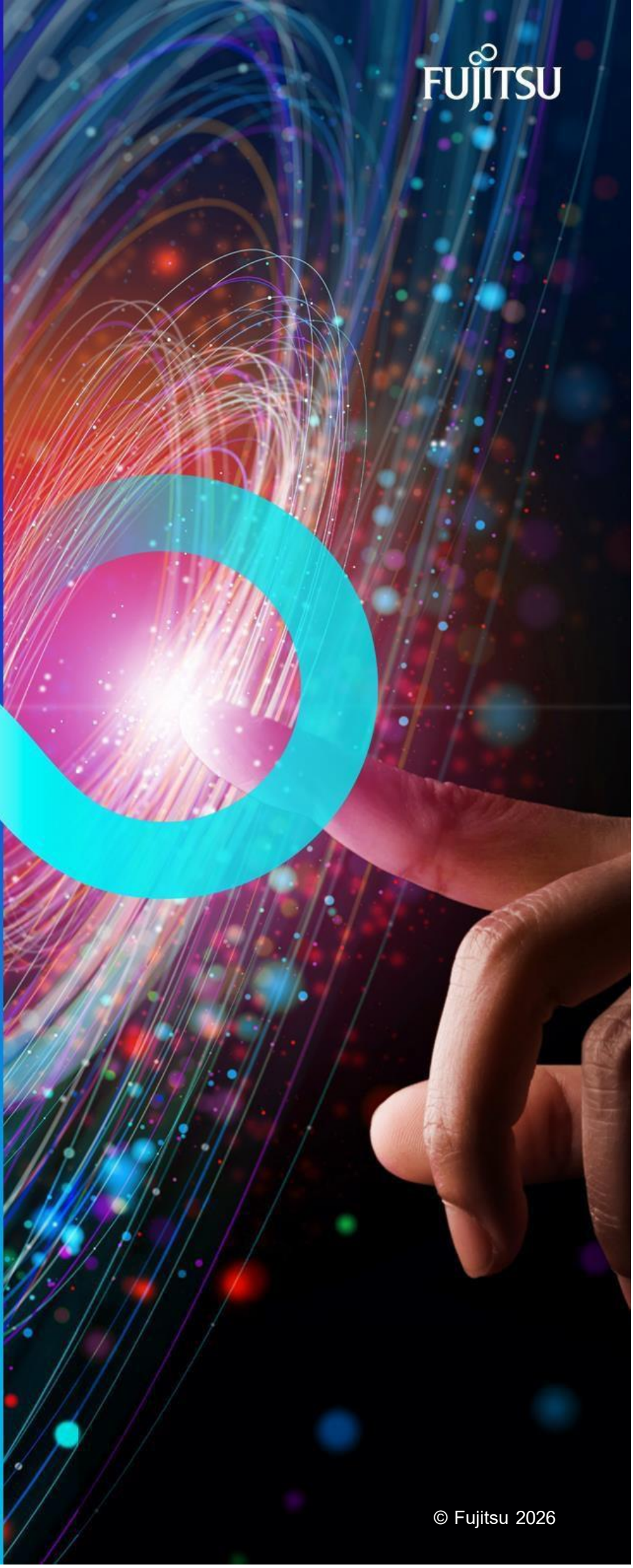
Service Definition

Infrastructure Protection



G-Cloud 15

Contents

Managed Security Service

Fujitsu is a proven security partner with 40 years of demonstrable capability in providing intelligent security solutions to organisations across both private and public sectors including FTSE250 companies operating in highly complex and regulated environments.

Fujitsu's security professionals are trusted advisors with the expertise to enable organisations to prepare for and respond to cyber security incidents effectively and efficiently. Fujitsu also provides guidance on the appropriate security controls to protect organisations, ongoing management of cyber security capabilities on behalf of customers, undertakes 24x7 security monitoring from its Advanced Threat Centre and UK Security Operations Centres (SOCs).

