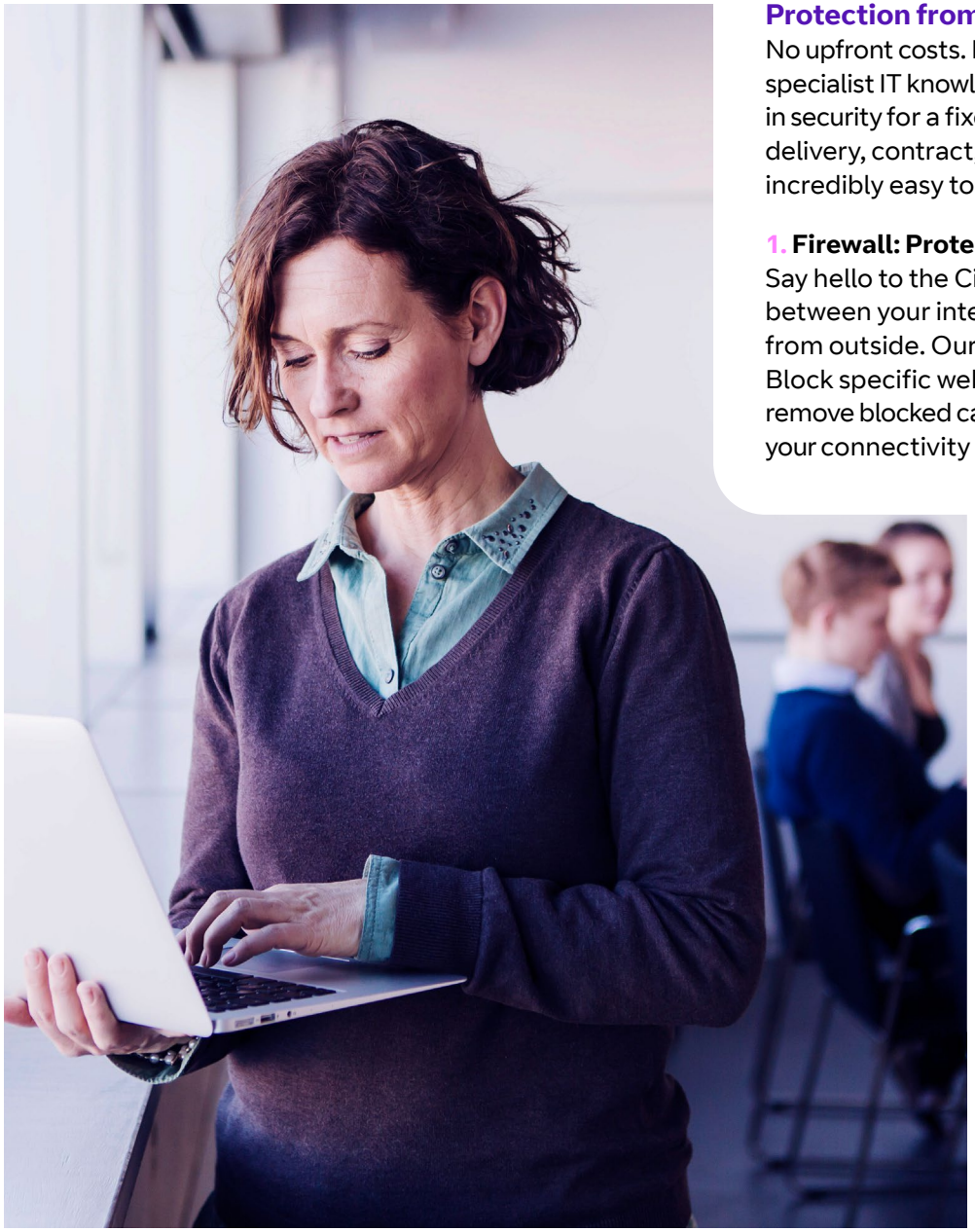
Security that packs a powerful punch

Spot and stop cyberthreats in their tracks with BTnet Security

Hackers attack every 39 seconds

That's an average of 2,244 times a day.[1] As well as the obvious disruption they cause, the time it takes to manage these attacks can put a huge drain on company time and resources.

