Future security

How will we keep networks secure in the future?

Paul Crichard, Chief Technology Officer, BT Security
Ruth Davis, Head of Commercial Strategy and Public Policy, BT Security

Will an open network leave you open to trouble?

As businesses increasingly turn to technology to improve operations, margins, and people's experiences, we need to change how we think about cyber security.

Things used to be simple

As a CIO, you could rely on the fortress model of cyber security where multiprotocol label switching (MPLS) connectors 'locked down' a set secure pathway between processing and storage at different locations. But, as people can now connect to corporate resources through many different routes, that model no longer holds true.

- Businesses are taking on more mobile and remote workers.
- 93% of employers[1] allow 'Bring Your Own Device' (BYOD).
- The Internet of Things is gathering pace, connecting vast numbers of devices to a business network.
- More businesses are investing in cloud-hosted services than physical kit.

CIOs are investing in new network infrastructure, such as hybrid networks, cloud access, software-defined networks (SDN), and network functions virtualisation (NFV).

The new world of 'future networks' is fundamentally different to the old fortress model – it's borderless, which has deep implications for how you approach cyber security.

Because in a future network, there'll be lots more ways to connect to it. This compromises network security[2] because there are -

- More breakout points to the internet
- More devices connected to it
- Vastly more data stored within it and travelling across it
- Many more third-party cloud-hosted services and infrastructure

In such a complex, vulnerable environment, it's both difficult and costly to protect from a cyber-attack.

In such a broad, complex, and vulnerable environment, it is both difficult and expensive to protect your network from a cyber-attack.

Taking steps towards building a future security architecture

The new environment demands a new way of thinking about cyber security. The old fortress model – where threat control is concentrated on the perimeter and security is something you buy in separately – just won't cut it anymore.
You need to think security from the get-go, embedding it in every project that touches your network environment.

We can help you -

1

Stay secure as you switch to cloud-based services

2

Use big data to reveal hidden threats

3

Make sure you're compliant in a much more complex environment

[1] Checkpoint – "The Impact of Mobile devices on Information Security"

[2] As devices become easier to connect to the network, security often suffers. This is because of the race to bring connected products to market, the shrinking size of many devices, and manufacturers paying more attention to the user experience than network security.

Stay secure as you switch to cloud-based services

As you switch to cloud-based services, you'll need help staying secure.

You want employees to work together securely wherever they are, with whatever device they're using, and to have access to all systems at all times. You need to be confident that the data you're processing and storing in the cloud is secure.

You want to detect and neutralise threats before they cause any harm. And if you switch to cloud services, you need to make sure you're still complying with all the right regulations.

Extend network security controls over the cloud

You want your employees to be able to collaborate and access your cloud-based resources whenever they need to and from wherever they are.

Now – our Managed Cloud Security service scans all your inbound and outbound web and internet traffic, from everyone using your corporate network, in real-time. It detects, analyses, and blocks threats as they happen.

It's easy to use, too. You can access detailed reports and apply security policies across your entire network from a single web portal.

Future – software-defined networks (SDN) will change your security demands. Your security services supplier won't set the pace anymore – with the cloud, you'll get the security you need when you need it.

SDN will start by replicating the security controls that you use with your network today, including the ones for your on-site equipment. As you move to cloud-based services that do away with the need for this type of kit, your security services will seamlessly follow suit.

You want employees to be able to collaborate securely, from wherever they are and with whatever devices they're using.

Keeping your business online

A major threat to any internet-based service is a Distributed Denial of Service (DDoS) attack. A DDoS attack works by hitting a website with an overwhelming volume of bogus traffic, which causes the site to crash.

There's been a steep increase in the number and scale of these attacks as hackers take advantage of the growth in connected devices, many of which have limited – if any – security.

Now – Our Managed DDoS Mitigation service protects your IP address against the three main types of DDoS attack: volumetric, state exhaustion, and application layer, so you'll know your employees and customers will be able to access the infrastructure, applications, and data all the time.