Fujitsu integrate market leading security technologies and expert professional services to support the assessment of risk, define requirements, provide technical and service design and security architectures, as well as ensuring effective deployment, operation and management of our Managed Security Services (MSS). Fujitsu also provides predictive cyber threat intelligence services and threat response services, underpinned by security orchestration, automation and response (SOAR), which provide timely and expert response services to mitigate the impact of potential and actual security incidents for our customers. Fujitsu services are aligned to NIST Cyber Security Framework core functions of Identify, Protect, Detect, Respond and Recover.

Figure 1: Cybersecurity Framework

As a global security and service integrator, Fujitsu provides security and resiliency consultancy services across the full delivery lifecycle. These services are seamlessly integrated within the operational, service and security framework within customer organisations, with our services perceived as an extension of our customers' security capability.

Fujitsu's relationships and close links with UK Government, national cybercrime agencies, academia, and our strategic technology partners, enables Fujitsu to achieve service intimacy with our customers. Fujitsu works with HMG Departments to support them to implement many of the security measures required to protect their information, technology, and digital services/assets to meet their SPF, National Cyber Security Strategy and Minimum Cyber Security Standards obligations.

In line with HMG requirements, Fujitsu holds Cyber Essentials and Cyber Essentials Plus certifications and design, build and manage ISO 27001:2013 certified frameworks for HMG where data is classified OFFICIAL through to SECRET and above. Fujitsu has a large pool of SC and DV cleared UK personnel and has experience of designing, building, and maintaining governance and security to deliver service offerings at OFFICIAL, SECRET and ABOVE SECRET classifications.

Why Choose Fujitsu

With Fujitsu's Managed Security Services, your security needs are underpinned with market-leading security technologies and professional services expertise. We assess risk, define requirements, provide technical / service designs, and ensure effective deployment and operation. Additionally:

- Fujitsu provide essential security capabilities to our Public Sector customers, supporting their drive to protect information assets in the face of emerging strategic and operational business challenges
- We are a critical component of our customers' approach to regulatory and legislator demands, helping them to manage their information security risks flexibly and effectively
- Fujitsu has been supplying computing and communications services to Government for many years, and pioneered the use of shared services in Government
- As one of the world's most experienced ICT providers, Fujitsu is combining innovation with responsible business practices to transform business and create a better future for everyone

Confidentiality and Integrity

Securing data when stored, accessed, or transmitted remains a top priority for organizations everywhere. As compliance demands increase, along with the potential penalties for failure, it's critical to keep your house in order. However, knowing exactly which controls to apply and where can be a headache.

Fujitsu's services provide you with the ability to protect your sensitive data and assets by examining data and controlling who and what can access these valuable assets. This increased visibility results in the ability to apply appropriate levels of control.

Fujitsu's has broad portfolio of industry leading network and endpoint security controls that enhances an organisations information security posture through continuous monitoring and the management.

Strategic Technology Partners

Fujitsu has strategic relationships with several global security vendors and has expertise in the definition, provision, design, implementation, test, integration, and operation of these technologies into a cohesive service.

Fujitsu actively monitors developing technologies and develops a roadmap of technologies which are relevant to the mass market and to specific industries.

Fujitsu recognises that HMG clients need to leverage existing investments, reduce complexity, reduce cost, evaluate options (i.e. Open Source) and ensure that Partners can meet HMG support needs (assurance, focus, etc.). In principle, Fujitsu focus on building and managing mutually beneficial partner relationships with key security vendors to drive project outcomes, improved service/contract management and enhanced resilience (support). Fujitsu maintain a portfolio of security technology partners that reflect our comprehensive managed and professional services capabilities

Security Portfolio

Fujitsu has an extensive portfolio of technology, consultive and managed services that include and compliment those described later in this.

Figure 2: Security Portfolio document

Scope

Overview

Today we operate in an environment that is constantly threatened by cyber-attacks. Increasingly attackers are now performing multistage incursions that exploit vulnerabilities, social engineering, data theft and spear-phishing techniques to create a persistent threat that is advanced, zero-day, and targeted.

Regular publicity serves to highlight the frequency and impact of these advanced threats to organisations with analysts estimating that:

- There is now over 1.4 billion pieces of malware programs out there.
- 560,000 new pieces of malware are detected every day.
- Every minute, four companies fall victim to ransomware attacks.
- Trojans account for 58% of all computer malware.

