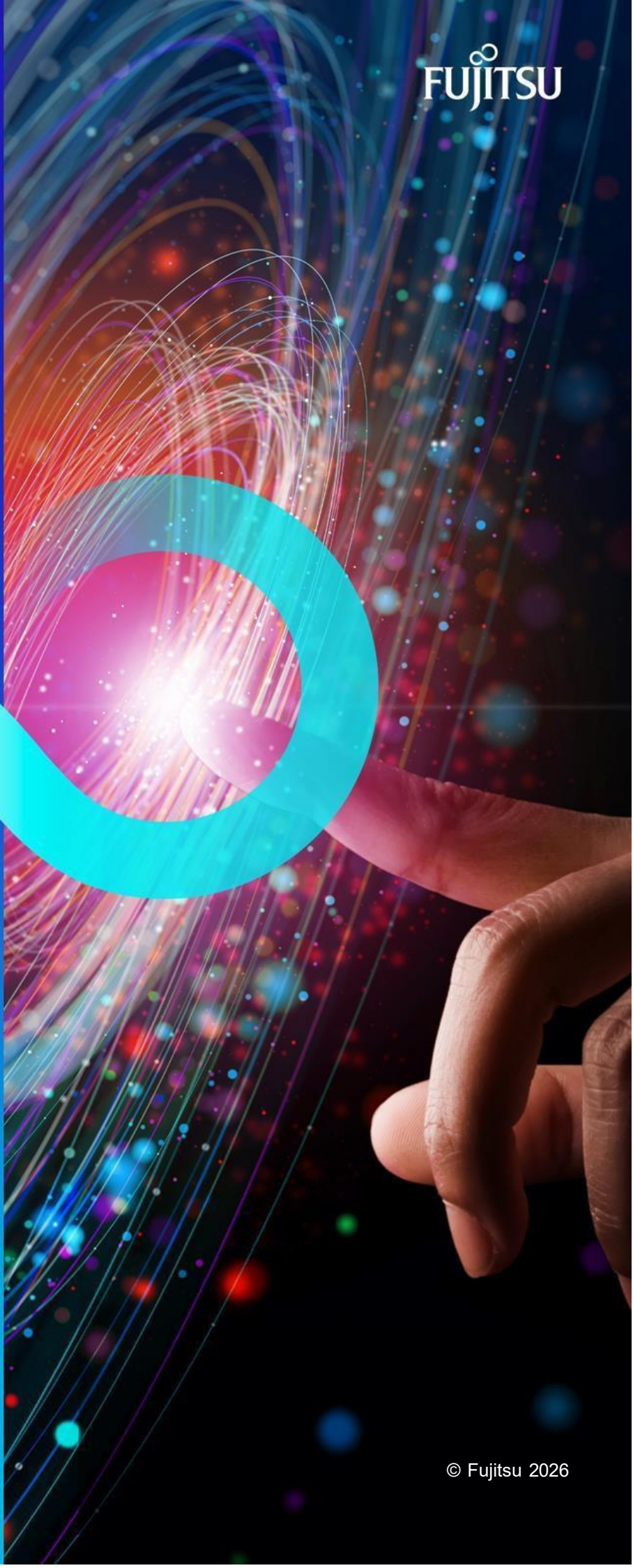
Service Definition

Data Protection Services



G-Cloud 15

Contents

Managed Security Services

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 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 possess extensive experience in designing, building, and managing and maintaining ISO 27001:2013 certified Information Security Management Systems (ISMS) for our clients. This expertise is particularly critical for HMG departments handling data classified from OFFICIAL through to SECRET and above, ensuring a systematic and robust approach to managing information security risks and achieving compliance.
- 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

In today's rapidly evolving digital landscape, safeguarding sensitive data—whether at rest, in transit, or in use—is not just a priority, it's an imperative. Escalating compliance mandates and the severe financial and reputational penalties for breaches make 'keeping your house in order' more complex and critical than ever. The challenge lies in precisely identifying and implementing the right security controls, in the right places, without stifling innovation or operational efficiency.

Fujitsu's comprehensive data security services empower your organisation to proactively protect its most sensitive information and critical assets. We achieve this by providing deep visibility into your data's lifecycle, meticulously analysing access patterns, and implementing granular controls over who and what interacts with your valuable information. This intelligent approach moves beyond generic security, allowing you to apply precisely the appropriate level of protection where it's needed most.