Future – As SDN develops, DDoS protection services will cover far more than just your own network infrastructure. Security will start further out, at web access firewalls and at the network circuits themselves. This will alert you to potential attacks much earlier because your security will detect increases in traffic well before they reach you.

Making sure the right people can use what they need

People need to be able to access the applications and data they need, when they need it, wherever they are.

Now – our **Cloud Access Security Broker** (CASB) service sits between your on-premises infrastructure and your cloud provider's, extending the reach of your security polices across all of your cloud services, users, and devices. From a single, centralised control point, you can make sure that the right people have access to the right systems and data at the right time.

Future – the way you manage your users' security will need to change. Today, people access the network from laptops, tablets, and smartphones. These authenticate the user's identity and access permissions.

But as we start to access the network from different types of device (including the IoT), it becomes more complicated to identify who's who, and what permissions they have. As you get more access points, you'll need more sophisticated security options to keep tabs on how identities transfer between different applications.

For secure communications across an insecure network, you need a public key infrastructure (PKI) service to authenticate users, restrict access to confidential information, and verify who owns sensitive documents.

Now – as a **certification authority** we can issue, renew, and revoke digital certificates, keeping authentication and encryption strong, and digital signing secure. You'll know your users are who they say they are and that confidential information is only going to the people who are authorised to receive it.

Future – once your identity protection is in place, you can shift your focus to the actual applications that you're using. This starts with certificating the application (confirming the application's authority and interactions, possibly using blockchain verification) and – potentially – new devices that'll come on-stream in the future.

As a certification authority we can issue, renew, and revoke digital certificates for strong authentication, encryption, and secure digital signing.

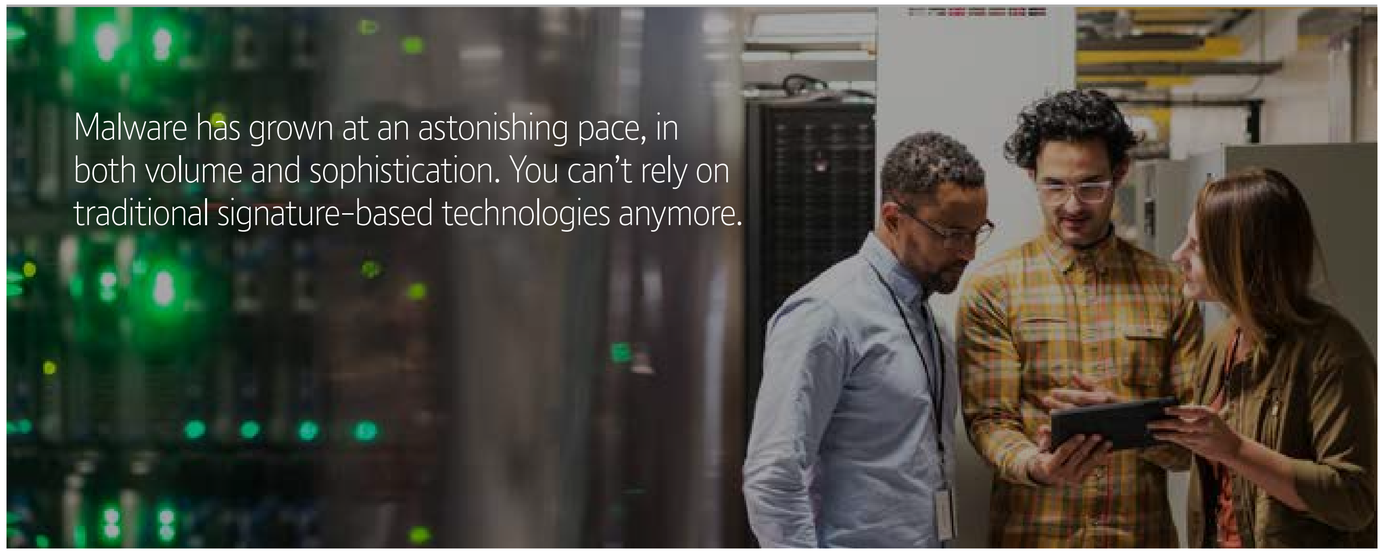
Nail down your endpoint device security

Every device that you add to your network (the 'endpoint' device) is a potential weak spot, especially ones that don't come with much security built in.