People, process, and technology must now come together to protect individuals and organisations from Cyber-attacks.

Detecting and containing these advanced threats requires a coordinated approach that utilises multi-layer countermeasure solutions to create a unified, proactive, and vigilant approach that provides security controls at all levels.

Visibility is key to preventing, detecting, and containing a security threat, and, without complete visibility, harmful threats are left unchallenged. This means organisations are exposed and need to re-examine their exposure to reputational challenges and their ability to respond to potential crises.

Infrastructure Protection

Fujitsu's Infrastructure Protection Services are designed to address threats against network and endpoints assets including laptops, desktops, and servers when deployed on-premises, in a data centre or cloud environment, services include:

- Intrusion Prevention and Detection Services (IPS / IDS).
- Remote Access Services (RAS).
- Network Security Policy Management (NSPM).
- Unified Endpoint Security (EPP, EDR).
- Unified Threat Management (UTM) and Next Generation (NGFW) Firewalls.
  - Can consolidate Firewall, IPS/IDS, Antivirus, Sandboxing, Remote Access, Application Control and Web Filtering onto a Single Appliance.
- Web Application Firewalls (WAF).

Intrusion Prevention and Detection Services (IPS / IDS)

Intrusion Prevention Systems (IPS) deliver the ability to detect and stop a variety of attacks that cannot be automatically identified by firewalls, antivirus technologies and other enterprise security controls. IPS technologies use a combination of several methodologies for detecting attacks. Each methodology has its own strengths and weaknesses, so by leveraging the strongest capabilities of each methodology, an IPS can detect an incredibly wide range of attacks. Where these controls are placed out-of-band and only detect attacks these solutions are called Intrusion Detection Systems (IDS).

Intrusion Prevention System (IPS) technologies are designed to counter this threat by alerting the organisation so that remedial action can be taken by proactively blocking malicious traffic.

Benefits of this service include:

- Protect organizations key businesses application when being accessed from unsecured networks including the

internet.

- Deliver industry-leading protection against new and dynamic threats.
- Proactive and centralised security management and monitoring.
- Scalability - our highly scalable service can meet the needs of all sizes of organisation.
- Brand and reputation protection - maintain the confidence of your customers, suppliers, and partners, and avoid the risk of negative press by protecting your organization's data from a breach.
- Support of regulatory compliance requirements.
- Protection of your customers' data - mitigate the risk of a data breach such as orders, payments, medical records and other personal or sensitive information.

Remote Access Services (RAS)

No matter what size organization you have, remote work is more common than ever. And with the COVID-19 pandemic, more businesses are having to rethink the way they operate. With remote access, employees can safely work from any device, platform, or network at their home office or abroad. Remote desktop functions allow them to remotely access important files and share their screen for meetings and troubleshooting. They also provide logging that is necessary for auditing, which is common practice, especially for organizations that need to remain compliant with regulatory guidelines.

Remote Access Service (RAS) solutions provide a robust and secure means and secure mechanism to access environments from an internet connection.

RAS has several configuration options that can be used within a single organisation to meet specific organisation requirements.

Using a RAS solution provides organisations with:

- Secure connections and the flexibility that organizations seek.
- Reduced requirement for and cost dedicated circuits.
- Reduced support costs.
- Scalability and elasticity.

Network Security Policy Management (NSPM)

As corporate networks, datacentres, and cloud infrastructure grow in size and complexity, so too does the challenge of maintaining visibility, compliance, security policy and procedures across a diverse infrastructure when deployed in physical, virtual and cloud environments.

With the dramatic rise in cyber threats, enterprises require controlled and centralised security policy management across the platforms and devices. Firewalls, routers, and web gateways not only filter network traffic for improved security, but also enable connectivity for critical business applications to function. Manually managing complex security policy requirements across a multitude of different devices, operational teams and business requirements, as well as security and compliance mandates, has become inefficient and error prone. Security Policy Management services can help organisation reduce operational cost and risk as well as enabling security and operations teams to keep up with the speed of the business.

