G Cloud 15
BT Service Definition for BT Managed Firewall Security Next Gen Full VAS (Virtual)

Contents

1 Product Overview

1.1 Introduction

The Managed Firewall Security (MFS) service, provided by the Supplier's Security is part of the Managed Security Services (MSS) portfolio. This document provides the definitive statement of what is included within the scope of the service as standard and indicates some of the main optional elements that may be offered over and above the standard. Buyers will need to engage with the Supplier in order to identify and scope their requirements prior to placing an order.

This service will be provided as a Virtual Machine (VM)-based firewall from either Fortinet, Palo Alto or Check Point.

1.2 High Level Service Overview

MFS provides a flexible framework for firewall and related security features, to fit different Buyer requirements. The Supplier provides service options for all stages of the Buyer "journey"; requirements capture, solution design, equipment procurement, installation and commissioning, in-life management, in-life security policy changes, in-life service changes.

MFS offers a fully managed service. Buyers retain responsibility for setting their security policy, and then the Supplier will manage all other aspects of the service. However, Please note that, at present, the Supplier is unable to provide the underlying AWS & Azure infrastructure. This must be provided and owned by the customer.

The Supplier's service management draws on its extensive experience in Buyer service and in managed security. The Buyer will call their local Helpdesk as first point of contact, and security support issues will be passed to BT's Security Operations Centre (SOC). The latter are quality accredited (to ISO27001 "Information Security Management") to assure the procedures and systems that handle sensitive Buyer information.

MFS will service domestic or multi-national Buyers. It is targeted towards companies who are moving their workloads to the cloud; protecting against associated threats, but supporting key business needs for controlled access to information. Buyers will usually be aware of the security threats, and of appropriate responses. However, whilst they may have previously attempted to implement security solutions themselves, they will be increasingly interested in the advantages of outsourcing aspects of their security requirements to a Managed Security Service Provider (MSSP). The internal challenges they will be facing include the costs and feasibility of tackling:

- recruiting and retaining the right people to provide 24x7 global response
- increasing sophistication of targeted hacking

- increasing volume of "nuisance" attacks; e.g. phishing, malware
- increasing incidence of extortion attacks
- increasing design complexity to enable online applications
- increasing need for high levels of resilience
- difficulty managing changes to network and security infrastructure; e.g. for new sites or for capacity upgrades

Hence the Supplier will be a strong contender to provide Managed Security Services;

- genuinely global reach
- high levels of accreditation and expertise, supported by strong vendor relationships
- brand credibility, sustainability, and trust
- cost effective and predictable cost solutions

The proposal is not to take over an organisation's security responsibilities. However, the Supplier can provide solutions that "outsource the grunt work", leaving the Buyer free to concentrate on broader security questions of organisational policy and compliance, user support and training, allowing them to concentrate on core business issues and enabling business capability/ flexibility.

As a virtual firewall offering, this will enable the Buyer to benefit from faster and more flexible provisioning, modification, cease and lack of CPE installation and maintenance costs.

1.3 Features Set Summary Tables

1.3.1 Summary Tables

The following Table 1 summarises each service component feature as a quick guide. Further information on each feature can be found in the appropriate section.

Various 'business rules' apply to which combinations may be chosen. The main points to note are that some categories are standard and must be taken (though there may be some choice within a category), and some are optional (which the Buyer may choose to take or not).

The "Included or Charged" column denotes whether each feature is explicitly charged for or included in the licenses or management fees.

This service description deals primarily with a fully managed service;

- Licences, matching requirements against options shown
- Service Provision; included
- Fault Management; included
- Configuration Management; included

- Performance Reporting; included
- Service levels; included

Note that platform services are included in the table below for information only, and because the choice has a bearing on how the MFS is designed, delivered and managed. They do not form part of the scope of this service.

Finally, note that the options below are limited to Fortinet, Palo Alto and Check Point as the supported vendor and are based on a virtual firewall.