Leveraging a broad portfolio of industry-leading network and endpoint security controls, Fujitsu goes beyond simply deploying technology. We strategically integrate these controls to continuously monitor, manage, and adaptively strengthen your organisation's entire information security posture. This holistic approach simplifies the complexity of security management, ensuring your defences are always optimised against evolving threats and compliance requirements. Partner with Fujitsu to transform your data security from a compliance burden into a strategic advantage, giving you the confidence to innovate securely

Strategic Technology Partners

Fujitsu leverages strategic relationships with leading global security vendors, ensuring our clients benefit from best-of-breed technologies seamlessly integrated into cohesive, end-to-end security services. Our expertise spans the entire lifecycle, from definition and design to implementation, testing, integration, and ongoing operation.

Our commitment to security innovation is underpinned by continuous threat intelligence and active monitoring of emerging technologies. Fujitsu proactively develops a strategic roadmap, ensuring our solutions incorporate the most relevant and effective advancements for both the broader market and specific industry sectors, thus future-proofing your security investments.

We understand the unique challenges faced by HMG clients, including the imperative to leverage existing investments, reduce operational complexity and cost, and rigorously evaluate all technology options (including Open Source). Furthermore, we recognise the critical need for partners who can meet stringent HMG support requirements for assurance and dedicated focus. To meet these exacting standards, Fujitsu strategically cultivates

and manages mutually beneficial relationships with key security vendors. This ensures we can deliver optimal project outcomes, streamline service and contract management, and provide the enhanced resilience and support critical for government operations.

Our carefully curated portfolio of security technology partners is a testament to our comprehensive managed and professional services capabilities, enabling us to deliver tailored, robust, and integrated security solutions that address every aspect of your security posture.

Security Portfolio

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

Figure 2: Security Portfolio

Scope

Overview

In today's interconnected world, organisations face an unprecedented barrage of cyber-attacks. Threat actors are no longer relying on simple exploits; they are executing sophisticated, multi-stage incursions. These involve a blend of exploiting vulnerabilities, leveraging social engineering, orchestrating data theft, and deploying targeted spear-phishing techniques to establish persistent, advanced, and often zero-day threats.

Regular publicity serves to highlight the sheer frequency and devastating impact of these advanced threats. Industry analysts paint a stark picture, estimating that:

- There are now over 1.4 billion pieces of malware programs in circulation.
- 560,000 new pieces of malware are detected every single day.
- Every minute, four companies fall victim to ransomware attacks, causing significant disruption and financial loss.
- Trojans alone account for 58% of all computer malware, underscoring the prevalence of stealthy infiltration tactics.

Effectively combating this relentless threat landscape demands a holistic and integrated approach, where people, processes, and cutting-edge technology converge to form a resilient defence for individuals and organisations alike.

Successfully detecting and containing these advanced threats necessitates a strategically coordinated approach. This involves deploying multi-layered countermeasure solutions that establish a unified, proactive, and vigilant security posture, delivering robust controls across all levels of your digital estate.

Unparalleled visibility is paramount for preventing, detecting, and effectively containing security threats. Without this complete insight, harmful incursions can remain undetected and unchallenged, leaving organisations critically exposed. This lack of visibility directly translates into heightened risks, forcing organisations to re-evaluate their vulnerability to significant reputational damage and their capacity to respond effectively during a crisis

Data Protection Services

Fujitsu's Data Protection Services are meticulously designed to safeguard your sensitive information, ensuring robust security without compromising essential user experience or business continuity. We achieve this through intelligent data inspection and granular control application, proactively preventing data leakage and providing a resilient defence against malicious content, whether at rest, in transit, or in use.

Complementing this, Fujitsu's state-of-the-art Security Operations Centres (SOCs) provide 24x7 Managed Security Services (MSS). These dedicated SOCs actively monitor, detect, and respond to threats around the clock, continuously enhancing your organisation's information security posture through expert oversight and proactive management of all security services.

The services are:

- Web Security Managed Service.
- Email Security Managed Service.
- Cloud Access Security Broker (CASB).
- Data Loss Prevention (DLP).
- Enterprise Data Encryption.

