FUJITSU

Cyber Resilience

Managed Detection and Response

Powered by and prioritised for Microsoft Security

Service Overview

State-sponsored espionage, cyber warfare, and financially motivated criminal organisations are exploiting technology weaknesses. Network intrusions are reported at record highs. The rapidly evolving threat landscape demands an adaptive Managed Detection and Response capability – to respond swiftly to the changes in threat actor Tactics, Techniques, and Procedures (TTP's).

You need a service solution that provides deep visibility into your network, across your critical information, technology assets, applications, and identities, from the endpoint to the end user, from the smartphone to the cloud.

Powered by **Microsoft Sentinel** and **Microsoft 365 Defender Security Suite**, Fujitsu's **Managed Detection and Response** (MDR) service operates 24x7x365 and is delivered onshore from our ANZ Cyber Resilience Centre by our team of security experts.

Our cyber security services extend beyond infrastructure protection and endpoint threat detection, providing a true end-to-end managed service outcome, integrating application activity monitoring, network monitoring, digital forensics, malware analysis, incident management, and threat hunting into a singular service outcome.

Achieving Business Cyber Resilience

- **Gaining security visibility** across your entire technology environment, including endpoints (Windows, Linux, macOS), networks, mobile (Android, iOS) and Internet-of-Things devices, on premise, work from home users, SaaS platforms, and the cloud.
- **Decreasing Mean-Time-To-Detect by leverage** of best-in-class technologies and operational processes that provide early threat visibility.
- **Fast track containment** by leveraging real-time detection and response capabilities combined with automated responses, accelerating containment, eradication, and recovery actions.
- **Demonstrating appropriate security risk management** to meet your cyber insurance provider and underwriter expectations, and reducing your effort and time to meet evolving cyber insurance policy conditions.

Our Story

We are a global leader in technology and business solutions that transform organisations and the world around us.

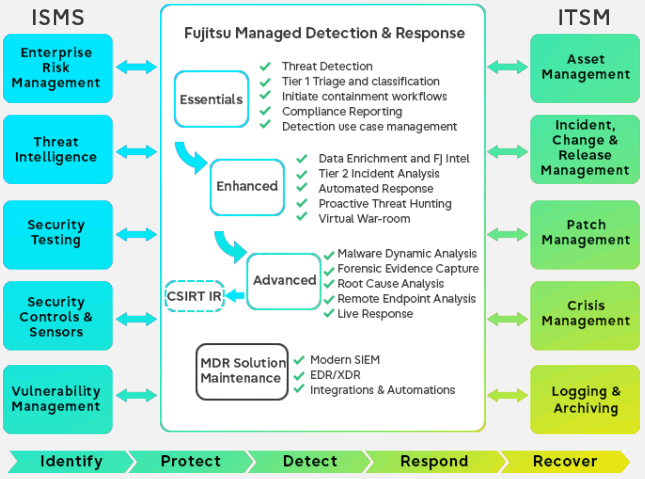
We put people first. We believe in the power of diversity. Our values of Empathy, Trust, and Aspiration drive everything we do.

Fujitsu is a Microsoft Gold Partner.

Microsoft

What we offer

- Fast tracked log onboarding using Microsoft's range of out-of-the-box connectors for the systems and cloud services that provide the greatest security value.
- Integration with your ITSM platforms, IT systems and extending your security tool stack.
- Security incident response playbooks to mitigate and manage diverse and evolving security events.
- End-to-end management of security incidents, from containment, eradication, and recovery, to incident governance and coordination (Major Incident Management).
- Comprehensive reporting for technical and operations stakeholders and compliance obligations.



Related Services:

- Threat Protect | Vulnerability Management
- Information Security Manager

Did you know?

