Are your security tools working in harmony?

Multiple, siloed security controls can miss sophisticated threats and create alert fatigue. 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.

Digitalisation is accelerating, meaning 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].

While digitalisation has fixed some problems, it's caused others. Security architectures have become more complex and harder to manage. Cyber security teams are experiencing alert fatigue, and threats are being missed as correlating findings across multiple tools increases in difficulty.

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

77% of security experts agree that detection and 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 and minimising the risk to your business. We'll continue to manage the Falcon platform, optimising your service to lower your cyber risk. Our comprehensive service covers the deployment, ongoing monitoring, continous improvement, and tuning of the platform, leaving you free to focus on other business challenges.

Benefits of Managed CrowdStrike Falcon XDR

Speed up your response – improve efficiency and productivity of your team by only responding to real threats that we've detected and investigated.

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

Relieve the pressure on your team – we'll set up and manage the service and take care of detection and response so your team can focus on critical tasks.

Reduce the cost of security – consolidate some of your siloed security tools and replace with Falcon modules and XDR, saving you money - all in one console.

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

- **Range of CrowdStrike Falcon Modules** – protects endpoints, cloud, containers, identity, data and more.
- **CrowdStrike Falcon XDR** – collects and analyses 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 (SOC) team will monitor, detect, and respond to threats round-the-clock. 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 businesses and stop breaches.
- **Recognised** – recipient of various accolades and leadership positions from independent evaluators and industry analysts – including Gartner, Forrester, and IDC.
- **World's largest threat centric data fabric** – all customers benefit from a cloud-native threat detection platform that is processing more than one trillion events per day to detect 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.
- Our solution is created by **combining our managed service capability with the industry's top technology partner for XDR – CrowdStrike.**

Why work with us?

We're the experts

Our team is extensively trained and accredited by CrowdStrike, so you know you can trust us. We're an Elite CrowdStrike Powered Service Partner.

24/7, 365 coverage

Our SOCs provide you with 24/7 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 and are CrowdStrike's 2024 GSI partner of the year in EMEA and APJ.

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 neutral

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 manage them on your behalf.

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