Cyber-attacks aren't going away. Help protect your business with BTnet Security.

BTnet. Dedicated internet access.

We know that when it comes to protecting your most valuable network assets, you need a security provider you can trust. So don't just hand your security over to anyone, leave it to us.

We've teamed up with Cisco to offer BTnet customers, who take our Cisco Meraki managed equipment option, a Unified Threat Management service. For that, you'll get a firewall, Advanced Malware Protection, content (URL) filtering, and intrusion detection and prevention, all in one box.

Because it uses the same support teams, contracts, and billing as BTnet, it's remarkably easy to manage. There are no upfront costs, no more equipment to find a home for, just a fully-integrated security service for a fixed monthly charge.

New cyber threats appear every day, so we help make sure you're always protected by regularly updating your service with security patches. And because we look after everything for you, you don't need any specialist IT knowledge or IT resource.

Powered by Cisco security

Cisco runs the industry-leading threat intelligence organisation, Talos.

The team of world-class researchers, analysts, and engineers collect and scrutinise information about existing and developing threats and use that insight to help protect you against attacks and malware. Our continual service updates are seamless; you won't even notice that you're being safeguarded from the ever growing threat landscape.

- 250+ full-time threat researchers work to keep your business safe.
- 1100+ decoy systems and other threat traps help us stay ahead of the cyber-criminal.
- Millions of malware sample comparisons every day weed out patterns to help identify new threats.

Firewall, your first line of defence

Your firewall builds a barrier between your secure internal network and untrusted external networks like the internet.

When you're defending your business, you can't rely on a run-of-the-mill firewall to do the job: you need a next-generation firewall with application control.

We've teamed up with Cisco to bring you a firewall that gives you control over your connectivity to the internet and cloud. The Layer 3 firewall helps control your traffic while the Layer 7 blocks specific web-based services, websites, and applications.

Starting with our default Layer 7 firewall policies template, we'll block all peer-to-peer (P2P) traffic and web file sharing at Layer 7 (you can add and remove categories whenever you want).

Security eye-opener

According to research by IT security consultants Webroot, more than **60 per cent of companies have already been hit by ransomware attacks**.

Source: Webroot Quarterly Threat Trends, June 2017

Advanced Malware Protection

Malware covers a whole load of bad stuff: computer viruses, ransomware, Trojan horses, spyware, adware, worms and more.

BTnet Security includes Advanced Malware Protection powered by Cisco AMP, one of the industry's leading malware protection solutions, analysing 1.5 million samples a day. Including global threat intelligence and malware-blocking to prevent breaches, AMP analyses files at point-of-entry to catch known malware.

The result? We detect threats faster so you're automatically protected.

Cisco AMP at a glance

- Detects cyber-attacks over 600 times faster than the industry standard.
- Time to detection: 3.5 hours average, compared with industry average of 100 days.

Source: 2017 Annual Cybersecurity Report

Content (URL) filtering

Protecting your business isn't just about controlling traffic on the network. It's also about protecting your reputation and keeping your employees safe.

Content (or URL) filtering allows you to block over 70 categories of websites including pornographic, racist and hate sites, peer-to-peer (P2P), parked domains, adware, and so on. You can also control access to social media.

Our content filtering system uses Webroot BrightCloud®. It's a constantly updated URL categorisation database that meets CIPA (Children's Internet Protection Act) and IWF (Internet Watch Foundation) standards.

You can customise your categories as well as blocking or allowing (black/whitelisting) individual websites. We'll start you off with a template that blocks some common categories so your service is ready from the get-go.

Intrusion detection and prevention

New threats appear every day. In a world where the cyber-criminal never sleeps, you need security that's always wide awake.

BTnet Security includes an intrusion prevention system (IPS) powered by the Cisco Sourcefire SNORT® engine, which is fully integrated into the Cisco Meraki equipment provided with your BTnet internet service.

SNORT identifies traffic patterns in real-time, creating rulesets. By comparing known threat signatures against a specified ruleset, intrusion prevention automatically blocks traffic that it identifies as malicious. Using the cloud, Sourcefire refreshes the rulesets automatically so you're always protected against the latest vulnerabilities, including exploits, viruses, rootkits, and more.

Intrusion prevention: the balanced ruleset

Our balanced ruleset counters vulnerabilities with a CVSS (Common Vulnerability Scoring System) score of 9+ in these categories:

- Malware-CNC: known malicious command and control (CNC) activity for identified botnet traffic (including call home, downloading of dropped files, and ex-filtration of data).
- Blacklist: URLs, user agents, DNS hostnames, and IP addresses suspected to be indicators of malicious activity.
- SQL Injection and exploit-kit: detection of SQL Injection attempts and exploit-kit activity.
- Whitelist: you can add these whenever you want.

Real threats: the WannaCry attack

Remember the WannaCry ransomware attack of 2017?

Computers worldwide were suddenly unusable as WannaCry locked or encrypted data, pending the payment of a Bitcoin ransom.

Why were so many organisations caught with their cyber-pants down? They hadn't kept their security up to date.

Cisco's Talos team used SNORT to detect and protect against WannaCry quickly. Through real-time traffic analysis and packet logging, they spotted the WannaCry signatures. After adding them to the SNORT database, the Cisco team used cloud technology to protect all Cisco Meraki kit users who'd enabled 'Intrusion Prevention'.

One simple precaution that could have helped save a whole load of trouble.

Cloud management

Cisco Meraki cloud management is compliant with the highest independent, industry-recognised standards: SSAE16; ISAE 3402 (SAS-70), including Type 11; ISO 27001; SOC1; and SOC2.

Cyber-threats are real and never-ending

If you don't want to get burned, don't put security decisions on the backburner. Visit **bt.com/btnet** today.

BTnet Security is only available for customers who have a BTnet internet access service with our Cisco Meraki Managed equipment option.

You can find full terms and conditions for the BTnet Security service at bt.com/terms (in the 'Broadband and internet access' section). If you would like to see a full service description, just ask for a copy when you call us.

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.

October 2018