Web Security Managed Service

Fujitsu's Web Security services are engineered to comprehensively safeguard your critical data and digital assets across both public and private networks, ensuring secure and resilient online operations.

We leverage a curated portfolio of market-leading web security products, selected through a rigorous evaluation process to ensure best-fit solutions that align with your unique threat landscape and operational requirements.

Our expert professional services team acts as a true partner, guiding you through the entire security lifecycle. This includes in-depth risk assessment, precise requirements definition, bespoke technical and service design, and robust architectural planning. We then ensure the seamless and effective deployment, integration, and ongoing operation of these solutions, providing continuous protection and peace of mind.

Fujitsu's Web Security service includes the following solution dependent features:

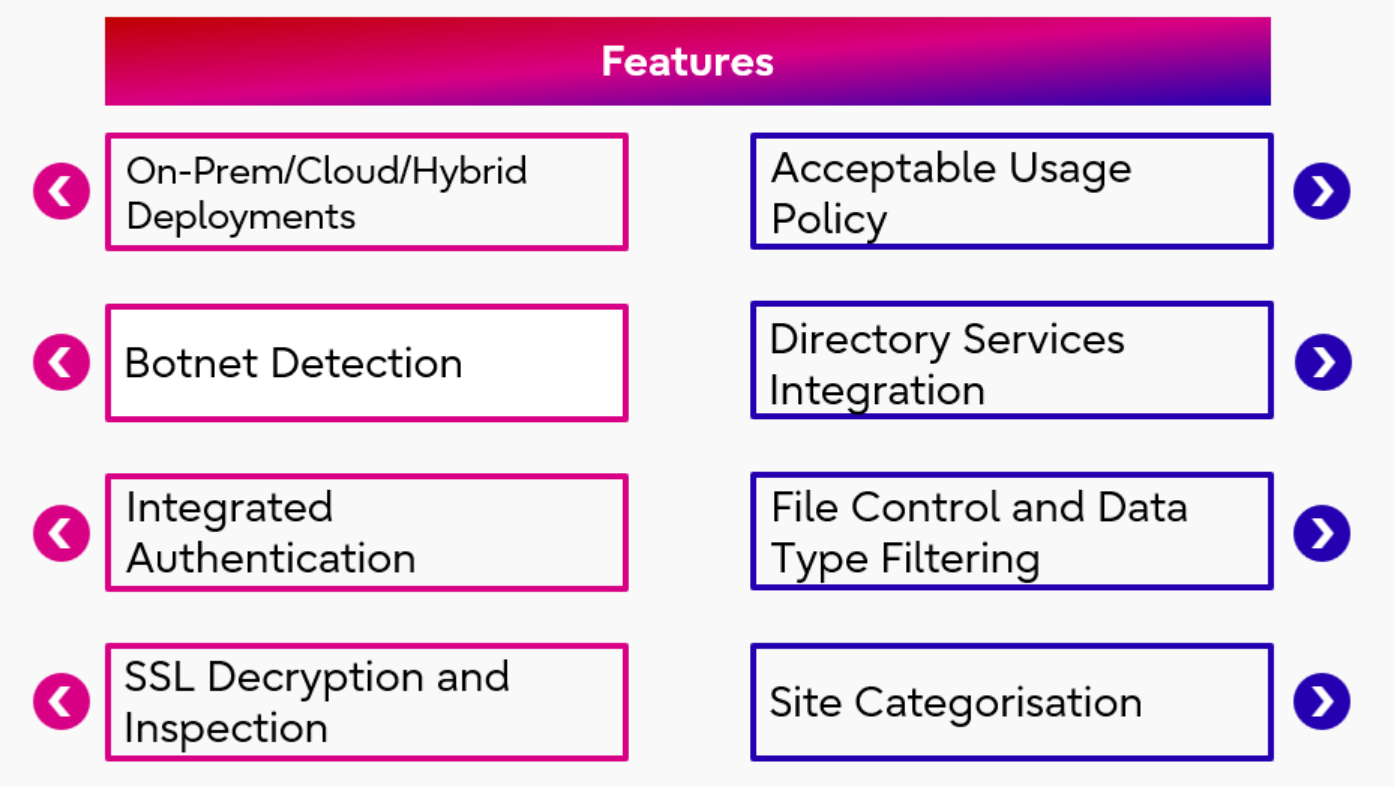


Figure 4: Web Security Managed Service

The Web Security Managed Service provides web content protection, monitoring and management. This is a 24 hours x 7 days a week service, it is designed to allow the Customer to enhance their information security defences through continuous monitoring and proactive blocking of malicious content, protecting users, infrastructure and services

Email Security Managed Service

We recognise email as a primary gateway for cyber threats, Fujitsu's Email Security service is meticulously designed to provide robust, multi-layered protection for your critical data across both public and private networks.

