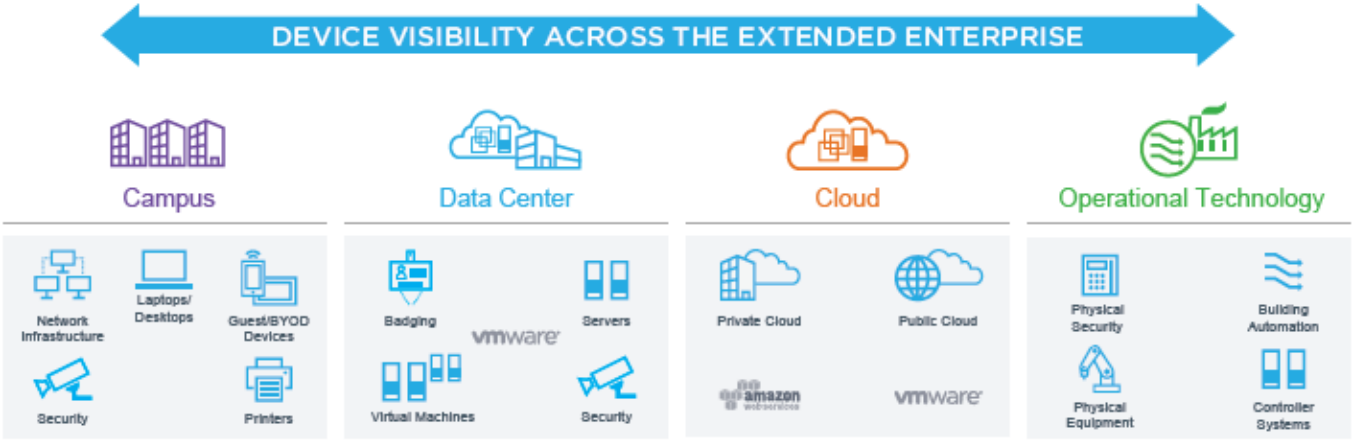
FUJITSU
shaping tomorrow with you

Continuous Diagnostics & Monitoring Services

Accurate device visibility is foundational to any security practice, especially with the explosive growth of connected devices. Fujitsu's Continuous Diagnostics & Monitoring (CDM) platform provides insight into the diverse types of devices connected to your heterogeneous network – from Campus and Data Centre to Cloud and Operational Technology networks. With one platform, you gain a consolidated view of traditional systems, mobile and IoT devices, virtual machines and cloud instances, as well as Operational Technology systems for an extended view of your whole enterprise.

With Fujitsu's CDM Platform & Services, we provide you with the core components for the speedy, detection, intelligence and alerts to enable fast response and remediation of security incidents.



Expanded Device Visibility Platform

As the convergence of IT and OT accelerates, networks with industrial and critical infrastructure systems are no longer air-gapped from IT networks. Hence, organizations face increased business risk as threats can jump between these domains. Bad actors take advantage of this IoT and OT attack surface to enter your network and move laterally to access sensitive information or cause business disruption.

Fujitsu's CDM Platform raises the bar on device visibility and scalability helping organizations looking to keep pace with more than 5 billion1 IP-connected devices on enterprise networks today. It includes foundational enhancements and innovative capabilities to scale and deploy in the largest and most complex enterprise networks.

shaping tomorrow with you

FUJITSU

Fujitsu's UEBA Features

- **Device Discovery** – Deeper insights into some of the fastest-growing devices on enterprise networks, including IPv6 systems and devices managed by cloud network controllers such as Cisco® Meraki
- **Agentless** – Passive only monitoring for ease of deployment, operational, management and ability to manage inventory OT devices safely
- **Auto Classification** - Cloud-based intelligence Auto-classify new devices as they are discovered and connected
- **Risk Assessment** - risk assessment to reduce your attack surface
- **Device Intelligence Dashboard** - A customizable device intelligence dashboard to improve security operations and speedier incident response
- **Control Automation** – Enforce network Segmentation, Policy based Enforcement, Network Access Controls (NAC) and integration with Cisco DNA Centre
- **Scalable** – Scalable & flexible architecture, enhanced deployment options enable management of up to 2 million devices in a single deployment.

Agentless Passive only Monitoring

Fujitsu's CDM platform allows organizations to seamlessly monitor every device on your network through passive discovery and profiling techniques, glean information by inspecting network traffic, directly integrating with network infrastructure and monitoring various networking protocols. This enables you to gain device visibility without scanning or accessing connected devices, thereby minimize operational risk in IT & OT environments. It removes traditional blind spots within your extended enterprise network and gives you an accurate and real-time inventory of these devices enabling quicker incident response.

