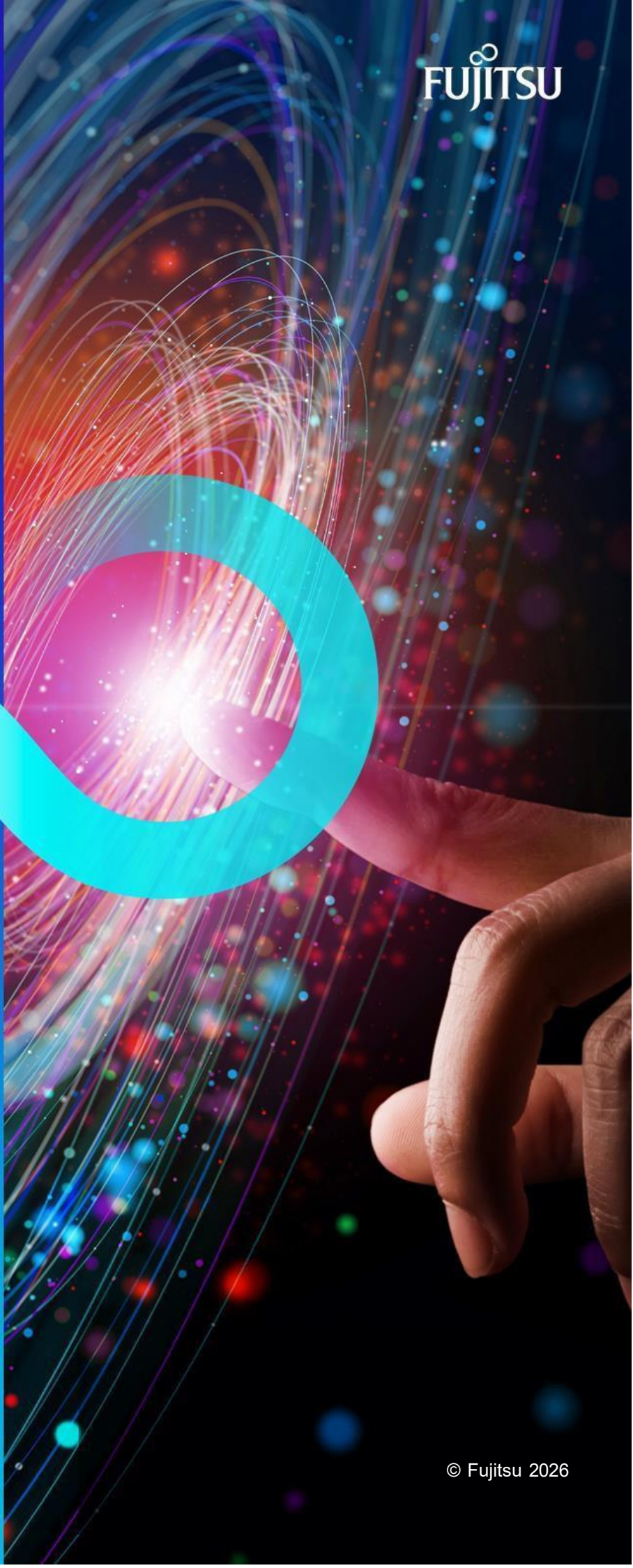
Service Definition

Identity and Access Management Service



G-Cloud 15

Contents

Managed Security Service 3
Why Choose Fujitsu 4
Confidentiality and Integrity 4
Strategic Technology Partners 4
Security Portfolio 4
Managed Security Service Pillars 5
Scope 6
Overview 6
Identity and Access Management Services 6
Identity and Access Management (IAM) 6
Privileged Access Management (PAM) 7
Certificate Management (PKI) 8
Business Continuity 8
Training and Consultancy 8
Additional Service Options 9
Onboarding and Offboarding 10
Onboarding 10
Offboarding 10
Service Levels 11
Objectives for Availability Incident Resolution Time 11
Objectives for Security Incident Response Time 11
Pricing 12
Commercial 13
Ordering and Invoicing Process 13
Minimum and Maximum Terms 13
Termination Terms 13
Supplier Termination 13
Consumer Responsibilities 13
Service Constraints 13
Service Exclusions 13

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 evolving technologies and develops a roadmap of technologies which are relevant to the mass market and to specific industries.

Fujitsu recognise 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 document.

