Multiple, siloed security controls can miss sophisticated threats and create alert fatigue. Are your security tools working in harmony?

With Managed CrowdStrike Falcon® Extended Detection and Response (XDR), we can provide complete visibility of threats across your security estate, improving threat detection and accelerating response and remediation.

With the acceleration of digitisation, companies tend to increase security tools to combat any potential new threats across their estate. CrowdStrike has found that the average enterprise organisation has 45 security tools deployed and active[1].

This has fixed one problem but caused others. Security architectures have become more complex and harder to manage. Cyber security teams are experiencing alert fatigue and threats are being missed due to the difficulty of correlating findings across tools.

All security tools need to be managed properly, with alerts triaged, and incidents investigated and remediated – all of which requires more skilled cyber security resources, which can be hard to find.

77% of security experts agree that detection & response is becoming more difficult[2]

Our solution – Managed CrowdStrike Falcon XDR

Working in partnership with CrowdStrike, our managed service will improve your security posture and help tackle these challenges. Our team of cyber security experts will set up, monitor and analyse security alerts across your key assets 24/7, responding to threats quickly – minimising the risk to your business. And we'll continue to manage and maintain the Falcon platform, optimising your service to lower your cyber risk.

Benefits of Managed CrowdStrike Falcon XDR

Speed up your response – with our service you can improve the efficiency and speed of your team by only responding to real threats that we've detected and investigated.

Reduce missed threats – siloed products can lead to threats being missed. We'll configure the platform and its components to ensure real threats are detected.

Relieve the pressure on your team – it's hard to find and retain experts. Our experts will setup and manage the service and they'll take care of detection and response so your team can focus on critical tasks.

Reduce the cost of security – by consolidating some of your siloed security tools and replacing with Falcon modules and XDR, you can save money.

Improve your threat visibility – by analysing threats across endpoints, identity, workloads and more, all in one console, helping to reduce false positive alerts and detect threats better.

Strengthen your protection – with our service you can protect not just the endpoint but identity, data, cloud, containers and more, all in one place.

1. www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is
2. Research Voice of the Enterprise: Information Security, Organizational Dynamics 2022

Key features
– our solution to help prevent breaches

- **Protection** – a range of CrowdStrike Falcon modules protecting endpoints, cloud, containers, identity, data and more.

- **CrowdStrike Falcon XDR** – collect and analyse threat data from CrowdStrike Falcon modules and third-party integrations all in one place.

- **BT's managed service and expertise:**
  - **initial set up** – we'll help design your security policy and provide implementation support to carry out the project delivery.
  - **in-life monitoring and management** – our Security Operations Centre team will monitor, detect and respond to threats quickly, 24x7x365. We'll automatically quarantine compromised endpoints, so your team don't have to[3].
  - **controlled deployment** – we'll work with you to test your security policy and fine tune it and configure the CrowdStrike Falcon platform and its components.
  - **continuous improvement** – we'll continuously improve and maintain the platform, optimising your service to lower your cyber risk.
  - **reporting** – we'll provide regular security reporting to help continually improve your security posture.

Why CrowdStrike for XDR?

- **Scalable and quick set up** – delivered via the cloud, removing the burden of installation, management and tuning of legacy on-premises solutions.

- **End-to-end security** – get the visibility, tools and protection every security team needs to safeguard today's modern enterprise and stop breaches.

- **Recognised** – accolades and leadership positions from independent evaluators and industry analysts – including Gartner, Forrester, and IDC.

- **World's largest threat centric data fabrics** – all customers benefit from a cloud-native threat detection platform that is processing more than one trillion events per day to detect, hunt, and respond to threats at unprecedented speed and scale.

- **One of the largest partner ecosystems in security** – with over 400 partner apps and dedicated integrations, our customers gain even more value from their existing tools.

Why work with us?

We're experts
Our team is extensively trained and accredited by CrowdStrike so you can trust us.

24x7x365 coverage
Our SOCs provide you with 24x7 support, every day of the year.

We're recognised
We've been named as a leader in the IDC MarketScape European Managed Security Services 2022 vendor assessment.

We're experienced
With over 3,000 cyber security experts with certified skills globally, we support some of the world's largest companies, nation-states, and critical national infrastructures. Plus, we protect our own business from over 4,000 cyber-attacks a day.

We're vendor agnostic
Our experience with multiple suppliers puts us in an exclusive position to advise you on the right partners for your own XDR journey and we can manage them on your behalf.

3. Powered by BT Eagle-i. Customer must have CrowdStrike Endpoint and is dependent on the GSM tier chosen

What could Managed CrowdStrike Falcon XDR do for you? Visit bt.com/security