Some of the benefits of Network Security Policy Management (NSPM) include:

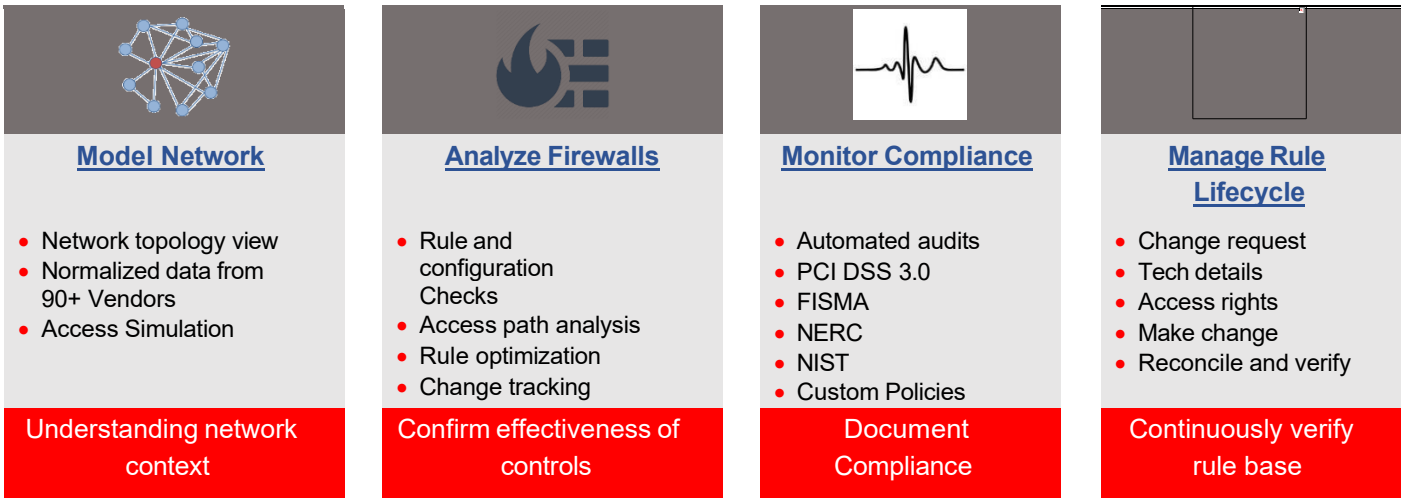


Figure 4: Network Security Policy Management

Unified Endpoint Security (EPP, EDR)

Isolated endpoint controls that only focus on a given type or attack are vulnerable. By consolidating technology, service, and process this enables the benefits of technology controls (EPP and EDR) to be enhanced with other services to form a MDR services that is now able to detect and recover from sophisticated attacks quickly.

Fujitsu's UES Managed Security Service (MSS) has been designed to protect organisations and businesses across all sectors. Endpoint security functionality falls into one of three main categories based on the primary ability to detect threats. By strategically combining endpoint technologies and their features the benefits of each solution can be used to complement one another to increase visibility, control, and protection of the endpoint.

- **Endpoint Protection (EPP)** are traditional antivirus solutions that utilise signature databases and mathematical analysis to protect against “known” malware as it attempts to enter or launch on a system.
- **Endpoint Detection and Response (EDR)** enables all activity both past and present to be examined to enable the full visualisation of malicious activities and campaigns to be realised. To protect against a detected or “known” malware these solutions are combined with an EPP functionality to protect an endpoint.

Unified Threat Management (UTM) and Next Generation (NGFW) Firewalls

Firewalls have evolved over the past 20 years from basic devices that restricted traffic to assets to now being able to protect the application and services hosted by the asset. This has seen functionality such as IPS, Antivirus, Web Filtering, Sandboxing, Application Control, and many more be consolidated onto a single appliance solution. This approach not only reduces cost but enhances security by bring once discrete controls under a single-pane-of-glass approach to administering security and protecting the organisation.

Unified Threat Management (UTM) and Next Generation Firewall (NGFW) provide a modern approach to security management that allows an administrator to monitor and manage a range of security applications and infrastructure via a single management console.