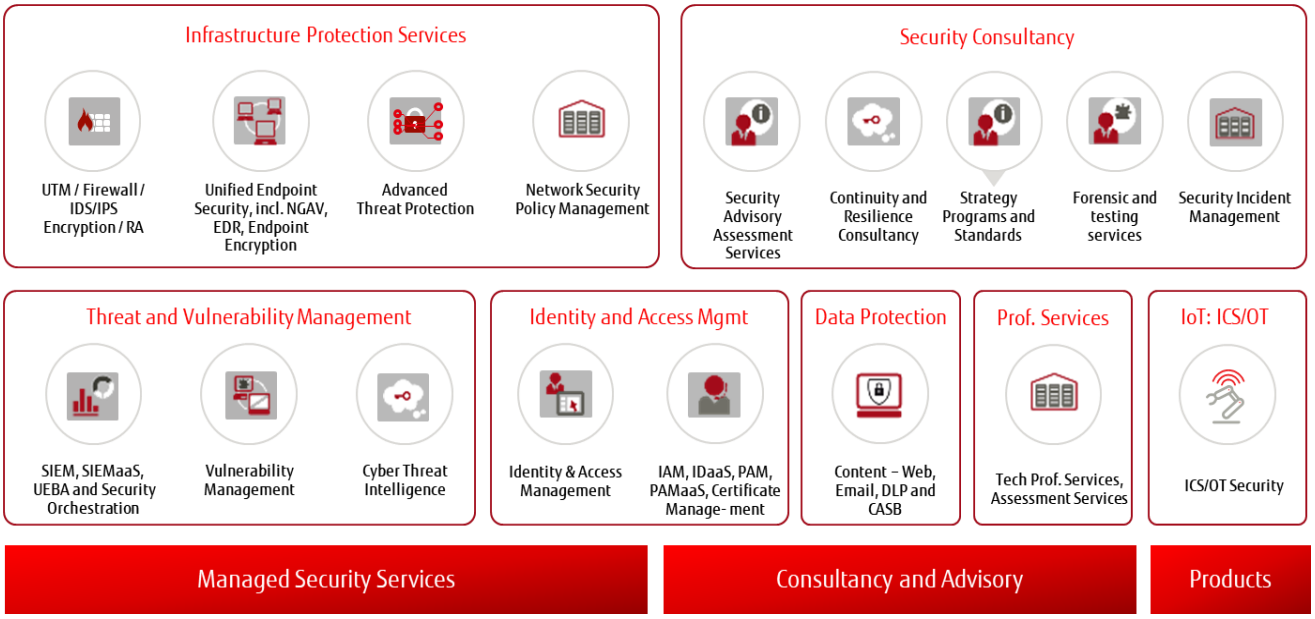


Figure 2: Security Portfolio

Managed Security Service Pillars

Each Fujitsu's managed security services is underpinned by technologies that are aligned to one of four service pillars; these include:

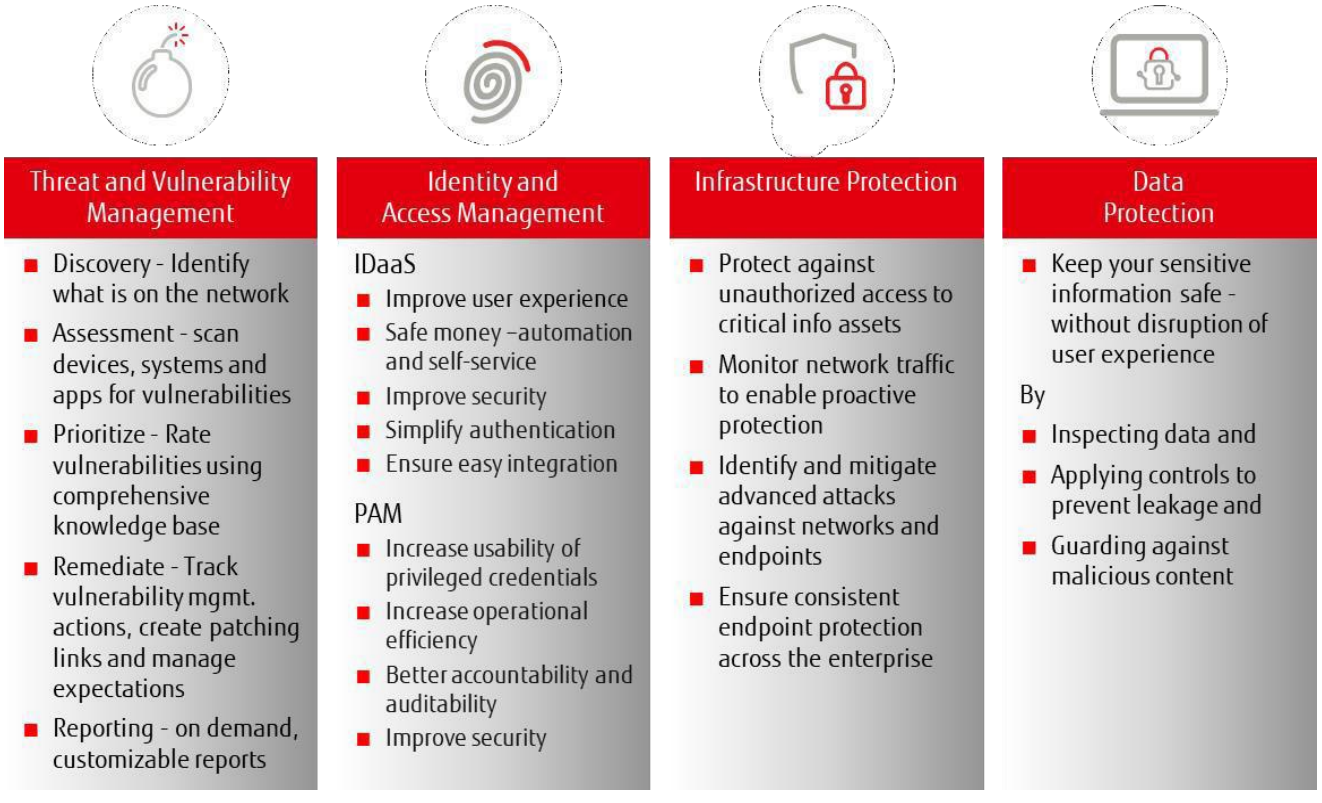


Figure 3: Managed Security Service Pillars

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.

Identity and Access Management Services

Fujitsu’s Identity and Access Management solutions provide you the freedom to manage users' access to relevant systems, applications, data, and resources, all in one place. Fujitsu have multiple service and pricing models available, including as-a-Service model, underpinned by best-of-breed technologies from partners.

Fujitsu's Security Operations Centres (SOCs) deliver a 24x7 MSS that enhances an organisations information security posture through continuous monitoring and the management of security services.

The services are:

- Identity and Access Management (IAM)
- Privileged Access Management (PAM)
- Certificate Management (PKI)

Identity and Access Management (IAM)

With freedom to manage users' access to relevant systems, applications, data, and resources all in one place, passwords and IDs stay safe and under your control, whilst compliance requirements are met.

All users can conveniently access the specific resources they need in a heterogeneous business environment, with single sign-on and self-service features, e.g., password reset for cost-effective management. Meanwhile, you can easily keep user credentials safe, controlled and in line with existing security policies - even if users are accessing cloud services.

Fujitsu’s IAM solutions relieves the complexity of securing users across multiple clouds, allowing you to get on with securely delivering agile services to customers.

The result is a complete, end-to-end identity management and governance solution for your entire organization.

- Improve user experience - with single sign-on, easy login to all systems

- Save money - using automation and self-service to create, manage and modify permissions
- Improve security - with strict policies, real-time monitoring and reporting of permissions and usage
- Simplify authentication - with resilient methods including single sign-on, multi-factor authentication, biometric identity, and access management
- Ensure easy integration - with full support of open interfaces and standards, e.g., Security Assertion Markup Language (SAML) and System for Cross-domain Identity Management (SCIM)