As we add more and more smart (and not-so-smart) devices, we need to make sure that our endpoint device security is watertight. It's not just about implementing security policies across all devices, it's also crucial that you can quarantine any suspicious devices away from the rest of the network until you've sorted out the problems.

Now – BT currently offers endpoint security endpoint protection and endpoint detection and remediation capability so that you can protect your fixed and mobile endpoints from emerging threats. We also offer network access control that ensures only trusted devices with the right set of privileges can connect to your network. As part of our broader portfolio we offer a wide range of enterprise mobility management and secure connectivity solutions as well.

Future – We will be adding capability to enable you to bring together threat telemetry from all of your endpoints, and feed this into your cyber security platforms. This means that you will be better able to detect and address emerging threats across your ever growing endpoint estate.



Malware has grown at an astonishing pace, in both volume and sophistication. You can't rely on traditional signature-based technologies anymore.

Use big data to reveal hidden threats

Although you now have much more data to protect, you can turn it into a strength by using the power of big data analytics.

The beauty of big data is that you can see patterns in your network analytics that you couldn't see before. This can help you pinpoint vulnerabilities that you didn't know existed. And when you're aware of the dangers to your network, you can make plans to defend against them.

We can help you:

Detect new threats quickly

Malware has grown in both volume and sophistication at an astonishing pace. It's no longer possible to rely on traditional signature-based technologies, which only detect malware that's already in use on the internet.

Now – using machine learning, our systems baseline 'normal' behaviour on your network and flag when anything falls outside that.

This highlights potentially suspicious behaviour (not detected by signature-based controls) to analysts. Supported by a range of security intelligence services, you can use this insight to defend against attacks before they happen.

Future – we use all available intelligence, analysis, and case studies to keep our services ahead of the global cyber threat.

By understanding abnormal traffic moving across carrier, mobile, and customer networks, we can see early warning signs of global threats, while automatically defending against threats at sector and local area-level. And the more info we get, the more we can standardise fast, automatic defence responses for both network devices and network perimeters (including IoT devices).

Minimise false alarms

Bigger networks invariably mean more security alerts. More endpoint devices, ditto. With the rapid increase in both threats and alerts, even the most experienced security analyst can find it difficult to sort the high-level threat from the low-level chaff.

That's why our Cyber Security Operations Centre (CSOC) blends machine-learning technology with the experience and insight of our analysts, to make sure we prioritise the right events.

And this reduction in false alarms across multiple networks brings a hidden bonus: less misconfigured networks, which were previously undetectable. And when you've spotted these low-level misconfigurations, you can do your housekeeping and help keep your network spick and span.

Keep scanning for vulnerabilities

Because it'll be relatively cheap and easy to change networks in the future, they'll always evolve and improve. That's a good thing. But the flipside is that new vulnerabilities will continue to pop up. So frequent vulnerability scanning is critical to a healthy network.

Now – our vulnerability scanning service brings our expertise to your scanning and reporting, and lets you integrate them with other BT Security Intelligence services.

Future – because we monitor threats from network provision through to the endpoint device for thousands of customers worldwide, we gather detailed intelligence on both attackers and researchers investigating new delivery mechanisms, and command and control tools. This early insight helps us keep ahead of the shady world of vulnerability exploitation

Horizon scanning

This is about looking now for potential future threats and understanding the implications of them on your organisation. Our Security Intelligence services scour the global network, open source intelligence feeds, and even criminal market places to identify upcoming threats. With the flexible nature of future networks, you need to keep an eye on how your vulnerability changes as you develop your network.

Incident response

You need to plan for security incidents. This might include attack simulation, where your organisation is attacked under controlled conditions so you can understand the likely effects and plan to mitigate them.

We draw on our own experience as a target, battling over 4000 attacks a day.

As a global organisation with security at its core, we lead the market in our ability to detect, respond, and defend against today and tomorrow's attackers. We know how to protect our reputation against the attacks we experience ourselves. And we provide security services to 170 enterprises and government organisations in 180 countries. Our frontline position gives us a unique insight into the global threat landscape.

