Secure every connection while cutting cost and complexity

Today's agile working means your traditional security perimeter is no longer a fixed, well-defined boundary. Many organisations have critical gaps in protecting their infrastructure, including branch locations and remote employees when they connect to the internet – and it's these weak points that hackers target.

Our Managed Cloud Security service provides real-time scanning and control of your users' web traffic, including those within the corporate network as well as remote and distributed workers.

As a cloud-based service, you don't have to buy or maintain any hardware, or be concerned about managing software licences. You just choose what security features you need, either as standalone items or as bundled packages, depending on the issue or security concern you want to address.

A consistent, global standard
By using a single central portal you can easily manage internet policies and reporting for all global users and sites. This helps to enforce consistent protection and policy across all users in your organisation.

We've partnered with leading providers of cloud security solutions, such as Zscaler and Cisco, to provide our Managed Cloud Security service.

Managed Cloud Security provides an internet security platform with services that scan and filter your network traffic, including SSL-encrypted sessions, as it passes to and from the internet. Optionally, you can select the types of traffic that you don't want to inspect – such as financial or healthcare connections – to maintain privacy.

The benefits of a consistent cloud-based security set-up

Effective, up-to-date defence
Full protection against threats with real-time scanning of user's web traffic, blocking known and zero-day threats before they reach your network.

Reduce cost and management
No upfront hardware costs or ongoing maintenance to pay. Manage security policy across multiple sites through a single centralised portal.

Extend current investments
Complements existing firewalls and extends the value of existing investments whilst providing additional protection to all users.

Protect your reputation and data
Block access to websites that contain inappropriate content in line with your usage policy. Helps to protect against data loss by intercepting traffic bound for suspicious internet destinations.

Stay in control
Define your web access policy rules and permissions for all global users and applications and apply changes in real-time.

Fill web security gaps and protect all users
Ensure consistent protection and policy for all users, both inside and outside the network.

BT

A smarter way to stay secure

Fast and reliable cloud infrastructure
- Global security nodes provide minimal latency when accessing cloud based applications, eliminating the need to reroute traffic via a central datacentre.

Web filtering
- Permit access to appropriate applications and content while preventing access to those that might increase risk, drain productivity, or lead to a potential loss of confidential information
- Reduce bandwidth congestion
- Ensure confidentiality by masking sites that collect information
- Discover, monitor, protect and control cloud application usage across the organisation.

Web security
- Proactively block known threats to stop them before they enter your corporate network
- Defend against the unknown "zero-day" threats using file reputation and sandboxing technology
- Identify and execute suspicious objects for analysis of malicious behaviour
- Provide secure web access to corporate users, branch offices, mobile and roaming users and guest Wi-Fi users.

Advanced persistent threat (APT) detection
- Reduce time for discovery, downtime and remediation of infected desktops by actively and continuously monitoring for threats that have penetrated your defences.

Mobile security
- Secure your users in any location
- Protect against browser based threats like phishing and spyware and also from malicious apps.

Access to cloud security experts
- We have a team of people with in-depth cloud security knowledge here to help you.

Cloud Connect Internet Gateway and Zscaler
- Cloud Connect Internet Gateway supports connectivity to Zscaler via Generic Routing Encapsulation (GRE) secure tunnels. This provides essential resilience if you use Zscaler's recommended GRE connection option
- You get two GRE tunnels per customer gateway to your choice of Zscaler locations. So if the primary Zscaler node is taken down for maintenance, or there's a failure in the route, traffic is directed to the secondary Zscaler node.

Why choose BT?

We're at the front line of cyber security: supporting customers in over 180 countries across the world. Operating globally – delivering locally.

We have 3000 security experts and 15 Security Operations Centres (SOCs) across the world – the same people who protect our business, also protect yours.

We have a team of highly skilled security consultants with a solid expertise in cloud security and every other security discipline. And we can offer one of the best global cloud infrastructure coverages in the world, with more BT data centres enabled for cloud services than any other service provider.

We're in a unique position and can seamlessly integrate our security offers with your BT provided WAN and LAN solutions for an unmatched one stop-shop experience for customers.

What could Managed Cloud Security do for you?
Visit bt.com/globalservices