# Identify, respond to and remediate security threats faster

The acceleration of digital transformation has increased your potential attack surface and cyber criminals are infiltrating organisations based on techniques that have grown in sophistication, volume, and diversity, it's a perfect storm that could lead to a devastating cyberattack unless you catch it before it's too late. Managed Extended Detection and Response from BT is a fully managed security threat detection and response service that enhances your existing Microsoft defender security controls. We will help you react at speed to new risks and remediate any security threats, while relieving the pressure on your in-house IT and security teams.

80%
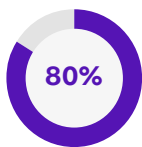
Over 80% of successful breaches[1] are unknown zero-day attacks. These can be new or evolved malware variants that infiltrate a system unrecognised or may be exploiting undisclosed vulnerabilities.

Understanding how to protect your business from these threats is critical in maintaining your security posture. But many organisations lack visibility or deep knowledge of the cyberthreat landscape which means attacks go unnoticed or reactions are inappropriate.

The need for speed

The faster you can detect and remediate a breach, the more likely you are to protect your brand reputation and bottom line from serious damage.

But in order to act quickly, you need skilled people, working to defend your estate round the clock. This can prove challenging as employees with key skills in security, cloud and collaboration technologies are extremely difficult to find and retain.

Partnerships that create value

Managed Extended Detection and Response Microsoft is available at the premium level of our Managed Sentinel service.

We'll supercharge your existing Microsoft 365 Defender and Defender for Cloud security controls to provide a fully managed threat detection and response service that delivers deeper telemetry across your cloud, end user and OT environments.

1 2020 State of Endpoint Security Final (morphisec.com)

Stay on top of increasing security threats

Our managed service is built on:

- **Automation:** With machine learning, a finely tuned rule set and years of experience, we can help you focus on real threats, minimising false positives

- **Remediation:** Detect breaches and remediate quickly to limit financial and reputational damage

- **Trust:** A co-managed approach to cybersecurity adds strength to your existing defences and enhances your security posture

- **Speed:** We see threats as they start to emerge, allowing us to protect you before a cyber attack happens

- **Intelligence:** Enhance what you've already bought with actionable threat intelligence derived from our holistic view of the connected world

- **Value:** Provide orchestration and oversight across all your estate, maximising the return on your investment.
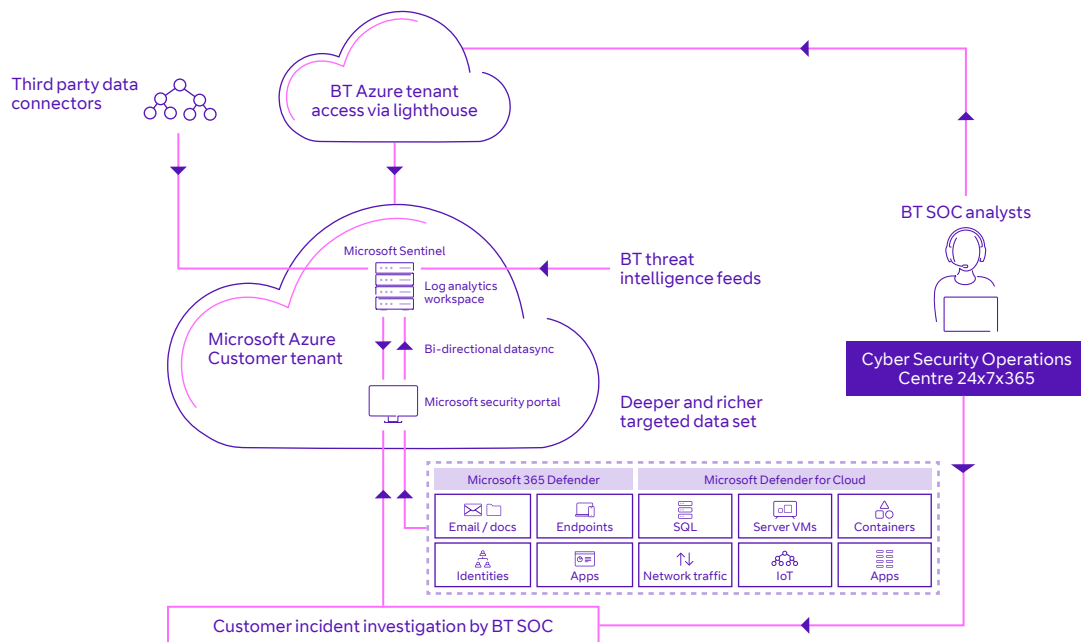
BT

Our set-up extends beyond just protecting your Microsoft services to also include multi-cloud, multi-platform, mobile devices and on-premises assets.

The added benefits of a co-managed approach

- **Enhanced security:** Our security analysts have seen varied attacks across hundreds of major networks and we've developed a robust set of rules that can be applied to your estate.

- **Reduced pressure on IT resources:** We can filter out false positives, saving time, ensuring we're only responding to genuine threats.

- **Risk mitigation:** Threat monitoring mitigates risk and helps comply with auditing and accountability standards, protecting you against financial losses.

- **Data protection:** Collecting and analysing network, device and cloud information to classify it according to the risk it represents helps safeguard business-critical data.

- **Compliance support:** Our reporting features can provide the information you need to comply with regulations, and the audit process.

How Managed Extended Detection and Response Microsoft works

Third party data connectors

BT Azure tenant access via lighthouse

BT SOC analysts

Microsoft Sentinel

Log analytics workspace

BT threat intelligence feeds

Microsoft Azure Customer tenant

Bi-directional datasync

Cyber Security Operations Centre 24x7x365

Microsoft security portal

Deeper and richer targeted data set

Microsoft 365 Defender | Microsoft Defender for Cloud

Email / docs | Endpoints | SQL | Server VMs | Containers

Identities | Apps | Network traffic | IoT | Apps

Customer incident investigation by BT SOC

Why choose BT?

Analyst recognition

We have been named a leader in the IDC MarketScape Managed Security Services 2022 Vendor Assessment, recognised for our ability to seamlessly integrate our security portfolio with wider network and cloud solutions.

Accreditation

Our CREST accredited threat intelligence capabilities lie at the heart of how we protect our customers

Microsoft Intelligent Security Association (MISA)

We are a proud member of MISA, a network of independent software vendors and managed security services providers who have integrated their solutions with Microsoft to help customers better defend themselves against a world of increasing threats.

What could Managed Extended Detection and Response do for you?
Visit bt.com/security