Feature	Included or Charged	Comments
Platform Services		
Azure public cloud AWS public cloud	Not included. This must be provided by the buyer	For virtual appliances, it is the buyer's responsibility to provide the underlying public cloud infrastructure from either AWS or Azure. The buyer can then provide management access to their VM through the Supplier's IMPSS platform.
Licences		
Fortinet virtual FortiGate - Standard	Included	The following options are available for Fortinet virtual firewalls: VM04, VM08, VM16, VM32, VMUL What model of licence the Buyer will need will be based on their usage and throughput which will be discussed with the Buyer. The Next Generation firewall will have optional UTM features enabled. The Buyer will be charged one price for 1 or more of these features.
Fortinet virtual FortiGate – Next Generation	Included	
Palo Alto virtual firewall – Standard Palo Alto virtual firewall – Next Generation	Included	Palo Alto's range of virtual firewalls suitable for deployment in AWS and Azure environments can be found by getting in touch. The Next Generation firewall will have optional UTM features enabled. The customer will pay one price for 1 or more of these features. What model of license the customer will need will be based on their usage and throughput which will be discussed with the Buyer. Palo Alto's VM Flex Series enabling users to create a deployment profile to configure one or more firewalls based on PAN-OS version, the number of vCPUs per firewall, the total number of firewalls supported by the deployment profile,

Feature	Included or Charged	Comments
		Panorama/Strata Cloud Manager management or log collection, and security services.
Check Point virtual firewall – Next Generation	Included	Note that there is no Standard / basic virtual firewall (i.e. only offering packet filtering or stateful inspection) available from Check Point. Instead Check Point's Next-Gen Firewalls are designed to be competitively priced whilst offering a range of UTM features. Check Point's virtual firewall offering (known as CloudGuard) is licensed by the number of virtual cores (vCores) assigned to the virtual machine running it. Details on Check Point's CloudGuard Network VMs can be found here: CloudGuard Network - Product Catalog - Check Point
UTM / Next Generation Services • Intrusion Prevention • Web URL Filtering • Web AV • Identity Awareness • Application Control • Anti-Bot • Threat Emulation	Included (with UTM bundle licence)	Optional value-add services which the customer can select in order to increase the level of security provided by the appliance. These features require a different software licence to that required for a Standard firewall, with appropriate sizing of the selected appliances also being needed. For Fortinet solutions, Anti-Bot must be configured alongside Anti-virus. For Fortinet and Palo Alto solutions, the Threat Emulation service has a prerequisite requirement of the Anti-Virus feature. Palo Alto's Advanced Threat Prevention bundle includes IPS, Anti-Virus, Anti-Bot and Application Control Check Point offers two bundled licence options: NGTX which includes IPS, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam and Application Control. NGTP includes the above plus Threat Emulation.
User Authentication - Buyer authentication Device Authentication - Pre-shared key	Included	Any authentication must be provided by the Buyer.
Service Provision		
Managed Delivery	Included	Project-managed installation and commissioning by a desk-based project

Feature	Included or Charged	Comments
		co-ordinator (This will not be applicable for Manage Service MS 1.
Lead Times (from receipt of validated order) 10 working days	-	For virtual firewalls, the overall lead time will depend on the status of the existing or new network infrastructure the firewall is to be deployed over.
Fault Management		
Helpdesk – 24 x 7 x 365	Included	
Proactive Monitoring	Included	Continuous checks on firewall performance and integrity. Proactive Monitoring is provided as MS1, MS2 and MS3 pricing, according to the service supported.
Reactive Maintenance - 24 x 365 - 1-hour response - 4-hour fix	Included	Reactive Maintenance is provided as MS1/MS2/MS3 pricing, according to the service supported.
Configuration Management		
FW Policy Management	Included	Subject to acceptable use policy.
Vulnerability and Patching	Included	The Supplier will identify, test, and implement patches for High and Critical Vulnerabilities in accordance with the Buyer's authorisation. Vulnerability and Patching is provided as MS1, MS2 and MS3 pricing, according to the service supported.
Buyer Reports		
Device reports mainly include: - CPU utilisation - Memory utilisation - Interface throughput	Included	
Event Logging (Local)	Charged	Option to forward logs locally to a Buyer hosted FortiAnalyzer instance.
Professional Services		
FW Policy Production	Charged	
AD-Hoc Security Consultancy	Charged	

1.4 Channel and Product Responsibilities

Responsibility for delivering the complete service within this document is shared between the MFS product line and the selling channel that owns the Buyer relationship. As a guide, the core functions are owned and delivered by MFS product line with Buyer-facing activities owned by the channels. A list of the main activities (though not all) is shown below with the relevant ownership.

