

Vulnerability Scanning Services



Almost daily, we hear of vulnerabilities that are announced enabling attackers, malware and rogue operators to compromise systems and services within the enterprise. Many of these vulnerabilities allow unauthorised access, which can go undetected by traditional security controls and enterprise management tools.

Fujitsu's Vulnerability Management (VM) Scanning Services allows an organisation to proactively gain and then maintain intelligence of the state of the assets within the enterprise. Discovery of vulnerabilities, and the subsequent prioritisation of remediation actions, enables a holistic security/risk view of the enterprise that cannot be readily achieved by the use of other systems and toolsets.

Our VM Platform & Services provide you with the core components for the speedy, detection, intelligence and alerts to enable fast response and remediation of security vulnerabilities before they become targets.

Why is Vulnerability Scanning Important?

Having intelligence of what has been deployed before, what exists now, and early intelligence of future problems provides a foundation to build confidence in the security of the enterprise. Vulnerability Scanning provides a key enabler for managing the security risk and protecting the organisation's reputation and revenues.

Fujitsu's VM Key Features?

- **Eliminate Blind Spots** – Complete visibility into network connected assets, network activity and events, with comprehensive vulnerability assessment coverage
- **Immediate Insight** - Benefit from clear, actionable dashboards and reports to quickly measure and analyse security effectiveness and risk
- **Prove Compliance** - Monitor and prove compliance with pre-defined checks against industry standards and regulatory mandates
- **Boost Productivity** - Take the time savings of adjusting reports or combing through spreadsheets and spend it on remediating vulnerabilities
- **Proactively Address Threats** - Identify threats and unexpected network changes. Get targeted alerts to quickly begin remediation
- **Prioritize Vulnerabilities** - Understand the impact of vulnerabilities in your network and prioritize remediation efforts
- Our services are backed up with our renowned global ISO20000 aligned service delivery capability, enabling us to provide an end-to-end service that can be integrated into an organisation's IT services

Fujitsu VM 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:

Vulnerability Management (VM) as a Service	Standard	Optional
Identify: Scan network for Devices	✓	
Scan: Scan network for vulnerabilities, identify new devices added to network (scheduled or ad-hoc)	✓	
Threat Intelligence – gather latest threat intelligence to search for “near” 0-day vulnerabilities	✓	
Remediation Report: Report on identified threats & score based on client priorities as well as threat severity	✓	
Remediation Action: In conjunction with Client, remediate identified threats, triage, investigation, classification & reporting of events and incidents; including standard SLA's		✓
External Cloud based Scans: Regular scans of external web sites (production/dev/test/DR) to ensure no known compromises		✓
OT Network: Enhanced monitoring of Operational Network (SCADA) environment		✓
Respond OPTIONS: enhanced cyber investigations and optional cyber threat response services		✓
Integration into SIEM environment		✓

Deployment

- Cloud based SaaS, appliance or VM deployment options to suit every infrastructure requirement
- 24x7 monitoring of the infrastructure and services
- Scalable and tailored solutions to meet the organisation’s specific requirements.
- Ability to facilitate regulatory (including PCI) and security compliance reporting for the enterprise.

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

© FUJITSU 2019. All rights reserved. FUJITSU and FUJITSU logo are trademarks of Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use

