# MANAGED EXTENDED SECURITY (MXS)

> *Immediately improve visibility into security threats, enabling your organisation to better responded to incidents while improving your overall security posture.*

## Solution Overview

**Cyber Security presents one of the largest threats to all small businesses in Australia. At Alliance Business Technologies we have developed a Managed Extended Security (MXS) offering empowered by Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud, to bring you a security stack that modernizes your overall business security posture and defense against threats.**

**This managed services support security bundle add-on includes a number of additional features beyond the standard Microsoft solution stack.**

**Benefits of our managed extended security bundle offering:**

**Leading Microsoft integrated security tools**
Prevent, detect, and respond to attacks with built-in unified experiences and end-to-end SIEM and XDR capabilities.

**Empower rapid response**
Help your security operations team resolve threats faster with AI, automation, and expertise.

**Comprehensive employee education**
Create the best frontline defense with employees undertaking cyber security phishing simulations and training.

**Overall organisational security awareness**
A framework with services that ensure your organisation is secure and capable of overcoming digital threats.

To learn more about how our IT services can help drive your business, call **1300 705 062**, email us at **sales@abtechnologies.com.au**, or visit our website at **www.abtechnologies.com.au**.

## ABT Corporate Snapshot

We are a member of the ASCS - Managed Service Provider Partner Program (MSP3), which is part of the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) that provides expert guidance to help entities mitigate cyber security incidents caused by various cyber threats. Our accreditations include ISO 9001:2008 Quality Assurance, GITC Accreditation Q-2645.

ACSC Australian Cyber Security Centre

Gold Microsoft Partner Microsoft

## Key Focus Areas

### ✓ Microsoft Sentinel (SIEM/SOAR)

A cloud-native security information and event manager (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise—fast. Aggregate data from all sources, including users, applications, servers, and devices running on-premises or in any cloud using built-in connectors, letting you reason over millions of records in a few seconds.

### ✓ Extended Detection & Response (XDR)

Automatically collects, correlates, and analyzes signal, threat, and alert data from across your Microsoft 365 environment, including endpoint, email, applications, and identities. XDR is an evolution of EDR (Endpoint Detection and response) where EDR focuses on the endpoint, XDR incorporates signals from the entire environment to track the threat lifecycle.

### ✓ Endpoint Protection and Response

Endpoint detection and response capabilities are put in place to detect, investigate, and respond to advanced threats that may have made it past the first two security pillars. In conjunction with being able to quickly respond to advanced attacks, Microsoft Defender for Endpoint offers automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale.

### ✓ Continuous Security Posture Assessment

MXS will continuously assess your infrastructure for threats and vulnerabilities, alerting us of each new detection and providing mitigation recommendations.