Securing dynamic networks: a guide for CISO and CIOs

October 2017

93% say security is a ‘must have or should have’ for customers of SD-WAN technology, which increases to 97% for network function virtualisation.

Paul Crichard,

Chief Security Technology Officer, BT

His current role involves bringing together the technical capabilities around the BT technology stack and ensure they have a future, a development path and options for revolution as well as evolution.

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

After nine years in UK Government, have spent time as Head of Cyber Research for Raytheon and Head of Incident Response for Vodafone Group.

Overview: Security must keep pace with evolving networks.

As networks evolve, so must an organisations’ approach to security. Recent research conducted for BT by a leading analyst[i] found that security is the C-suite’s top consideration when looking at network services. But networks are changing as new ‘internet native’ applications and services drive demand for more bandwidth, performance and flexibility[ii]. New technologies such as software-defined wide area networks (SD-WAN), network function virtualisation (NFV), hybrid WAN and application performance management (APM) are able to meet these needs. And whilst these are delivering the desired flexibility and performance – they are also disrupting traditional notions of how to handle network security.

Digital transformation and the unstoppable growth in data volumes is prompting organisations to deploy these new networking technologies to push ever more business traffic over public Internet links and cellular networks, and thus outside of the boundaries of an organisation. The consequence is that the traditional security perimeter is disappearing and the resultant increasing Internet break-outs are multiplying the number of potential points of entry that hackers might exploit. It’s a complex, vulnerable environment, that’s both difficult and vital to protect.

Although MPLS and Ethernet services still have a very important part to play in the network landscape, the advent of these new technologies means that they need to be included in a wider networking, with the security strategy embedded within it, that incorporates local Internet breakout and cellular bandwidth provision.

This paper provides a summary of the key security considerations in this hybrid network landscape, as well as some suggestions as to how 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

The evolution of network technology is driving a parallel change in the role that security technology plays in this new virtualised environment.

Previously it was simple to design a network with the hardware and software applications in the data centre being the focus of the security defences. As software extends to start controlling the network it also needs to control the security as well.

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

Dynamic networking availability means that data destinations in a customer's network will be increasingly hosted on virtualised technology, which in turn means that the network security functions will also need to be virtualised so that they flex with the network. Any move to a virtualised environment needs to be as smooth and seamless as possible, as well as speedy and automated. Those service providers who can be trusted to deliver will be those who make these complex challenges seem simple. If things are made simple, organisations will quickly look to streamline or orchestrate a range of security services from basic service management through to full incident response and threat intelligence. For this full security technology and process life-cycle, which includes service initiation, system management, detection and response, to be successful, it has to be supported by skilled practitioners.

In the same way that network technologies are changing, the roles of different security technologies are becoming more blurred. This makes, it difficult for CISOs and CIOs to provide clear direction and strategy. The coming together of networking and security strategies and operations, together with the need for new skills within those teams, means that the CISO and CIO teams must align quickly to ensure joint success.

Securing a flexible, hybrid network

The following section takes a look at a few different ways in which the network is evolving.

It is essential in each case to evaluate the risk versus the threat in order to identify any new security considerations. It also allows us to better understand where traditional perimeter security controls may still be a valid option.

The growth in network traffic will accelerate the rate of adoption of various network services to augment core MPLS and Ethernet services. This increased diversity makes it hard to maintain the appropriate level of security required for any given service. A bigger, diverse network also introduces a lot more complexity to the data, making it harder to identify anomalous behaviour.

- **Detect new threats quickly** – use threat intelligence and horizon scanning to identify and address emergent threats before they can do serious harm. This includes providing clear and contextually aware information to those who can respond.
- **Secure, policy-based routing** – be sure to consider security end-to-end and deploy appropriate security measures. Ensuring that those controls are tailored for maturity, network pathways, application usage and data centre locations but with clear and flexible options.
- **Performance vs security** – the scaling of security devices, and their ability to adapt dynamically while the network and compute power are scaling accordingly.
- **New sources of data and response** – these new technologies bring a variety of new sources of data that can be used to detect threats. It also enables an advanced response by using the orchestrated capabilities across the environment. This includes understanding the underlying log systems, for example Amazon Web Services (AWS), to detect potential breaches in the fabric of the data centre and mitigate the 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

Today, many organisations' security defences are focused mainly 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.