This comprehensive service is underpinned by best-of-breed email security products from our strategic technology partners, ensuring advanced defence against phishing, malware, spam, and other sophisticated email-borne threats.

Fujitsu's security professional services team collaborates closely with your organisation, offering end-to-end support from initial risk assessment and precise requirements definition to tailored technical and service design, and robust security architectures. We ensure the seamless deployment, rigorous testing, and continuous, effective operation of your email security solution, customising it to your unique environment.

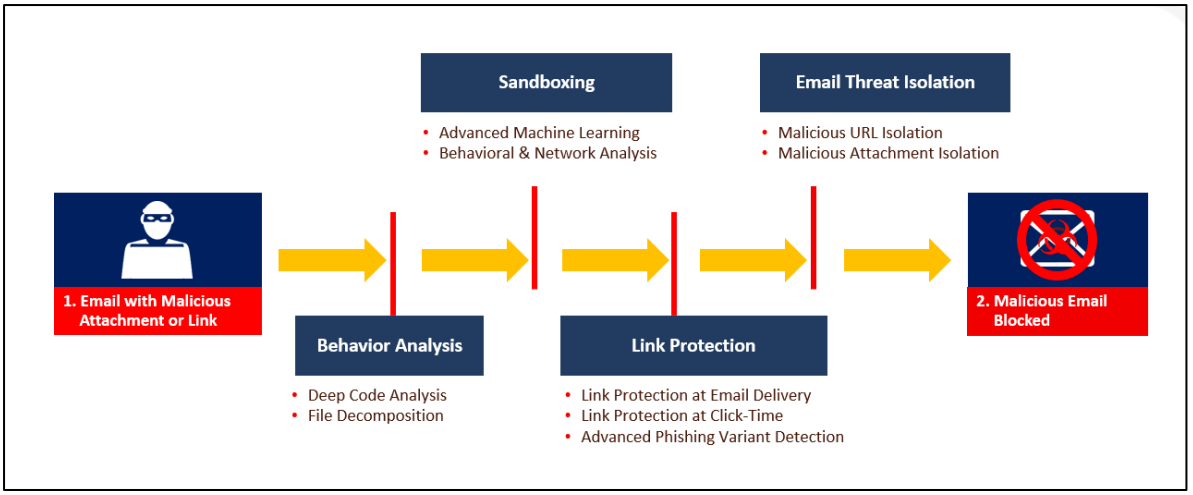


Figure 5: Email Security Managed Service

Fujitsu's Email Security service can provide:

- Inbound and outbound email content inspection
- Mitigation against malicious email based on security threats
- Flexible on premise, Cloud based or hybrid solutions.
- Centralised enforcement of security policies at group and user level.
- Centralised archiving and reporting management.
- Integration options with web security and DLP solution.

Cloud Access Security Broker (CASB)

As cloud adoption becomes the default, securing your data and applications across diverse cloud environments becomes paramount. Fujitsu's Cloud Access Security Broker (CASB) proposition offers a structured and adaptable approach to gaining comprehensive control and management over your organisation's cloud usage.

Our consultancy-led engagement process is fundamental to our approach. We work closely with you to thoroughly understand your unique cloud security requirements, ensuring the CASB service is precisely tailored to your specific policies, compliance needs, and operational context.

The Fujitsu CASB Managed Service delivers proactive cloud application monitoring and robust security management to enhance your cloud security defences, through increased visibility, proactive control of activities and continuous monitoring of your multi-cloud environments.