These solutions:

- Offer an adaptive architecture that delivers network and security functionality with integrated detection and automated responses to cybersecurity threats.
- Deliver high-performance, multi-layered security with centralized visibility and ease of management. This enables the enforcement and delivery of comprehensive protection throughout the enterprise from a centralized, unified, and flexible approach to network security that combats against the ever-increasing threat landscape.
- Can protect mission critical environments; the firewall solutions can operate as a high-availability cluster, eliminating downtime and ensuring the highest levels of resilience.
- Consolidate once discrete security and network solutions onto a single platform, functionality possible includes anti-virus, firewall, Data Loss Prevention (DLP), Intrusion Prevention Systems (IPS), web-filtering, SSL decryption, sandboxing, SD-WAN, site-to-site, and remote access virtual private network (VPN), anti-spam and traffic shaping.

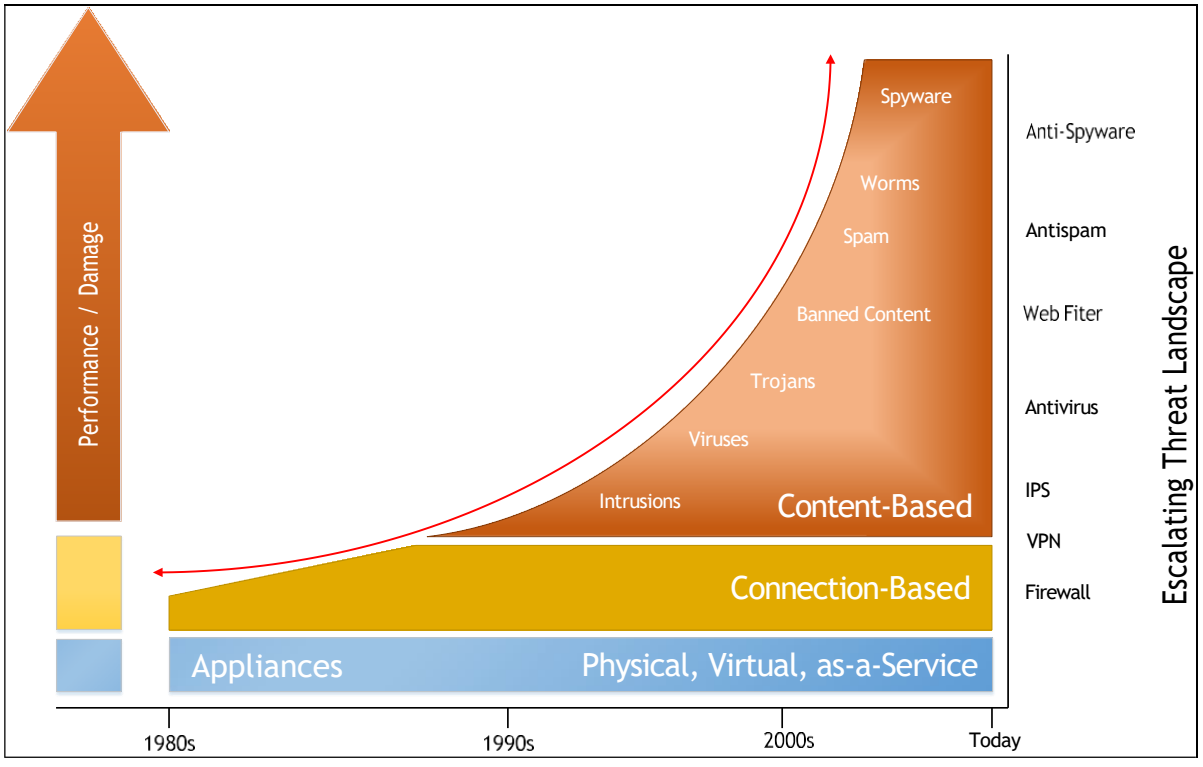


Figure 5: Unified Threat Management

Web Application Firewalls (WAF)

Web applications are a major vector for criminals seeking to penetrate your network - and securing them has until now been notoriously difficult and complex. Web Application Firewall changes the game, with comprehensive protection against all kinds of app-based threats, highly flexible deployment options, and remarkable ease of use.

