

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' 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, including Zscaler, Netskope, Palo Alto Networks, and Cisco, to ensure you have choice of strategy and current investments.

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.

Managed Cloud Security Zscaler enhanced by Eagle-i

Our transformational cyber defence platform for detecting and responding to cyber threats is now enhancing our Managed Cloud Security Zscaler service. If Zscaler identifies suspicious traffic, for example an attempt to connect to a command and control server, this will of course be blocked. However, it is important to quickly assess and manage the resulting risk of malware spreading laterally across the organisation, infecting other devices within your estate.

Eagle-i will review incoming alerts against our extensive threat intelligence database, notify you of the event, and – using our experience managing threats across multiple customer environments – recommend appropriate courses of action.

Depending on your service level we can even automate that response across different security controls to limit the opportunity for malware to spread, reducing the time and cost of recovery and the overall impact to your organisation.

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.

Digital Experience Monitoring (DEM)

Vendor-specific offering which provides organisations with telemetry, analytics and dashboards to understand performance and determine if user experience is affected by end point, network or application for any user, any device, anywhere.

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 data centre.

Features of Managed Cloud Security

Secure Web Gateway

Establish proxy-based visibility and control over web traffic with deep awareness of cloud activity and data interactions in transit.

DNS (Domain Name System) Security

Mitigate attacks perpetuated through DNS infrastructure.

Cloud Access Security Broker (CASB)

Monitor and secure cloud service usage by employees to quickly identify and remediate threats.

Data Loss Prevention for Endpoint (DLP)

Deliver comprehensive data protection at all points of potential compromise from an endpoint device.

Firewall in the cloud

Provide the foundation for consistent cloud-delivered security for all users and locations with a next-generation firewall in the cloud.

Why work with us?

Partnerships that create value

We have well established relationships with multiple vendors, providing a breadth and depth of security services. Our solution is created by combining our managed service wrap with the industry's top technology partners for Managed Cloud Security- Zscaler, Palo (Prisma), Netskope, Cisco, and Skyhigh.

Accredited professionals

Our accredited experts will manage the design, set-up, deployment and management of the service to ensure your segmentation policies are implemented successfully.

Trusted global partner

We're positioned as a leader in the IDC MarketScape European Managed Security Services 2022 vendor assessment.

What could Managed Cloud Security do for you? [Visit bt.com](https://www.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 2024 Registered office: One Braham, Braham Street, London, England E1 8EE. Registered in England No. 1800000

JN: 1441114433 | May 2024