Fujitsu's CASB Managed Service can provide:

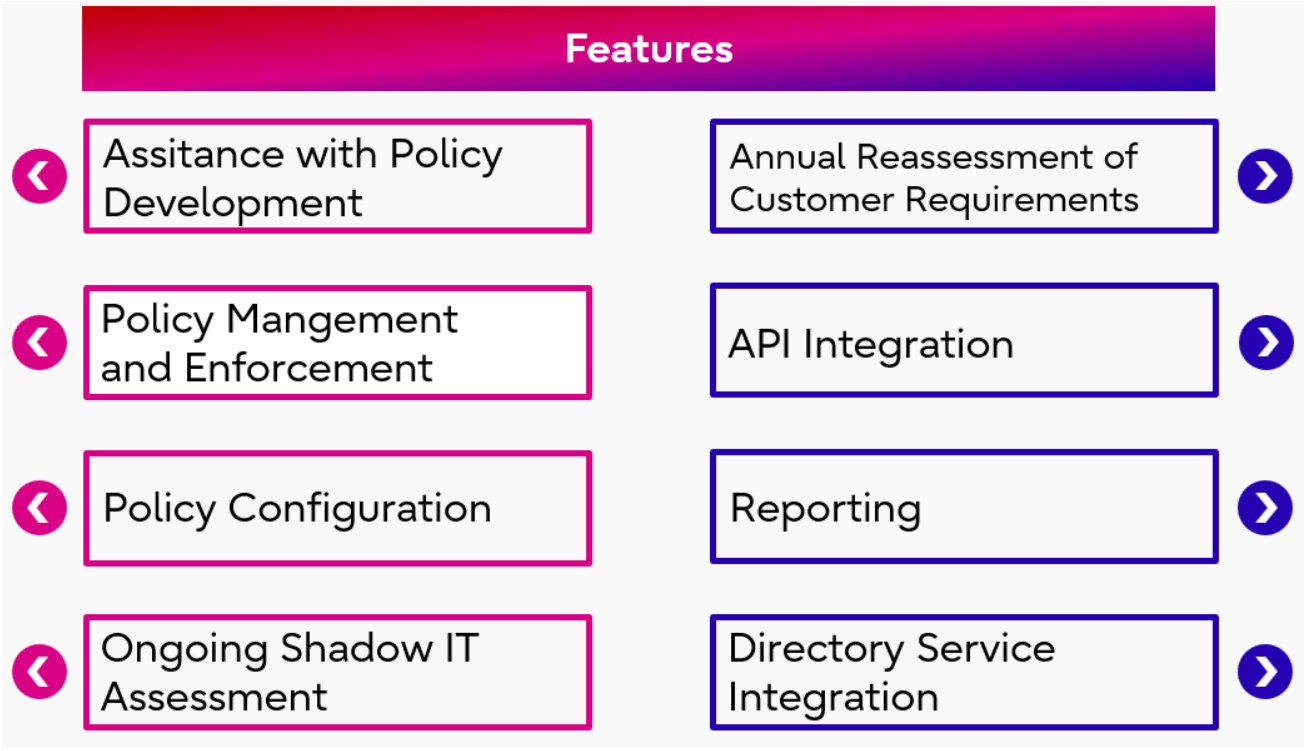


Figure 6: CASB Managed Service

The CASB Managed Service provides cloud app monitoring and management. This is a 24 hours x 7 days a week service, it is designed to allow the Customer to enhance theircloud security defences through improved visibility, continours monitoring and proactive control of activities that would otherwise expose sensitive data within cloud environments.

Data Loss Prevention (DLP)

Fujitsu's Data Loss Prevention (DLP) Services are meticulously designed to inspect, identify, and protect information you deem sensitive, ensuring it never leaves your control without authorisation. Our expert consultants engage proactively with your organisation from the initial strategic 'visioning' phase, enhancing conventional problem-solving to collaboratively develop a bespoke DLP strategy. This strategy is meticulously aligned with your overarching business objectives, regulatory landscape, and evolving threat profile.

Fujitsu's comprehensive DLP Managed Service delivers end-to-end protection, encompassing critical phases such as:

- Intelligent Data Classification: We collaborate with your organisation to precisely define and categorise the sensitive information that requires protection, aligning with your business policies and regulatory obligations
- Continuous Data Discovery: Our service actively locates sensitive information, whether it's at rest within your infrastructure (on-premise or cloud), in motion across your network, or in use within cloud applications. This ensures no sensitive data goes unnoticed.
- Dynamic Data Protection: We implement adaptive protection mechanisms that range from educating users with real-time warnings to enforcing robust controls like mandatory data encryption, redaction, or outright blocking of unauthorised transfers. Our unified policy engine ensures consistent protection for both on-premise and cloud-based data.

