possible to tackle them holistically. A multi-layered approach to security, enhanced by intelligence and advanced data analytics, will allow you and your teams to be far more proactive. It's a crucial step that can make your organisation more agile and flexible, whilst protecting your data, assets and reputation. It gives you the freedom to grow and change while shielding you from the risks.

Security from BT – let us protect your business, the way we do ours.
We have operations in over 180 countries and support some of the world's largest companies, nation states and critical national infrastructures. This gives us a unique perspective on securing networks. Being on the front line means we see how and where cyber-attacks happen. We're constantly watching, learning, predicting and responding to the latest threats to protect our customers' businesses – and our own.

We know a security breach can destroy a reputation overnight. We also know security is the number-one digital enabler, allowing a business to run at speed and to build customer trust and investor confidence.

So we've built a team of 2,500 security experts in 14 global centres. The same people who protect our network also protect yours. This team uses unique tools and insight to stay one step ahead of criminal entrepreneurs.

As a global leader in managed security services, we're able to see the big picture. We can deliver a cohesive security capability as an integral part of our wider network solutions.

Issued: May 2018
Find out more at: www.bt.com/business/intelligentconnectivity
PHME: 82801

Offices worldwide

BT