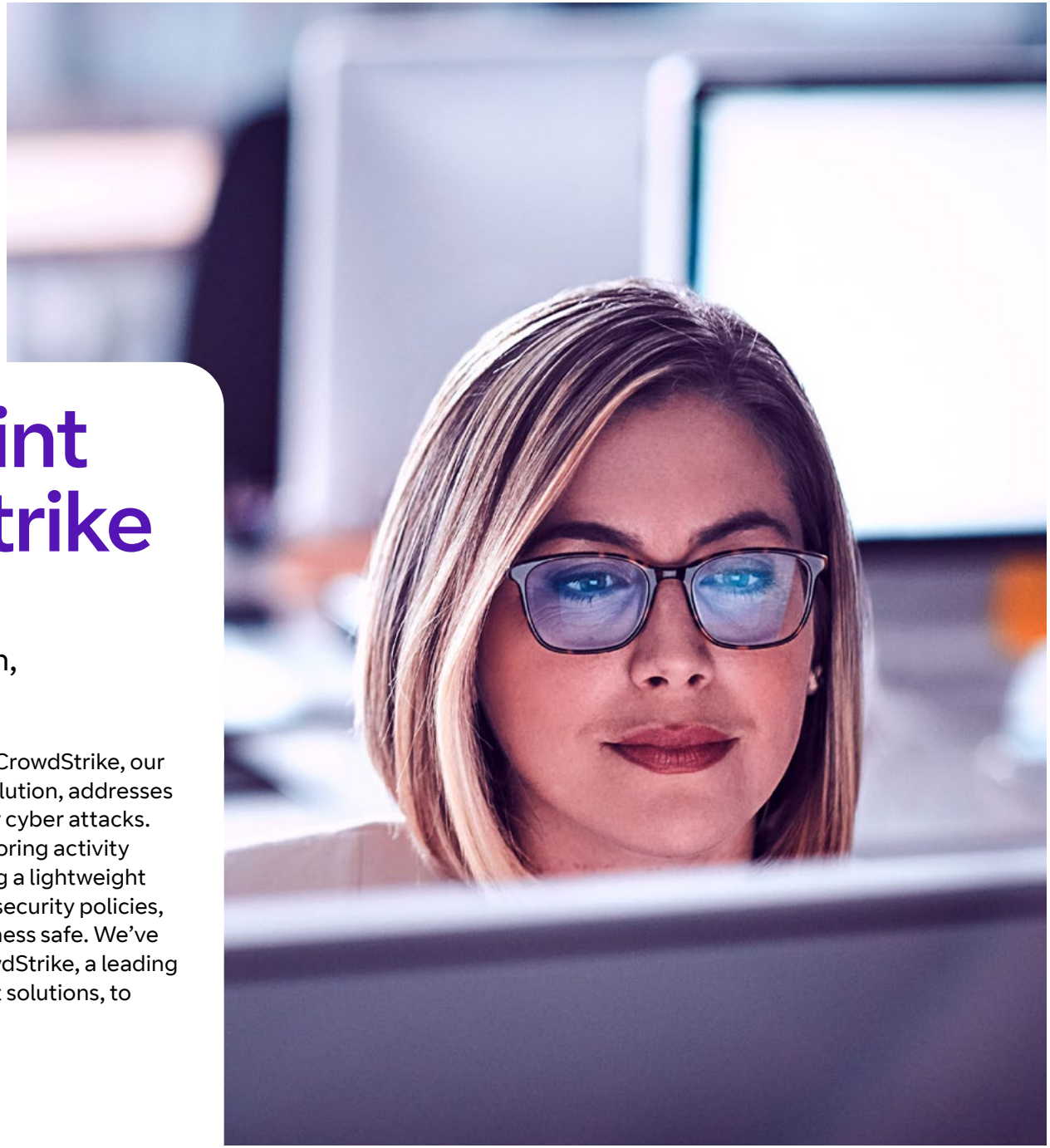
Managed Endpoint Security CrowdStrike

Managed Endpoint Security CrowdStrike

A fully comprehensive solution for endpoint protection, providing best-in-class prevention, detection, and response capabilities.

The constant evolution of IT environments means attackers are using more and more sophisticated methods to infiltrate networks, with the endpoint being your last line of defence. As ransomware attacks rise, organisations are becoming more concerned about cyber damage and disruption. The expanding use of ‘file-less’ and stealthy infiltration, combined with ‘living off the land’ (using common IT tools for attacks), threatens the confidentiality, integrity and availability of endpoint assets.