Web Application Firewall (WAF) solutions are designed to:

- Protect organizations key businesses application when being accessed from unsecured networks including the internet.
- Deliver comprehensive protection without degrading throughput or application response time.
- Increase your application and network security and reduce business risk.
- Defend web applications and sites from both known and unknown attacks, including all application-layer and zero-day threats using a multi-tiered approach to security.

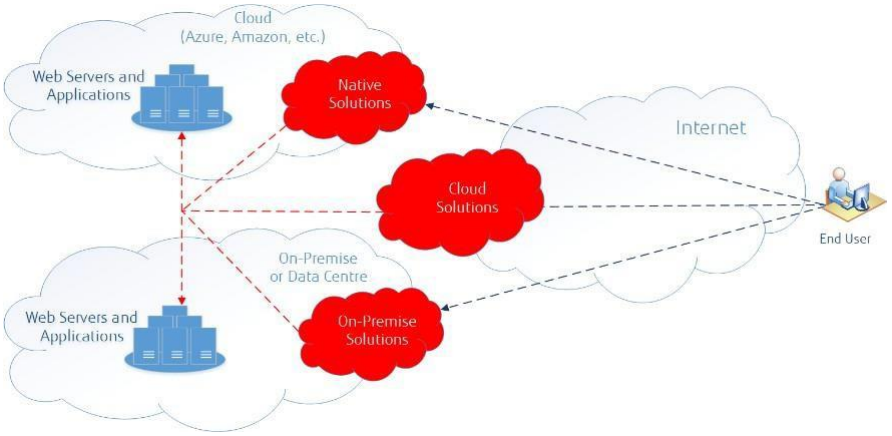


Figure 6 Web Application Firewalls

Service Delivery

Service Management

Fujitsu's Managed Security Services are operated under an ITIL-aligned, ISO/IEC 20000 compliant service management framework. Fujitsu will implement and maintain the agreed policies for the MSS and any changes to the policies will be managed through the Managed Service Change process. The MSS shall contain the following principal elements:

- Incident Management.
- Problem Management.
- Change Management.
- Release Management.
- Configuration Management.
- Service Level Management.
- Quality Management.
- Availability and Capacity Management.
- Service Continuity Management.
- Continuous Improvement.
- Third Party Management, where required.

Fujitsu's Security Operations Centres (SOC) will respond to security incidents using the following approach:

- Event Analysis - Upon detection, events which impact on security will be analysed to ascertain whether they need to be upgraded to a Security Incident for further action.
- Security Incident Categorisation – If the event is defined as a Security Incident, it will be categorised considering the cause, priority, potential impact, and the urgency of response in line with the agreed ITIL based Service Management framework.
- Security Incident Response – The security analysts, resolver groups and service management team, plus identified Customer stakeholders as defined within the overarching Service Management Framework and Communications Plan, will agree on the most appropriate course of action. When a course of action has been implemented, its effectiveness will be assessed so that if the chosen course of action needs to be extended further appropriate action can be taken.
- Post Incident Analysis - After each Security Incident, post incident analysis shall be undertaken to:
  - Ensure that the conduct of the investigation was appropriate.
  - Consider lessons identified, where conduct of the investigation could be improved.
  - Ensure that all mitigating actions have been taken.

Security and Information Assurance

Fujitsu's MSS are provided from our ISO 27001 certified support organisation and use ISO/IEC 20000 based operational procedures to deliver availability and operational service levels based on a standard service management toolset. Fujitsu provides MSS from its SOCs to a number of Public Sector Customers.

Business Continuity

Fujitsu has achieved ISO22301 certification and Fujitsu's SOCs and service delivery functions are underpinned by robust and tested Business and Service Continuity. From a MSS perspective Fujitsu will retain configuration back-ups for rebuild/restoration purposes using Fujitsu's standard environment platform backup processes. To support HMG in Business Continuity planning, Fujitsu provide BCP/DR services separately through the G Cloud framework.