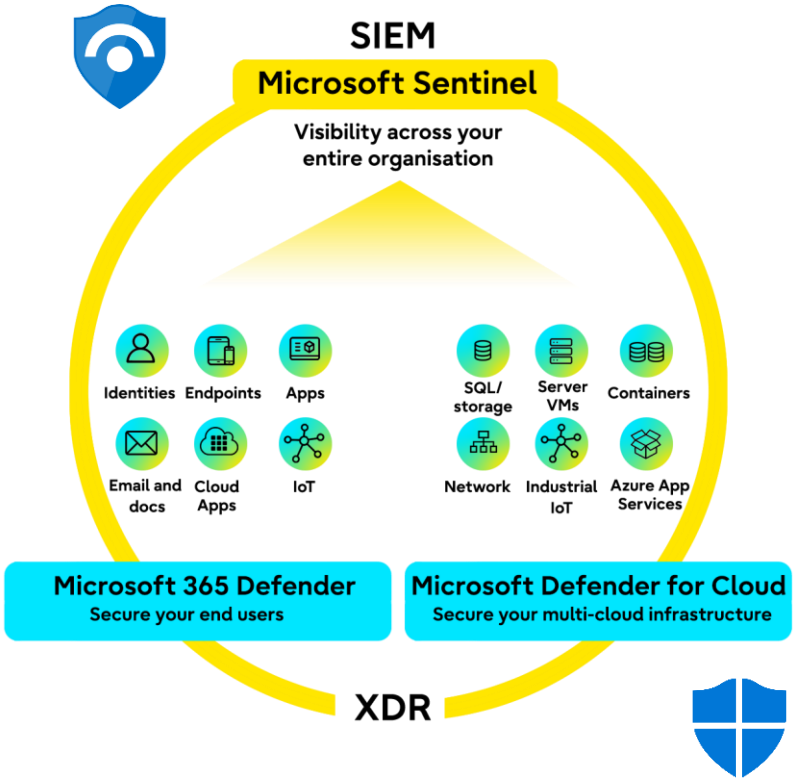
- The number of reported ransomware attacks doubled between 2020 and 2021 and industry reports suggest this trajectory won't continue.
  Verizon 2021 Data Breach Investigations Report
- On average, attackers dwell within compromised networks for up to 21 days before they are discovered or initiate ransomware and cyber attacks.
  Mandiant M-Trends 2022
- Insider threats make up 22% of security incidents, leading to loss of intellectual property, customer and other sensitive information - resulting in reputational damage and financial penalties.
  Verizon 2021 Data Breach Investigations Report

Compliance Assured

Fujitsu's MDR service provides the monitoring, detection, response, and reporting capabilities required by government and industry regulators and insurers.

The Microsoft Defender Compliance Portal provides a range of out-of-the-box compliance reports and tools to track compliance performance across your organisation.

We also tailor reports to address your specific compliance requirements, such as the ASD Essential Eight, as well as provide the situational context for how compliance with a particular standard impacts your threat profile.



Enterprise-wide Insights

Microsoft Sentinel provides a centralised platform to collect, analyse, and enrich security logs and telemetry across your organisation using out-of-the-box connectors for both your existing security IT solutions and your Microsoft cloud services such as Azure AD, Defender for Endpoint, and Defender for Cloud Apps.

Far from simply ingesting logs and generating low-value alerts, Microsoft Sentinel takes several approaches in discovering the threats that matter the most to your organisation:

- Microsoft's User and Entity Behaviour Analytics (UEBA) engine leverages machine earning to discover anomalous, risky behaviours, revealing insider threat activity that would otherwise remain undetected.
- Microsoft observes billions of threat signals each month, resulting in timely and contextual threat intelligence used to enrich logs generated within your environment.
- Out-of-the-box detection signatures that provide full coverage the MITRE ATT&CK® framework.

At the centre of it all is our dedicated team of cyber security experts, who, as well as responding to security events, adopt an "assume breached" position by continuously and proactively conducting threat hunting to search for undetected threats and compromise indicators beyond the dashboards and alerts.

Defend All Bases

Leveraging the Microsoft 365 Defender suite*, Fujitsu's MDR Service secures your entire enterprise.

- **Defender for Endpoint** is a complete Extended Detection and Response capability, enabling next-gen anti-virus, remote response actions, and threat detection.
- **Defender for Office 365** provides advanced security features across your online Exchange, Teams, and SharePoint services.
- **Defender for Cloud Apps** rich visibility, control over data travel, and sophisticated analytics to identify and combat threats across your Microsoft and third-party SaaS based applications.
- **Defender for Identity** leverages monitors your on-premise Active Directory signals to detect and investigate advanced threats, compromised identities, and insider threats.

** May require additional technology and software subscriptions.*

Our service package tiers have been designed to meet the needs of most public and private sector organisations. We can also customise a service package to suit your unique requirements.

Essentials	Enhanced	Advanced
✓ Threat Detection	✓ Data Enrichment & Fujitsu Intel	✓ Malware Dynamic Analysis
✓ Tier 1 Triage & Classification	✓ Tier 2 Incident Analysis	✓ Forensic Evidence Capture
✓ Initiate Containment Workflows	✓ Automated Response	✓ Root Cause Analysis
✓ Compliance Reporting	✓ Proactive Threat Hunting	✓ Remote Endpoint Analysis
✓ Detection Use Case Management	✓ Virtual War Room	✓ Live Reponse

FUJITSU