Managed Endpoint CrowdStrike, our endpoint security solution, addresses the threats posed by cyber attacks. By constantly monitoring activity at the endpoint using a lightweight agent and applying security policies, we’ll keep your business safe. We’ve partnered with CrowdStrike, a leading provider of endpoint solutions, to deliver this service.



Protects you from threats

By outsourcing your security monitoring to us, you're putting your endpoints in safe hands. Our team of certified security analysts will be keeping watch over your business' security 24/7, in real time. Our world-class SOC will be continually monitoring your endpoints, analysing and alerting you to any threats, and making sure that you're free to focus on what really matters to your business. We provide a wealth of security experience, and we'll treat your business as if it were our own.

You can deploy the CrowdStrike Falcon agent on endpoints in any location, which means we can protect them wherever they are in the world. Managed Endpoint CrowdStrike offers high-level protection through a combination of machine learning and behavioural detection at cloud scale, supported by 24/7 threat hunting, to prevent more than 41,000 potential breaches annually, worldwide.

Simple and scalable cloud-based solution

Our Managed Endpoint Security is based on CrowdStrike's Falcon technology. CrowdStrike is the world's first cloud-native endpoint protection platform and needs no on-site infrastructure. This means you can deploy it rapidly, onto tens of thousands of endpoints in less than a single day. The cloud-native nature of CrowdStrike allows for effortless scalability without costly upgrades or migration onto your networks.

Zero impact on the endpoint

CrowdStrike is powered by a single, lightweight agent that provides everything you need to stop breaches, with maximum effectiveness from day one. This lightweight agent works everywhere, including on virtual machines and in data centres – providing protection even when endpoints are offline. It carries out searches without any performance impact on endpoints or the network.

A smarter, simpler way to manage endpoint security

- Get more accurate, intelligent and faster insights with AI-guided security management from a single cloud-based dashboard.
- Manage complete endpoint security from a single cloud console to reduce complexity.
- Get rapid updates through a 'single agent' architecture simplified design.
- Eliminate routine tasks and improve endpoint security decisions, through simplified workflows with context-aware recommendations.
- Our solution uses Autonomous Security Management to learn from admins, organisations, and the security community.

Detect a wider range of threats and snuff out any danger

Our endpoint security solution includes Advanced Machine Language (AML) to detect new and evolving threats before they can affect you. It constantly monitors and instantly blocks files that behave suspiciously. And by using Memory Exploit Mitigation, it can block zero-day exploits against vulnerabilities in popular software.

Key Features

Next generation antivirus
Protects against both malware and malware-free attacks. Benefits from machine learning to block known and unknown malware, and provides protection even when devices are offline.

Block ransomware
Indicators of Attack prevent sophisticated file-less and malware-free attacks , before they do damage.

Behavioural analytics
Combines the latest machine learning and behavioural analysis with integrated web protection technologies, to prevent malware, spyware and ransomware attacks in real time.

Endpoint detection and response
Delivers continuous, comprehensive endpoint visibility that spans detection, response and forensics to ensure you miss nothing and stop all potential breaches.

IT integration
EDR integrates with leading Security Information and Event Management systems (SIEMs), orchestration and automation, and ticketing systems.

Application and device control
Controls file, registry, and device access and behaviour; also offers whitelisting and blacklisting.

Proactive threat hunting, 24/7
Provides 24x7x365 threat hunting that goes beyond the passive automated detection offered by current security technologies. Focused on detecting threats that have bypassed other controls.

Prioritisation
Pinpoints the most urgent threats in your environment and resolves false positives.

USB device control
Provides admins with full control of the USB devices in use in their environment, and reduces the risks associated with those devices.

Endpoint integration
Provides attack attribution and identification of unique adversary TTPs (tactics, techniques and procedures).

Real-time and historical search
One-click visibility of current and historic (up to 90 days) endpoint activity across your entire environment.

Record everything
Continuous monitoring across all major platforms (Windows, Linux, Mac) and full cloud recall of events without scanning.

Real-time response and containment
The solution's cloud-based architecture allows you to get answers in seconds without putting any stress on your endpoints.

Application usage
Real-time application inventory of all applications in the environment. Identifies which applications are in use in your environment, who is using them, and how often they're being used.

Why work with us?