Training and Consultancy

Fujitsu has a broad range of consulting capabilities. These range from technical architecture consulting, advising on security best practices, supporting major service transitions, delivery of MSS that support and facilitate highly successful first-time security deployments on a global scale. Fujitsu's experienced Governance, Risk and Compliance (GRC) focused consultants can help customers align their security strategies to those of the business.

Fujitsu can also provide business focused consultants to work with customers to facilitate and enable the required process engineering to rapidly integrate MSS and mature incident response processes that enable you to derive the benefits and return on investment in the MSS. Additionally, Fujitsu's consultants can undertake training of Customer personnel including knowledge transfer and structured maturity development for MSS and the underpinning technologies.

Additional Service Options

Dependent upon the MSS chosen the services comprise service level options and also optional enhancement and ancillary services dependent upon specific or wider Customer requirements where the complete support requirement is not covered by a specific control these can be defined and agreed as part of the requirements definition phase. Examples could be the following:

- Secure DevSecOps and, secure CI/CD for application development.
- Controls to secure data and enable discovery within Cloud based services, lessons identified, and where conduct of the investigation could be improved.
- Security requirements for Applications/Digital Services.
- Asset Management (for integrated delivery with Vulnerability, Patching mechanisms etc.).
- Mail Gateway technologies to support secure connectivity post GCF/GSi requirements.
- Managed Detection and Response (MDR) utilising Extended Detection and Response (EDR) technology

Onboarding and Offboarding

Onboarding

Fujitsu's approach is to work with the G Cloud customer to define the detailed requirements to produce a quotation that includes the agreed scope of the services and delivery approach. Fujitsu's Onboarding process has five overarching phases:

- Definition of the scope.
- Discovery - conducting a detailed analysis of the current estate.
- Design of the new infrastructure based on definition and discovery.
- Develop the solution.
- Deploy, test and release.

The approach is defined by the following key components:

- Project/programme management activities aligned to PRINCE2/Managing Successful Programs.
- Robust change management.
- Externally verified risk management processes.
- Active security management.
- Staged approach with formal entry and exit criteria, controlling stage progression.
- Offboarding

Fujitsu will collaborate with you to define the scope and timescales required as part of the Off Boarding. The approach to off boarding will ensure an orderly transition of the transferring services to the replacement supplier.

A key priority for Fujitsu in any service exit event is maintaining the contracted levels of service for the remaining period of the Term. As such, Fujitsu would look to collaborate with the new incoming supplier to:

- Agree a strategy for exit arrangements that is cost effective, and risk managed to maintain the integrity of the service.
- Agree the commercial terms for any exit services required from Fujitsu
- Agree the new supplier's transition timescales, with the aim of ensuring a seamless transfer of services.

Service Levels

Technical response times for the Fujitsu Managed Security Services are outlined below:

Objectives for Availability Incident Resolution Time

Service Measure	Description	How it is measured	Service Level
Priority 1 Security Event	Support Team will call you within 30 minutes of a Security Event being classified as Priority 1 Security Event	Measured from the time that the work is formally assigned to the appropriate Support Team resolver group until the first attempt by the Support Team to call you. Measured in minutes and seconds within the applicable Hours of Service.	≥90%
Priority 2 Security Event	Support Team will call you within 60 minutes of a Security Event being classified as Priority 2 Security Event	Measured from the time that the work is formally assigned to the appropriate Support Team resolver group until the first attempt by the Support Team to call you. Measured in minutes and seconds within the applicable Hours of Service.	≥90%

Table 1 Availability incident Resolution Time

Objectives for Security Incident Response Time

Service Measure	Description	How it is measured	Service Level
Priority 1 Security Event	Support Team will call you within 30 minutes of a Security Event being classified as Priority 1 Security Event	Measured from the time that the work is formally assigned to the appropriate Support Team resolver group until the first attempt by the Support Team to call you. Measured in minutes and seconds within the applicable Hours of Service.	≥90%
Priority 2 Security Event	Support Team will call you within 60 minutes of a Security Event being classified as Priority 2 Security Event	Measured from the time that the work is formally assigned to the appropriate Support Team resolver group until the first attempt by the Support Team to call you. Measured in minutes and seconds within the applicable Hours of Service.	≥90%