Function	Responsibility
Pre-Sales	
Sales Collateral (e.g. Service Description; Pricing; Contracts; Customer Requirements Form (CRF)	Product Line
Account Management	Channel
Technical Design and Commercial Qualification	Channel
Security Policy	Buyer & Channel
Provide access to device configuration where appropriate i.e. Azure Lighthouse	Buyer & Channel
Customer Proposals and contracts	Channel
Compliance to Service Description	Channel
Bid submission	Channel
Bid Authorisation	Product Line
Technical Design Authority sign off	Product Line
Provisioning	
Data Capture Form (DCF) completion, MFS contract	Buyer & Channel
Order Entry	Operations
Global Portal application - to include access to BT Security Change Manager	Channel
BT Security Change Manager – Buyer builds on system	BT Security Change Manager Support
Network access – ordering, tracking, liaising with Managed Security Services Project Manager	Channel
Procurement, Installation & Commissioning	Operations
Account / Contract Management	Channel
Customer Project Management	Channel
Project Delivery	GS DBPM
Customer Billing	Channel
In-Life	
First line Help Desk	Channel MFS contracts
• Raising faults to appropriate helpdesk using Expedio FM	Channel
Software/Configuration Management	Operations (SOC)
Proactive Monitoring	Operations (SOC)
Customer Service Management	Channel
Ongoing compliance to site planning guide	Buyer
Ongoing ownership of Security Policy	Buyer
Contract Management	Channel
Contract Renewal	Channel and Product Line
Optional Items	
Consultancy e.g. Security Policy Production	Systems Engineer

1.5 Country Availability

For the geographical availability of the virtual firewall, please refer to the latest version of the Managed Firewall Services DCF.

2 Detailed Service Components

2.1 Network / Platform Services

MFS does not directly include the provision of associated network / platform services Amazon Web Services (AWS & Azure), however, these services can be bought separately from the Supplier's Global portfolio and provided under a different contract.

Note that the Supplier will not be liable for service issues (e.g. performance of the service, delays in performing management activities, responding to faults) if the Buyer's arrangements for the provision of network services are found to be at fault.

2.1.1 Internet Access Dimensioning

It is the Buyer's responsibility to define their Internet access circuit bandwidth, sufficient to meet their requirements, plus provision for in-band management access from the BT SOC. The minimum additional bandwidth required for management purposes is 256 Kbps. The actual size will be determined during the design phase.

2.2 Equipment & Applications

2.2.1 Overview and Virtual Firewall Options

There is a choice of Virtual Firewall Options available from Managed Security Services (MSS).

Virtual Firewall - This option provides a managed firewall hosted on the Buyer provided infrastructure (including public cloud and private cloud). In the event of an infrastructure failure, the Supplier will work with the Buyer who will use their local procedures with the relevant infrastructure providing team to remedy the incident.

The following table summarises the ownership of different service elements for the Virtual Firewall Options:

	Supplier Owned	Buyer Owned	Supplier Takeover /Adopt	Service Wrap Only
Standard or Non-Standard	Standard	Standard	Non-Standard	Standard
Software maint ordering and renewal	The Supplier	The Supplier	The Supplier	The Buyer

The Supplier is responsible for ensuring software licences and any required vendor support contracts are placed and renewed for the term of the Buyer's contract with the Supplier. Prior to end of a contract term, unless the Buyer notifies the Supplier otherwise, the Supplier will extend 3rd party support contracts by one year (at a time).

If the Buyer subsequently cancels within the one-year period, they will be liable for costs incurred but not recoverable by the Supplier in renewing these licences and contracts.

2.2.2 Firewall Technology

The Fortinet firewall applications are based on Stateful Inspection technology. The firewall accesses and analyses data derived from all communication layers. The state and context data of each communication is stored and updated dynamically, providing virtual session information for tracking connectionless protocols (e.g. User Datagram Protocol (UDP)- based applications). Cumulative data from the communication and application states, network configuration and security rules, are used to generate an appropriate action, to accept, drop or encrypt the communication. Unified threat management capabilities are available such as Intrusion Protection Services (IPS), Anti-virus protection, Anti malware etc.

2.2.3 Firewall Licences

MFS currently supports the "Bring-Your-Own-Licence" (BYOL) option as standard on virtual firewalls. Note that Fortinet no longer offer "Pay-As-You-Go" (PAYG) licencing through their Fortimeter platform. However, PAYG licencing from all vendors can be considered on a case-by-case basis. BT will ensure all software licenses and any required vendor support contracts are placed and renewed for the term of the customer's contract with BT.

2.2.4 Access Speed

The throughput achieved by the firewall will be dependent on a number of factors such as the specific applications deployed, the security policy implemented, Network Address Translation and network and Buyer server delays, as well as the effect which VPNs and UTM (Unified threat management) features may have on throughput.