Enterprise Data Encryption

Fujitsu Enterprise Data Encryption service has incorporated technology, from a market leading technology partner, which meets Federal Information Processing Standards (FIPS) 140-2 (up to Level 3) and Common Criteria EAL4+ standards; with Encryption Key Management best practice aligning to NIST SP 800-57. The service couples a key management service with a range of Customer selectable encryption services to meet corporate data privacy requirements in Hybrid Cloud environments, such as:

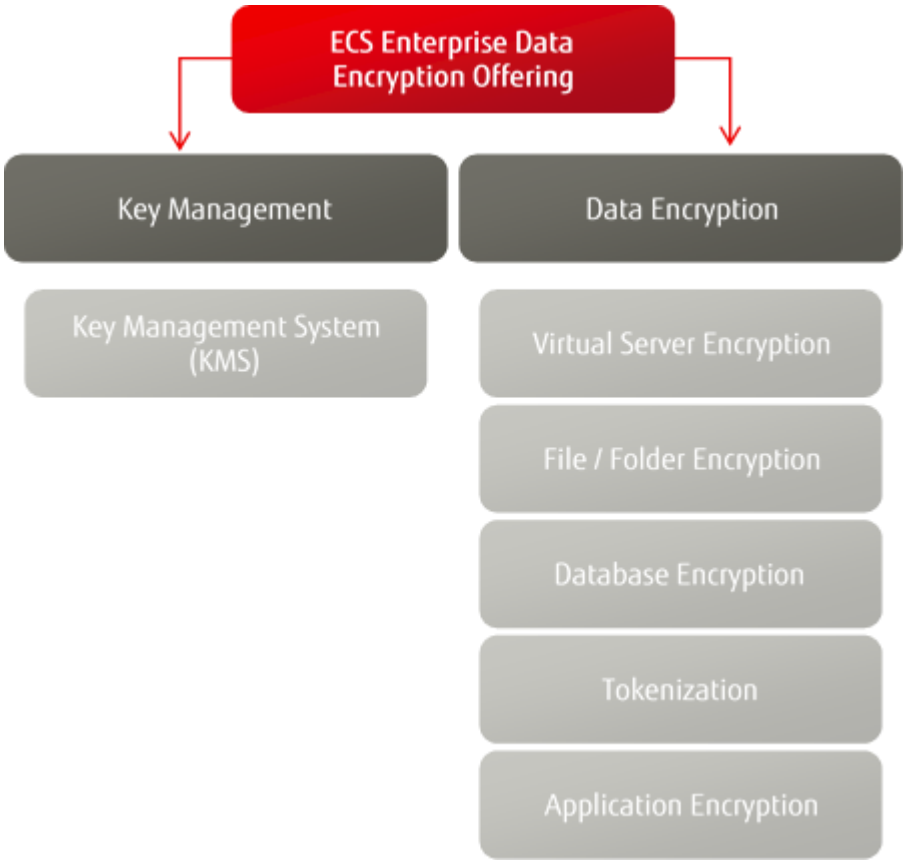


Figure 7: ECS Enterprise Data Encryption Offering

Fujitsu Enterprise Data Encryption Offering is comprised of a Key Management Service that consists of selectable Data Encryption Services.

You can purchase a combination of these services to:

- Align to your corporate data protection policies
- Meet regional data protection regulations
- Meet industry specific compliancy across a wide range of industries

Service Delivery

Service Management

Fujitsu's Managed Security Services (MSS) are delivered with unwavering reliability and adherence to global best practices, underpinned by an ITIL-aligned and ISO/IEC 20000 compliant service management framework. This robust governance ensures consistent service quality, operational excellence, and a mature approach to security management for your organisation.

Fujitsu is committed to the proactive implementation and diligent maintenance of all agreed MSS policies. Recognising the dynamic nature of cyber threats and evolving business requirements, any necessary changes to these policies are managed through a transparent and agile Managed Service Change process. This approach fosters co-creation and continuous stakeholder engagement, ensuring policies remain relevant, effective, and fully aligned with your organisation's evolving security posture.

Our comprehensive MSS is structured around the following principal elements, designed to provide layered and adaptive protection and contains the following 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 several 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 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.

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