Trust us to keep you compliant

You're facing a perfect storm of increasingly complex digital architecture and a raft of legislation, frameworks, and standards —

- The new General Data Protection Regulations (GDPR)
- The Network and Information Security Directive (NISD) from the European Union
- The Payment Card Industry Data Security Standard (PCI-DSS)
- International standards ISO27000
- National Institutes of Standards and Technology (NIST) framework
- SysAdmin, Audit, Network and Security (SANS)

As you adopt new network technology and ways of working you need to be confident you're staying compliant and mitigating security risks.

You need a partner you can trust. Our Security Consulting practice can help you with -

Governance, risk, and compliance

We'll run a 'maturity assessment' to benchmark your current security position against regulations or standards, such as GDPR or ISO27000. We'll then do a gap analysis to identify where you fall short, helping you get up to scratch in line with your budget and needs.

Cloud security consulting

Your journey to the cloud is safe with us. We'll make sure you're using the policies, controls, and technologies you need to protect customer data as you migrate your business to the cloud.

Data security consulting

We'll work with you to devise end-to-end security solutions to protect both your data and the data you hold on your customers. We can also help you with data classification, encryption, and data loss prevention.

You're facing a perfect storm of increasingly complex digital architecture and a raft of new legislation focused on network and data protection.

What are the benefits to your business?

As well as making your business more secure, integrating security into your network architecture can bring -

- Higher security, more business – it sounds obvious but it's worth stating here: if your people trust that this new, cloud-based technology is safe and secure, there're more likely to embrace it and all the transformative possibilities it brings.
- Faster internet, less bandwidth – your mobile or distributed users can access the internet directly, without you having to 'back haul' internet traffic through your internal network and its perimeter security appliances. People will find the internet easier to use, and you'll save on bandwidth costs.
- Less fuss, less cost – because managing your entire security policy and reporting is simple. A single web portal covers your entire network estate.
- It's easier to optimise your network when you can see it all – a single security portal gives you a view of the entire network, not just security. See what's underperforming and then fix it.
- Safeguard the reputation of your business - your reputation is invaluable. A secure business stays up and running, keeps customers happy, keeps their data safe, and is compliant with all regulations and security standards.
- More productive security team - your security team will be able to prioritise workloads and get ahead on problem areas in the network.
- Easy access to technical skills – our people are experts so you don't have to be. If you need to get hold of otherwise expensive expertise, you can speak to our Cyber SOC team.

Why BT?

We'll make sure your journey to the cloud is safe – and you can deliver security services from it once you're there.

- It's safer to adopt cloud services
  Our cloud security architecture is integrated with our Managed Security Service.
- Your network will come with security built-in
  We embed virtual security as standard into our dynamic network services.
- You'll stay compliant, even in the cloud
  We'll help you decide the best way to move to the cloud and still stick to the rules.
- It's easy to make the jump
  We have a tried-and-tested process for getting networks up and running in the cloud.
- We use global data to protect you
  Our big data gives us a unique insight into the threats facing thousands of global customers. As soon as we see a threat to one customer, we can defend all customers against it.
- We keep things consistent
  We've rolled out a standard operating model of cyber SOC capabilities to work on all our technology.
- We keep you updated
  With Security Threat Monitoring, you'll get a clear picture of threats.
- We move fast
  Our Cyber Assessment Lab assess all new security technology within six months of it coming to market, so we can make sure we're always supplying you with the world's leading security solutions.
- We've got the tools to spot threats
  Our advanced data analytics and new deception technology shows up insider threats and intruders.

We are on the front line of cyber security

Protecting organisations in more than

180

countries

A unique insight into the global threat landscape

We've been protecting data since Tommy Flowers invented Colossus in the 1940s

Defending BT against

4,000

cyber-attacks a day

Find out more at **bt.com**

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract. © British Telecommunications plc 2017. Registered office: 81 Newgate Street, London EC1A 7AJ. Registered in England No: 1800000