2.2.5 Protocols

The MFS filters only IP protocols. Non-IP protocols can be passed through the firewall provided they are encapsulated within an IP V4 protocol.

2.2.6 Routing and Mapping

Internet/Edge Design Best Practice

Redundancy is a necessity in all network architectures that require high availability or failover. However, when an enterprise network connects to a single ISP via a single Internet connection redundancy is a null issue because there is only a single ingress/egress point.

Static Routing

Static routing is the preferred routing option for all MFS deployed firewalls deployed with a single ISP or "outside" connection and this meets normal design best practice. There are no advantages to deploying dynamic routing in this instance; therefore there is no need to run routing protocols and their associated processes etc.

A maximum of 50 static routes/prefixes can be configured on MFS supplied/configured firewalls. If additional static routes are required, pre-authorisation must be obtained via the Special Bid process.

Rip

Routing Information Protocol (Rip) is not currently supported on any MFS firewall deployments.

OSPF

OSPF (Open Shortest Path First) is not currently supported on virtual firewalls.

BGP

Border Gateway Protocol (BGP) is supported on virtual firewall on Public Cloud.

When there are multiple connections to one or more ISPs or multiple resilient firewalls, the de facto standard Internet routing protocol is Border Gateway Protocol (BGP). BGP propagates routing tables through the Internet, determines routing conditions for path selection, and converges upon failures.

If BGP is required for a Buyer solution (i.e. in a high availability design), then required BGP instances must be terminated on devices external to the firewall, i.e. a router that can either on the inside or outside of the firewall. The BGP communication can be easily passed through the firewall using the standard BGP TCP port number (179), however the firewall does not actively join the BGP process.

If there is an external router terminating routing protocols from the ISP or extranet connection, or internal routing processes on the enterprise network, then the MFS would normally use static routing for forwarding transit traffic, however OSPF can be used, assuming the caveats listed in the OSPF section below are followed.

Please note - the Supplier's services have standard high availability designs that employ BGP as the core routing protocol, these standard designs are available from the MSS design team.

Unless the firewall is participating in a routing process, it is advised to always block routing protocols on all MFS

Mapping

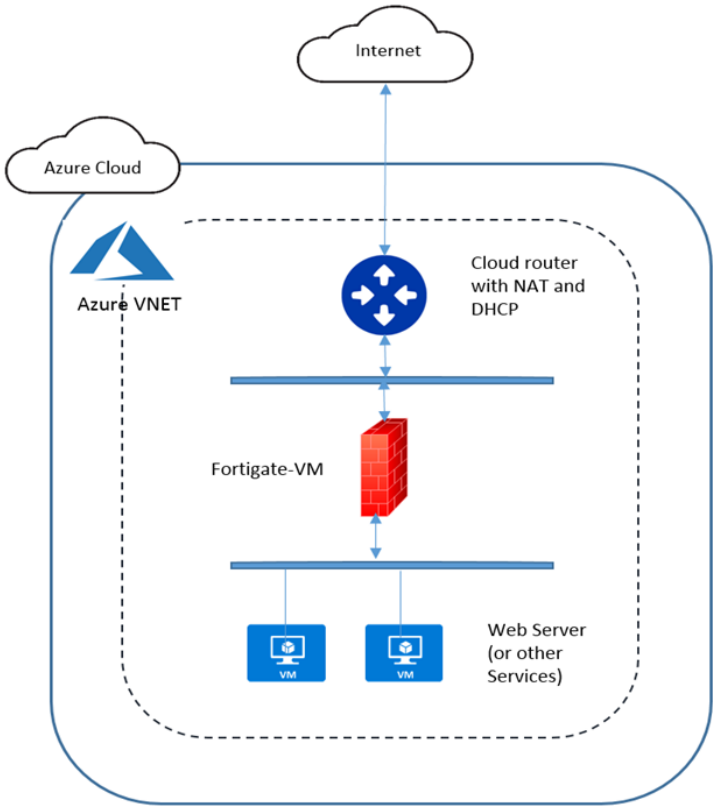
There are two types of Network Address Translation (NAT) currently supported; one to one address mapping and Hide Mode. No other NAT is supported.

One to one NAT mode allows the mapping of a single IP address to a unique public IP address. It enables certain hosts to be reachable from the untrusted side of the firewall.

Hide Mode, the firewall can be configured to hide all (or a proportion of all) internal traffic behind one single public IP address, on the Internet facing interface. All outgoing traffic on the Internet will appear to be sent by the NAT Hide address.