Table 2 Security Incident Response Time

Pricing

Fujitsu's Lot 3 Data Protection Service is highly flexible, scalable, and customisable, with the final price being determined very much by individual customer requirements. As there are many customisable options, pricing can only be determined once the Contracting Authority's environment, infrastructure, skills, and desired outcomes are established. As such, an initial scoping and discovery activity (conference call) will be undertaken to determine your resource profiles and requirements so that pricing may be provided

Fujitsu can collaborate with you to develop alternative commercial models, this includes financing options that would allow the spreading of capital expenditure over the term of a contract, effectively removing the capital expenditure requirements and delivering the consulting and technology elements as operational costs.

Commercial

Ordering and Invoicing Process

You will be invoiced for the charges on completion of the set up and provisioning of the Managed Security Service and a monthly in arrears charge for the ongoing management of the service. When remitting payment, you will include the applicable Fujitsu invoice that the payment applies to.

Minimum and Maximum Terms

There is a minimum term of 12 months

Termination Terms

You may terminate a Managed Security Service (MSS) by giving not less than ninety (90) days' notice to the other party. Should you decide to terminate the Service, termination fees will apply as detailed within the contract and will be dependent upon the specific MSS being terminated. Additionally, should you terminate a service, you shall be liable for any Software Licensing or Hardware support costs that arise because of the early termination.

Supplier Termination

Fujitsu may terminate a service by giving not less than ninety (90) days' notice to you.

Consumer Responsibilities

Successful delivery of the Fujitsu Managed Security Service is subject to the following dependencies upon you:

- Maintain the applicable Customer Security Policy regarding the services.
- Advise and agree any security testing with Fujitsu prior to commencement.
- Notify Fujitsu of potential Security Incidents via the Service Desk using the agreed method of incident logging.
- Promptly log all Security Incidents with the required details of the Security Incident.
- Use all reasonable endeavours to ensure that no incidents are reported which relate to equipment and services that are beyond the scope of the Support Services.
- Deploy software components onto servers for log file collection (for example agents) and install all pre-requisite patches and applications within agreed timescales.
- Provide Fujitsu with timely access to customer equipment and designated customer staff
- Utilise the Fujitsu-provided software in accordance with the prevailing license terms.

Service Constraints

Fujitsu shall not be liable for the customer's take up, non-take up or other discretionary use of the information provided by Fujitsu or of any of the recommendations or options generated from the Service and activities under this Service Definition.

Service Exclusions

The following elements are not included in the Service and are therefore not included within this Service Definition:

- Hardware and software; plus, ongoing licensing and support. These would need to be defined as part of the initial requirements definition with you.

About Fujitsu

As one of the world's leading IT companies, Fujitsu is at the forefront of pioneering technology in the UK since we made our initial investment over 40 years ago. As a key strategic partner we deliver essential services, from our secure hybrid IT which underpins critical national infrastructure to our investment in emerging technologies to boost national capability. Drawing on our Japanese technology expertise we provide bespoke digital transformation solutions. This unrivalled expertise has allowed us to specialise in emerging focus areas; Hybrid IT, AI & RPA, Data analytics, Agile application development/transformation and Security. Together, we offer a full package of solutions to support the UK as a long-term industry supplier.

We believe in realising the significant alignment between the UK and Japan in emerging technologies and in creating a UK-Japan 'Innovation Bridge' to support the UK's science and technology superpower objectives. We are committed to investment in UK skills and research and development, driving customer outcomes and promoting social value. We employ 124,000 people around the globe, including around 8,000 people across the UK, promoting diversity and inclusion as a DWP Disability Confident Leader. We are recognised as a Times Top 50 employer for Women since 2017, a Stonewall Top 100 Employer for 2023 and were awarded an EcoVadis Silver Rating, the world's largest provider for sustainability ratings.

Contact: government.frameworks@fujitsu.com