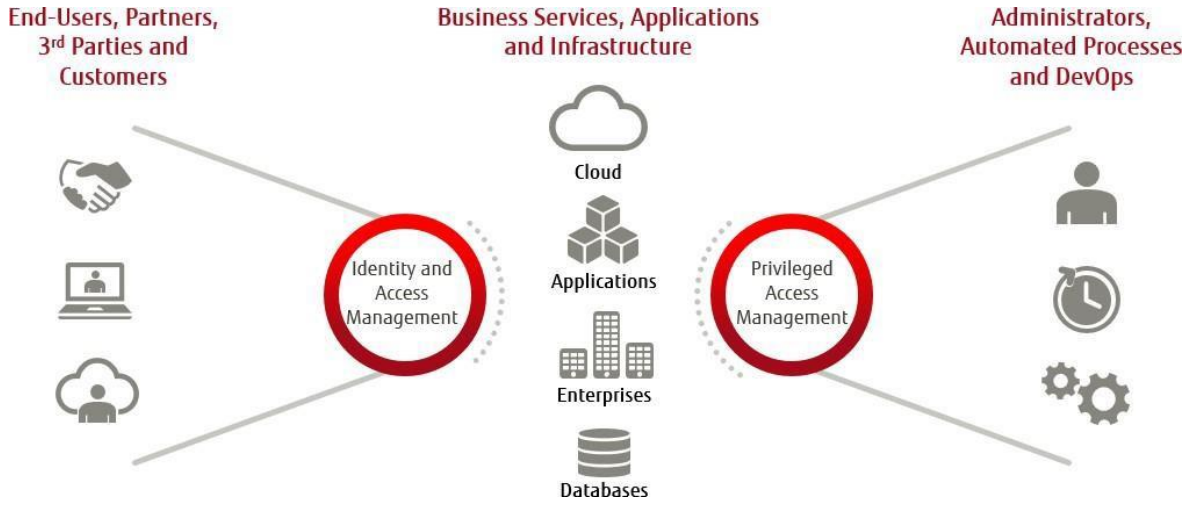


Figure 4: Identity and Access Management

Privileged Access Management (PAM)

Certain employees in organisations have specialist usage rights to access sensitive information. For example, business administrators and developers can install software, create new users and accounts, and other actions. These high-level access rights are extremely attractive to cyber criminals. If breached, this can cause substantial disruption and even long-term damage.

Fujitsu's Privileged Access Management (PAM) solutions are designed specifically to keep your environment safe. Featuring a higher level of security with enhanced controls and traceability features, PAM integrates easily with your existing operations and access infrastructure to create a cost-effective, compliant solution. Environments could be anywhere - on premise or in the cloud or hybrid.

Privileged Access Management provides:

- Increased usability of privileged credentials
- Increased operational efficiency – cost-effective
- Improved accountability and auditability
- Enhanced security which helps to meet compliance and regulatory requirements

Figure 5 Privileged Access Management

Certificate Management (PKI)

Public Key Infrastructure (PKI) and Certificates are the foundation of many identities and security features. For example, device identities (workstations, servers, IoT devices, etc.) rely on certificates. If this foundation is poorly managed and vulnerable, it can collapse, causing significant financial and reputational loss , as well as disruption to your services.

Fujitsu's Certificate Management services takes care of internal and external certificates, ensuring a trustful and solid foundation for your digital business environment. Fujitsu's Certificate Management Services consists of two offerings.

External Certificate Management

Secure and trusted access and communication with your services is key to a successful and effective business. Widely trusted and well managed SSL certificates enable trust for your services and guarantee business continuity, whilst also protecting your reputation and brand.

- Fully managed service includes SSL certificates from globally trusted Certificate Authority
- Optimized usage and costs of SSL certificates according to your business requirements

Internal Certificate Authority

Fujitsu's Internal Certificate Authority service takes care of your internal Certificate Authority (CA) and all the certificates issued from it. This service provides many levels of secure key management, including hardware security modules (HSM) and HSM as a Service. Poorly managed CA and poorly secured CA keys are often the most common issues that organisations face.

Commonly, this service is known as Microsoft PKI Management or Microsoft CA Management.

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 an 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 and enhancement and ancillary services options, 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 underpinned 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 work 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 work 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

Severity	Title	Definition	Resolution Time	% Target
1	Critical	Severe business disruption: business unit or sub-unit unable to operate, critical system component failed or severely impaired	4 hours	95
2	Major	Major business disruption: critical user or user group unable to operate, or business unit experiencing significant reduction in system performance	8 hours	90
3	Medium	Minor business disruption: single user unable to operate with no circumvention available	16 hours	90
4	Low	Minor disruption: single user or user group experiencing problems, but with circumvention available	3 days	90
5	Very low	Enquiry: single user or user group requiring assistance but with no direct impact on business. For example, a request for information. Also used for change requests.	5 days	80

Table 1: Availability Incident Resolution

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 work 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 customer 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