2.2.7 Single Firewall Solution Design

The example diagram shows a deployment of a single instance FortiGate-VM in Azure.



2.2.8 High Availability Firewall (Resilient)

High availability (HA) is a configuration in which two firewalls are placed in a group and their configuration is synchronized to prevent a single point of failure on your network. A heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down. Setting up the firewalls in a two-device cluster provides redundancy and allows you to ensure business continuity.

2.2.9 VPN Feature Set

2.2.9.1 Remote Access VPN

The Remote Access VPN feature for the Managed Firewall enables remote users to gain access to their company's private network so that employees can work remotely from home or whilst roaming.

The Managed Firewall will be configured to set up a basic VPN service with IPSEC or SSL VPN Tunnel methods. Typically the SSL VPN tunnel method will require a Digital certificate which can be BT provided or Customer provided.

Note : This should not be considered as a Remote Access end to end Service

Customer's users will be verified through the customers already chosen authentication method. i.e. Radius/LDAP. It is the customers responsibility to manage their end clients and users.

User Authentication - MFS will set up the authentication requests to point to the customer's Radius or LDAP server. The customer will be responsible for their own User Authentication resource method, implementation and in-life support. SAML may be supported but will be classed as non-standard. User databases on the gateway are NOT supported.

Remote Client Software - It is the responsibility of the customer to obtain and manage the endpoint software and support in-life their end clients/users.

Renewal of any certificate or necessary licensing will be the responsibility of the customer.

IPSec Site-to-Site VPNs

IPsec VPN provides an authentication and encryption scheme to ensure the privacy and integrity of communications over Public Networks such as the Internet.

- **BTs MFS to MFS (Site to Site VPNs),** for creating a VPN over the Internet. The VPN is set up between two MFSs, which are owned by the same customer. As the VPN is setup on two firewalls the management charging applies to both ends of the tunnel.
- **Extranet - 3rd party to MFS (Extranet VPNs),** for creating a site-to-site VPN over the Internet. The VPN is set up between an MFS, and a 3rd party or customer-owned device. Extranet VPNs set up between the following devices are standard; Fortinet and Palo Alto.

Due to the complexities of not owning both sides of the VPNs, provision should be completed after the firewall has been brought into service first.

Site to Site VPNs

High Level Description

This service option provides secure connections between customer sites over the Internet. IPSec tunnels are set up between firewalls (that have been provided to the customer as part of the MFS). This enables the customer to use the public Internet as a secure part of their WAN connectivity solution, rather than private network alternatives like MPLS or frame relay.

Encryption

The IPsec encryption protocol used is 3-DES or AES.

Authentication Scheme

The authentication between firewalls is carried out using Shared Secrets or Digital Certificates. MFS can make use of the BT Managed PKI service to issue the Certificates if these are purchased alongside the MFS product and subject to the design.

Extranet VPNs

An Extranet is a Virtual Private Network which is built between different corporate networks, thus enabling secure communications (with authentication, control and encryption) between these organisations over the Internet. For instance, a company may set up extranet VPN tunnels between its own sites and its various suppliers' networks.

Extranets will only be provided once the firewall has been brought into service. This is due to the long lead-times that connecting these VPNs can have.

The MFS definition of an Extranet is either:

- A VPN between MFSs belonging to different organisations. In this scenario, BT manages both ends of the IPSec tunnels, but the management of security policy is more complex than where both ends are owned by a single customer.
- A VPN between a MFS and a non-MFS firewall, regardless of the whether the same or different organisations; again, management of security policy is relatively complex.

The following rules are applicable for Extranet VPN connections:

- The following Firewall types are available as standard; Fortinet and Palo Alto. Any other firewall types will have to follow the special bid process.
- NAT is usually not available as part of a VPN terminating on the BT Managed Firewall.
- BT will need to know what networks (i.e. the encryption domain) are behind the distant Extranet device (e.g. 3rd party firewall), and the services that are to be supported.
- Authentication is via Pre-Shared Keys only; ie not Certificates, because MFS doesn't manage both ends of the VPN.
- Either the customer needs to supply the pre-shared secret, or shared secrets need to be agreed / negotiated with the customer.

IKE and IPSEC settings need to be aligned; e.g. use of 3DES at both ends.

Usage regulations for encryption

It is the customer's responsibility to ensure compliance with the strict encryption export/import/usage regulations for all countries where the 3rd party or customer-owned device is to be used.