Let BTnet Security protect your business, data, colleagues and customers. More specifically, BTnet with our Cisco Meraki managed equipment and built-in security. It goes way beyond a basic firewall. It powers up your connectivity. It comes with Unified Threat Management (UTM), which shields you from cyberattacks. It updates automatically, keeping your business on top of emerging threats. And it's plug-and-play, so you can start protecting your organisation straight away without spending hours setting up. You'll be free to focus on your business, embrace new technologies, and stand up to cybercriminals.



Protection from every kind of threat

No upfront costs. No separate hefty equipment. No need for specialist IT knowledge or resources. Just four layers of built-in security for a fixed monthly charge. And with the same delivery, contract, billing and support team as BTnet, it's incredibly easy to manage.

1. **Firewall: Protect your network. Control your traffic.**
Say hello to the Cisco firewall. Your first line of defence between your internal network and anything coming at it from outside. Our Layer 7 firewall lets you control traffic. Block specific web-based services and applications. Add or remove blocked categories at any time. Get total control over your connectivity to the internet and cloud.

2. **Advanced Malware Protection: Detect cyberattacks, fast.**
Computer viruses. Ransomware. Trojan horses. Spyware, adware, worms. The list of malware threats goes on. BTnet Security works with specialist malware partner Cisco AMP. AMP uses global threat intelligence and malware, analysing and blocking 1.5 million samples a day. It detects cyberattacks over 600 times faster than the industry standard[2]. That's within 3.5 hours, compared to an industry average of 100 days. With this kind of super-speed, you'll be protected before trouble's even begun.

3. **Content (URL) filtering: Protect your people**

It's one thing to face an attack on your business, but quite another when it impacts on the lives of your people. Our content (or URL) filtering lets you block over 70 categories of websites. Pornographic. Racist and hate sites. Peer-to-peer (P2P), parked domains adware. Even access to social media. It's ready from the get-go. It's constantly updated. It meets the highest standards. So you can customise categories, block or allow individual websites, and let your employees work without fear of compromise.

4. **Intrusion detection and prevention: Stay alert**

Cybercrime never stops, so you need security that's always on. The Cisco Meraki equipment has a built-in intrusion prevention system (IPS). It identifies traffic patterns in real time. It automatically blocks anything seen as malicious. And it constantly refreshes. So your network is secure against the latest threats, day and night.

Five reasons to trust Cisco

1. It runs the industry-leading threat intelligence organisation, Talos.
2. It employs 250+ full-time threat researchers.
3. It uses 1100+ decoy systems and other threat traps.
4. It makes millions of malware sample comparisons every day, weeding out patterns and identifying new threats.
5. Its continual updates are seamless; you won't even know they're happening.

Cisco in action

Do you remember the WannaCry ransomware attack of 2017? Computers worldwide were brought to a standstill, pending the payment of a Bitcoin ransom. 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. Then they used cloud technology to protect all Cisco Meraki kit users who'd enabled 'Intrusion Prevention'.

It's a lesson for us all. Keep your security up to date, and you won't get caught out.

Cybersecurity. It's all in the details.

Defence	System
Firewall	Layer 3 (to control traffic) and Layer 7 (to block specific services and applications). You'll start with our default Layer 7 firewall policies template. We'll block all peer-to-peer (P2P) traffic and webfile sharing at Layer 7. You can add and remove categories whenever you want.
Advanced Malware Protection	Cisco AMP. Enabled by default.
Content (URL) filtering	Webroot BrightCloud®. It meets CIPA (Children's Internet Protection Act) and IWF (Internet Watch Foundation) standards. Blocks a range of website categories with our standard template. It can be easily customised and updated.
Intrusion detection and prevention	Cisco Sourcefire SNORT®. Enabled by default. Looks at traffic patterns in real-time and creates rulesets, then compares them to threats. It will automatically block anything identified as malicious. Our rulesets look at vulnerabilities with a CVSS (Common Vulnerability Scoring System) score of 9+ in the following 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.
Cisco Meraki Cloud Management	Compliant with SSAE16; ISAE 3402 (SAS-70), including Type 11; ISO 27001; SOC1; and SOC2.

1 Source: University of Maryland. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds. 2 Source: 2017 Annual Cybersecurity Report.

How to get in touch

Cybercrime never stops evolving. Choose security that responds to changing threats,and get more protected every day. 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

August 2020