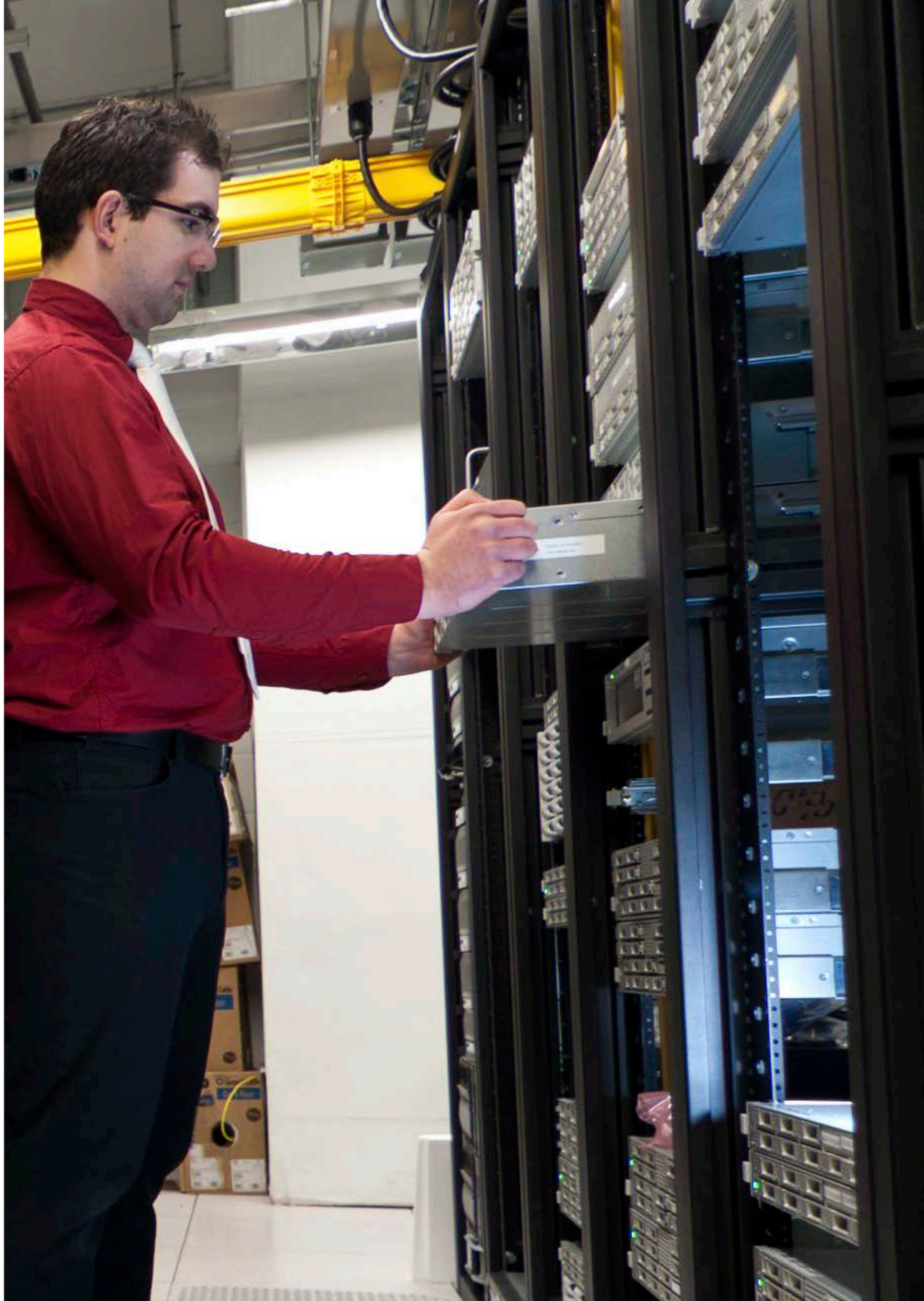
The evolution to a new world of virtual routers, firewalls, isolation tools and the creation of virtual links between all of these, represents a significant shift from that traditional networking model, and may require a rethink around some of the following security areas:

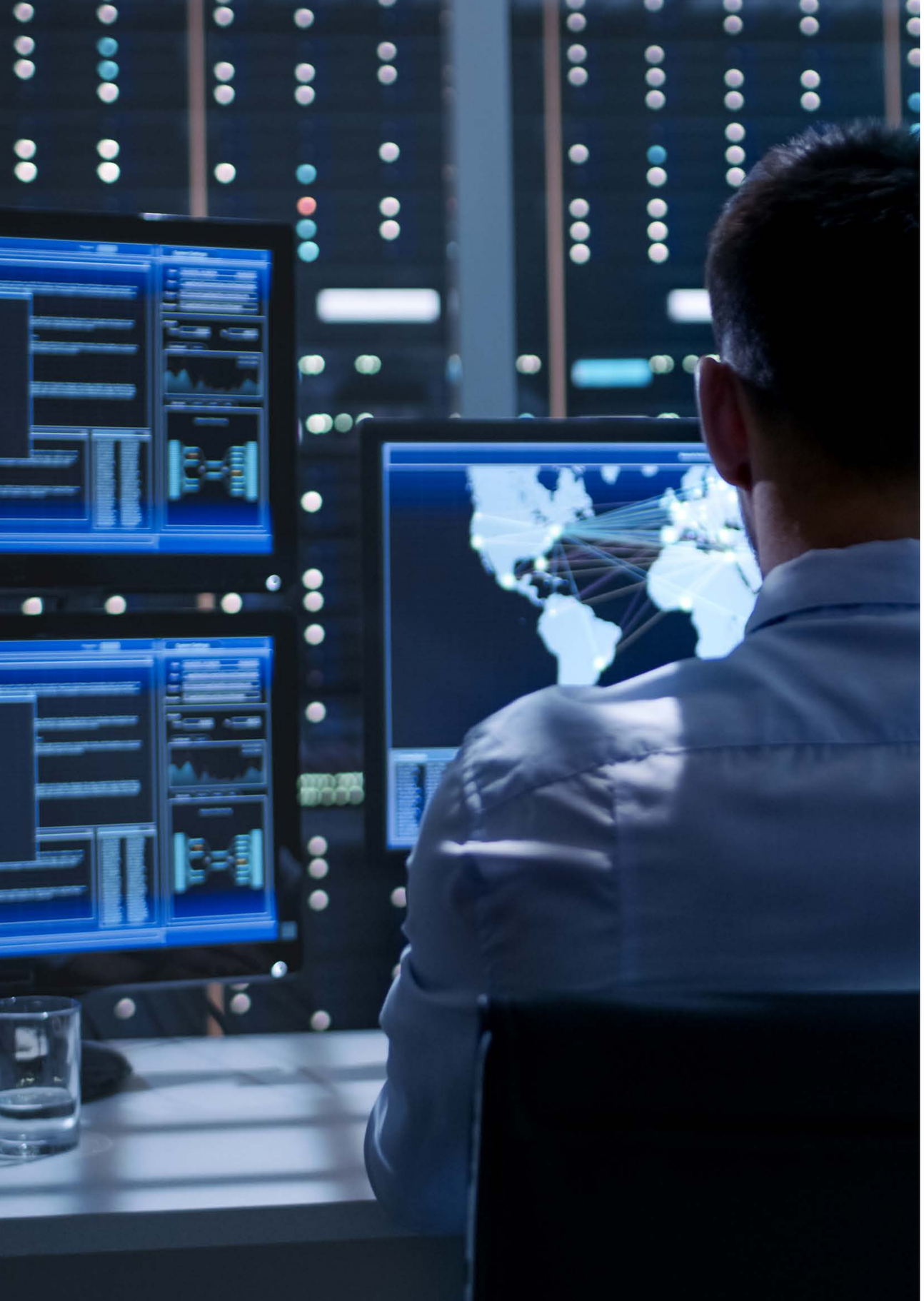
- **Policy enforcement** – security policy must be inherent in the overall fabric of network policy design as a cohesive part of routing decisions, application usage and network behaviour.
- **Device authentication** – ensure that the right devices are connecting to the right part of the environment.
- **Access governance** – identity control needs to work at a local and global level defining user access based on their role and location. Privileged access management should also be considered for critical services administration combined with multi-factor authentication for maximum flexibility.
- **Compliance** – assuring compliance across different geographies and vertical markets means policies, data locations and allowable data usage become important to define.
- **Detection** – having a coherent view of all assets to sustain defences and detect anomalies becomes more important than ever.

Securing branch networks

The flexible potential of branch environments requires cohesive security that is able to flex with the network technology and applications whilst remaining compliant with whatever local and global regulations apply.

- **Local internet breakout** – there are compelling business arguments for local internet break-out, but it also has the potential to greatly increase the attack surface, making individual branches more vulnerable to data theft or the bypassing of controls.
- **Compliance** – it is essential to ensure compliance with any pertinent regulations. For example, many branches could process credit card transactions but the cost of implementing PCI DSS regulations at each branch may well outweigh the benefits. In these circumstances the effective use of encryption and a good understanding of the role of each stage of the processing can ensure that the right systems process and store the right data.
- **Multi-layer end point modules** – endpoint security is a risk to and an opportunity for the flexible estate. The mix of endpoint devices in use, both corporate and guest devices, must be properly managed and maintained. However this provides the additional benefit of providing further layers of defence and analysis for behaviour and anomaly detection.
- **Responsive hosted defences** – those defences that previously worked inline, based at the data centres now need to be applied flexibly to create both detection and defensive layers without delaying the user's applications.





Conclusion

Safeguarding systems, devices, users and data in the context of these new networking technologies forces a re-look at security from a number of different angles, some familiar – others not so.

With the right approach, skills and services it is possible to tackle them holistically. A multi-layered orchestrated approach to security for protection and response, enhanced by intelligence and advanced data analytics will allow CIOs and CISOs to be far more proactive. This is a crucial step in giving a business the agility and flexibility it needs, while ensuring the protection of its data, assets and reputation, merging the ability to provide enhanced detection with business enablement.

Security from BT – let us protect your business, the way we do ours.

With operations in over 180 countries supporting some of the world's largest companies, nation states and critical national infrastructures, we have a unique perspective on securing networks. Our front-line position 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 and can deliver a cohesive security capability as an integral part of our wider network solutions.

Issued: October 2017
Find out more at: **BT.com**

Offices worldwide