Passive monitoring techniques

- SNMP traps
- SPAN traffic
- NetFlow
- HTTP user-agent
- RADIUS requests
- DHCP fingerprinting
- MAC classification
- TCP fingerprinting
- Power over Ethernet
- Network infrastructure polling

Control Automation

Fujitsu's CDM Service provides sophisticated and extensible Network Control automation and orchestration. This Orchestration provides an enhanced level of security posture by enabling a flexible work environment including BYOD devices without the inherent risks associated with it. It also integrates with Vendors products to enable:

- Enforce Network Segmentation
- Policy based Enforcement
- Network Access Controls (NAC)
- Integration with Cisco DNA Centre

These advanced features allow for full policy based control over who is allowed onto the network, what they can do and ability to monitor, remediate and quarantine suspicious activity 24*7 seamlessly at machine speed.

Device Intelligence Dashboard – Improve Security Operations and Incident Response

Security Operations teams lack a comprehensive view into connected devices and their classification, connection and compliance context. This hampers incident response and compliance reporting.

Fujitsu's CDM platform includes a customizable web dashboard that provides a consolidated view of your device landscape and compliance across the extended enterprise. The dashboard works in concert with the Enterprise Manager and provides insight into the diverse types of devices connected to your heterogeneous network.

Security analysts can use the device intelligence dashboard for incident response. During a threat outbreak or security incident, analysts can quickly get the device context they need, including device classification, connection, compliance and risk status at their fingertips. This eliminates tedious manual processes to identify devices, where and how they are connected to the network, and their current security posture. It optimizes incident response processes and reduces your mean time to respond. You can also tailor device intelligence views for other IT functions such as compliance and risk reporting, asset management and executive reporting.

Fujitsu CDM Services offer

- A managed CRC Service for triaging and incident management
- 24/7 monitoring
- Secure CDM Management services
- CDM as a Service - supply, integration and management
- Optional advanced Automation & Orchestration features

Summary of features:

Continuous Diagnostics & Monitoring (CDM) as a Service	Standard	Optional
Install: Install Server configure network flows	✓	
Scan: Scan endpoint behaviour & begin baseline formulation	✓	
Remediation Report: Report on identified threats & score based on client priorities as well as threat severity	✓	
Advanced Remediation Action: In conjunction with Client, remediate identified threats for managed service, triage, investigation, classification and reporting of events and incidents; including standard SLA's		✓
Automation & Orchestration Services: - Network Segmentation, Policy Enforcement, NAC, Integration		✓
Integration into SIEM tool		✓

Service Levels

In today's business world, security is a 24*7 requirement; Fujitsu provides around the clock service availability with a number of service level options designed to meet specific business needs.

Fujitsu's Cyber Resilience Centre (CRC)

Fujitsu's state of the art CRC provides a focal point for:

- The co-ordination of security monitoring and security incident management.
- Providing situational awareness through the broad view of the security threat landscape due to the breadth of the Fujitsu Client base and the links with Cyber Security agencies and strategic technology partners.
- The ongoing support and tuning of the technology platforms to enable the service to retain current against the emerging security threat.
- Security event and incident related information to better enable risk mitigation.
- Expert security advice and reporting.
- Compliance assessment and support of associated reports and remedial actions.
- Fujitsu's Advanced Remediation includes options such as - Incident response, Incident Management, End-User blocking, Endpoint re-imaging, end-user education etc...
- Fujitsu's Automation & Orchestration Services allow for full policy based control for clients with the ability to monitor, remediate and quarantine suspicious activity 24*7 seamlessly at machine speed

Benefits

Efficiency

- Reduction in time to detect threats
- Accelerate the speed to respond to threats
- Proactive services that can mitigate threats as they arise

Cost Savings

- Reduces the cost of hiring, training and retaining high quality security professionals
- Flexible aaS model can reduce capex expenditure
- Directs spend to appropriate controls and activities

Security

- Details difficult to detect insider threats
- Enables breaches to be detected or avoided and improves incident handling and containment
- Monitors the effectiveness of security controls
- Streamlines the auditing and reporting of compliance obligations
- Provides information to better inform risk management decisions

CONTACT FUJITSU
Email: cybersecurity@au.fujitsu.com

Address:
Lvl 3,4 National Cct
Barton, ACT 2600
Australia
Tel: +61-2-6250-9600