Cut through the noise and quickly get to the heart of any security threats

The need for scalability and flexibility is driving more and more organisations to move to the cloud. And that means thinking about security in a new way. Microsoft Sentinel collects data from all your applications and devices so you can quickly spot suspicious behaviour and eliminate any threats. But to realise all of this, you need the right people with the time to manage it on your behalf – and the expertise to understand what the alerts mean and how to build on the intelligence and insights you gain.

A Security Event and Incident Management (SIEM) service, when set up properly, will flag up suspicious activity on a network, whereas an underutilised SIEM is simply a waste of time, money and resources. Networks don't sleep – and cyber criminals don't clock off at five. So continuous security monitoring isn't a choice. You need to be on it 24x7x365.

A sentinel that never sleeps

Managed Sentinel allows you to free up your IT and security team – and get a global community of security experts on your frontline, working to orchestrate, monitor and defend your business.

Our global Security Operations Centres monitor networks 24x7 every day of the year and our team has extensive experience of supporting large customer environments. You'll be able to tap into their skills and expertise and get contextualised and actionable information that's ready to use. Our premium service combines the benefits of Managed Sentinel with Extended Detection and Response, allowing for faster breach detection and remediation and deeper telemetry across cloud, end user and OT environments.

The cost of data breaches at organisations with a mature use of security analytics was 33% lower than organisations with less mature analytics.

Source: IBM Cost of data breach report 2021

The average number of days to detect and contain a data breach in 2021 was 287. For breaches that were detected and contained under 200 days, the breach cost was nearly 30% lower.

Source: IBM Cost of data breach report 2021

45% of organisations used more than 20 tools when specifically investigating and responding to a cybersecurity incident.

Source: IBM Cyber Resilient Organisation study 2021

The benefits of a managed service

Deployment and enablement

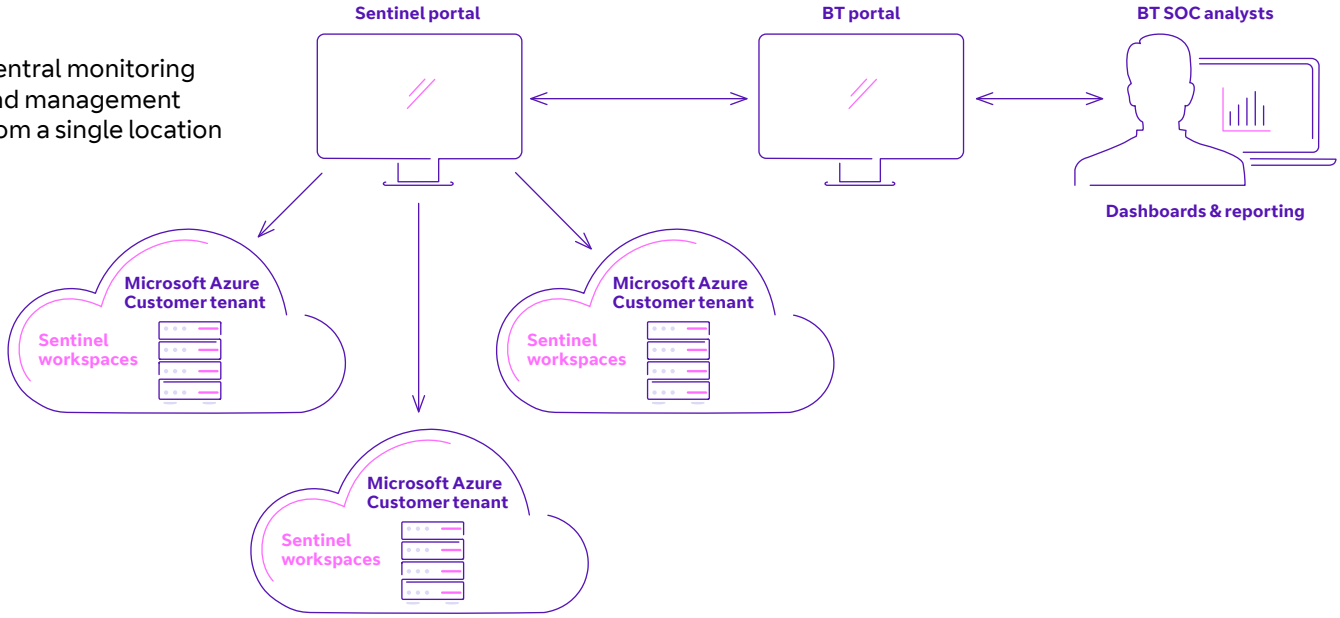
- User case assessment – rules are written in accordance with your technology and architecture
- Build, configure and continuously optimise your Managed Sentinel service
- Onboarding log sources and data is easy because of our security expertise and wealth of knowledge
- Customised client reports which allows you to interpret your data and make informed decisions
- Building and tuning Security Rules – to ensure minimal false positives and a focus on real threats.

Managed Detection and Response In-Life Service

- Triage, investigation and threat response from trained and skilled SOC analysts – so you don't have to worry about building and maintaining your own SOC infrastructure
- Tuning and optimising your Microsoft Sentinel environment
- Expert analysis of your risk and threat landscape, providing continuous improvement to your security posture.

How it works

Central monitoring and management from a single location



A security guard that takes cloud control to a higher level

We have a ringside seat on the connected world and can combine curated intelligence from trusted third parties with our privileged knowledge to identify threats based on adversary, industry and vertical analysis – and their relevance to you.

Our Security Advisory Services team provides expert guidance to navigate today's complex cybersecurity landscape. And within our advisory services, we've developed the threat prioritisation framework to identify the prioritised risks relevant to your business.

The framework combines the industry-standard MITRE ATT&CK® methodology with our own threat intelligence and security expertise to generate a threat map specific to your organisation. This creates a strategic, insights-driven approach to managing threats based on attack vectors that we know are used against organisations in your market.

You can also see if your security investment is aligned with your business priorities, so you avoid under- and over-spending.

Why work with us?

Get proactive experts on hand

Our experienced SOC analysts, based in our global Cyber Security Operations Centres will monitor your Microsoft Sentinel workspace around the clock, giving you the information you need to respond proactively.

Take advantage of our global experience

We have many years of experience protecting both ourselves and the largest global organisations from a myriad of security threats, all of which will be available to you.

Tap into our technical expertise

We can provide you with technical consultants on an "as needed" basis, thus complementing your organisation's in-house skills and providing analysis and design expertise which will optimise the performance of your solution.

Benefit from a network of specialists

We have taken a strategic approach to ensure we deepen and expand our relationships with partners who complement our capabilities – to provide you with the best solutions we can.

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

April 2022