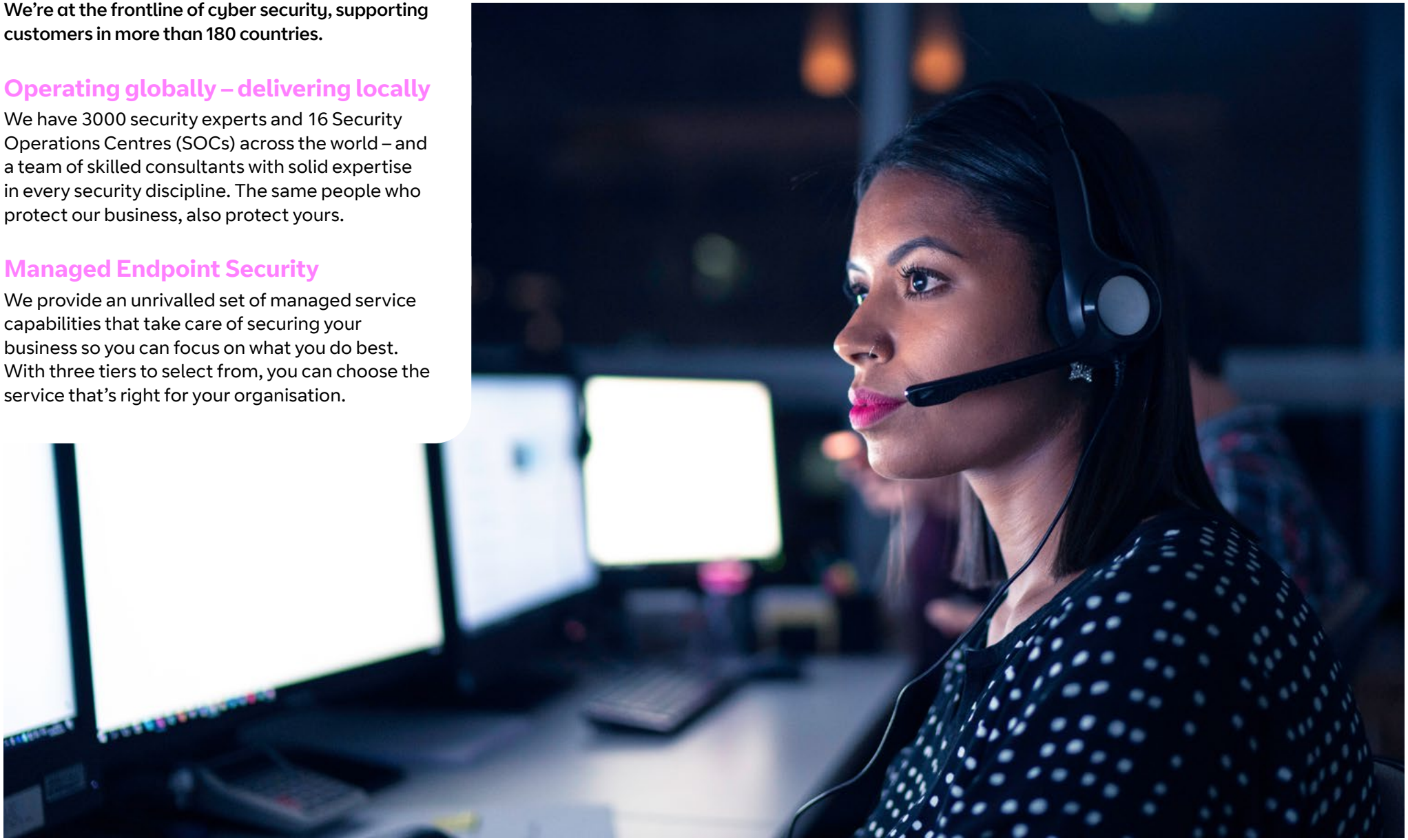
We're at the frontline of cyber security, supporting customers in more than 180 countries.

Operating globally – delivering locally

We have 3000 security experts and 16 Security Operations Centres (SOCs) across the world – and a team of skilled consultants with solid expertise in every security discipline. The same people who protect our business, also protect yours.

Managed Endpoint Security

We provide an unrivalled set of managed service capabilities that take care of securing your business so you can focus on what you do best. With three tiers to select from, you can choose the service that's right for your organisation.



What could Managed Endpoint Security do for you?

Find out.
Visit bt.com/threatdetection

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 2021. Registered office: 81 Newgate Street, London EC1A 7AJ. Registered in England No. 1800000.

May 2021