FUJITSU

Cyber Resilience

Managed Detection and Response

Service Overview

State-sponsored espionage, cyber warfare, and financially motivated criminal organisations are exploiting vulnerable technology. Application and 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 application, network, user activity and across your critical information and technology assets, from the endpoint to the gateway, from the smartphone to the cloud.

Powered by industry leading security technology and Australian cyber security innovators, 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 technology environment, including endpoints, networks, web applications, mobile 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.

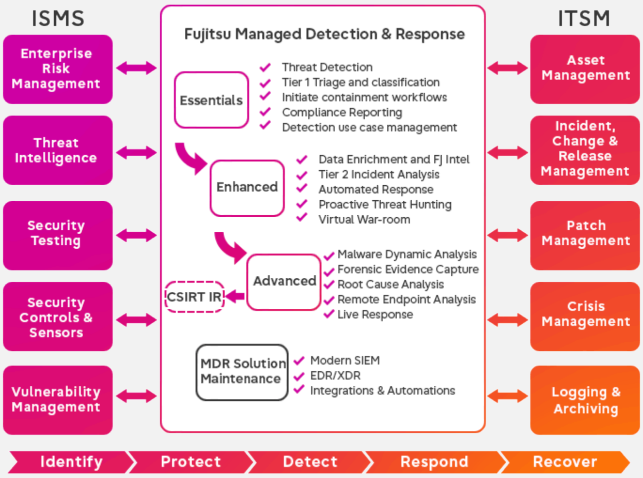
Our Story

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.

What we offer

- Security log onboarding prioritising the sources that provide the highest security value. This combats alert fatigue by isolating the signal from the noise.
- 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.



ISMS

Enterprise Risk Management

Threat Intelligence

Security Testing

Security Controls & Sensors

Vulnerability Management

Fujitsu Managed Detection & Response

Essentials
- ✓ Threat Detection
- ✓ Tier 1 Triage and classification
- ✓ Initiate containment workflows
- ✓ Compliance Reporting
- ✓ Detection use case management

Enhanced
- ✓ Data Enrichment and FJ Intel
- ✓ Tier 2 Incident Analysis
- ✓ Automated Response
- ✓ Proactive Threat Hunting
- ✓ Virtual War-room

Advanced
- ✓ Malware Dynamic Analysis
- ✓ Forensic Evidence Capture
- ✓ Root Cause Analysis
- ✓ Remote Endpoint Analysis
- ✓ Live Response

CSIRT IR

MDR Solution Maintenance
- ✓ Modern SIEM
- ✓ EDR/XDR
- ✓ Integrations & Automations

ITSM

Asset Management

Incident, Change & Release Management

Patch Management

Crisis Management

Logging & Archiving

Identify → Protect → Detect → Respond → Recover

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.

Reporting can be tailored to address your compliance requirements and informed by our security expert insights to your risk posture context and support security investigation and reporting.

On the journey to ASD Essential Eight? Our MDR service is your answer to the centralised logging and monitoring of your security controls required to reach Maturity Level 3!

MITRE ATT&CK®

Threat Intelligence

User Behaviour Analytics

Expert Security Analysts

Custom Detection Rules

Attacker Behaviour Analytics

Proactive Threat Hunting

Our dedicated cyber security experts are empowered by Machine Learning, Threat Intelligence and Data Analytics.

Gain Insights

It isn't enough to just forward all of your infrastructure logs and telemetry to your SOC. To protect against the latest threats faced by your organisation, those logs must be analysed, normalised and enriched, and to craft high-fidelity and high-confidence detection signatures. This isn't a one-time process – attackers are evolving and so must our approach.

We provide full coverage of the MITRE ATT&CK® framework, and we ingest the latest threat intelligence from our regional and global teams, and external partners. We understand who the threat actors are, who they are targeting, and how they operate. This enables us to constantly and rapidly develop, refine, test, and implement custom detection signatures for the threats that matter the most to your organisation.

Powered by Machine Learning, our User Behaviour Analytics (UBA) and Attacker Behaviour Analytics (ABA) engines read between the lines to discover anomalous, risky behaviours, revealing insider threat activity that are often missed by static detection rules.

Finally, by adopting an 'assume-breached' position, our cyber security experts are researching beyond the dashboards and alerts to hunt for both known and unknown threats that may be lurking deep within your environment.

Extended MDR

Fujitsu's MDR packages all the benefits of Extended Detection and Response (XDR) into three service tiers to suit most companies and organisations. We can also tailor our offerings to suit your specific needs.

- **Automated Response Actions** to quickly contain an incident, such as isolating systems, disabling a user account, or modifying firewall rules.
- **Dynamic Malware Analysis** for understanding unknown malware samples and providing additional indicators to search for across your environment.
- **Major Incident Management** because security incidents aren't just a technology problem, they're a business problem and often require the input and expertise from your broader organisation.

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

Intellectual Property © 2022 Fujitsu Australia Limited and Fujitsu New Zealand Limited. All rights reserved. This material is authored by Fujitsu Australia Limited and Fujitsu New Zealand Limited (Fujitsu). Fujitsu is the copyright holder of this material and provides the material for the purpose of the evaluation of the contents. Fujitsu does not authorise the use, reproduction, modification or adaptation of the material without Fujitsu's prior written consent. **Legal Disclaimer:** The information in this document supersedes all previous information, representations, agreements or understandings. This material does not constitute an offer capable of acceptance nor does it result in a binding contract between the parties. The supply of the goods and services referred to in this document will be subject to entry into a formal agreement. All brands and products referenced in the document are acknowledged to be trademarks or registered trademarks of their respective owners