2.2.10 Unified Threat Management / Next Generation Firewall Features

Buyers may select optional services to be deployed on their BT Managed Firewall, depending on the firewall model. The Supplier will configure these services in accordance with the chosen tier of service (where applicable), and within the limitations of the third-party software used to deliver the service. The Supplier cannot guarantee that this software will operate without fault or interruption or, in particular, to intercept or disarm all malware.

In general, these should be regarded as 'lite' services; requirements for full featured IPS or complex URL policy management, service reports or heavy throughput are best handled by dedicated appliances.

2.2.10.1 Firewall Enhanced Intrusion Prevention Service

Traffic passing through the Buyer's firewall will be constantly monitored for attacks, in accordance with the applicable intrusion signature files. The initial service will be implemented with a default configuration setting.

The service includes subscription to the necessary signature updates, which will be implemented upon release by the supplier; the Supplier will not be responsible for evaluating these signatures beforehand; but shall disable the appropriate signature (where possible) in the event of conflict with legitimate Buyer traffic.

An IPS policy will be captured and agreed with Buyer before implementation and each Buyer will receive an Incident Response Plan detailing exactly what should happen and when for the level of service purchased.

IPS signatures will be updated via the Buyer's internet connection.

IPS Events will be logged to the Supplier's Management platform over a secured connection and used to troubleshoot any issues and drive reporting. The reporting will be provided via the Supplier's Security portal in near real time so that Buyers can view top 'blocked' traffic as it happens.

Firewall Enhanced Intrusion Prevention Service - Silver

The Silver service provides automated blocking, with a minimal level of tuning but no proactive monitoring or alerting.

The intention is to offer Buyers the ability to select a risk level that they wish to accept which will determine the level of alerts that are logged. As a minimum the Supplier will automatically push updates as they are available and block high impact / high confidence attacks, as defined by the supplier of the software used to deliver the service.

The service will be initially tuned according to data gathered from a 'detect and watch' period along with Buyer provided information on their operating environment. In life IPS tuning will be incorporated in this package to periodically review logs and refine event alerting. Reporting will be available via the Supplier's My Account portal.

Firewall Enhanced Intrusion Prevention Service - Gold

IPS Gold Service – In addition to IPS Silver, the gold service offers an increased level of human interaction alongside the firewall vendor automation. The detect and watch period will be the same but the tuning carried out by the Supplier in conjunction with the Buyer before enabling the IPS 'blocking' per Firewall/firewall pair will be more in depth. Reports will be available on the portal and regularly reviewed with a BT Security Optimisation Manager.

Firewall Enhanced Intrusion Prevention Service - Platinum

IPS Platinum Service – In addition to IPS Gold, the Platinum service offers a more personalised service for each Buyer account through increased human interaction alongside the firewall vendor automation. A detect and watch period will be employed before tuning, which will be carried out by the Supplier in conjunction with the Buyer. After tuning the IPS 'blocking' per Firewall/firewall pair will be enabled. Reports will be available on the portal alongside a nominated Security Optimisation Manager in office hours. Proactive alerting with helpdesk diagnostics is available for critical block alerts as detailed in an Incident response plan.

IPS Proactive Monitoring

IPS Proactive Monitoring will only be available for the Platinum level Service. In this service we will automatically ticket blocked events for investigation by our 24x7 Monitoring team. An engineer will be assigned within 15 minutes of receiving the ticket and aim to highlight any potential 'false positives' to the Buyer within a target time of 1 hour. Contact will be via the nominated Buyer Service desk. If the ticket is deemed to be a legitimate block event, then no further action is required as the IPS is fulfilling its function correctly and protecting the Buyer traffic. If we suspect that the block is stopping legitimate business I.e. an internal server performing a regular routine, then this will require a tuning request to update the policy and allow this action. Finally, sometime, it's possible that the block will highlight a vulnerability within the Buyers' environment that needs to be addressed. They may decide to monitor this going forward whilst they remedy the situation internally.

2.2.10.2 Firewall URL Filtering Service

This Service allows the Buyer to block access to Internet sites which it deems to be undesirable. Internet sites are arranged into groups which are regularly updated by the vendors; the Buyer may choose to block or restrict access to any or all groups.

Upon trying to access a blocked/ restricted site, the end user will receive an appropriate (Buyer definable) message to advise either:

1) that their request has been completely blocked, or
2) that they need to first confirm acceptance of their organisations acceptable use policy (or similar warning). Upon acceptance, the page will be delivered.

In the event of any change in the Buyer's policy, the Supplier will implement the necessary alterations via the standard configuration management process.

2.2.10.3 Firewall Anti-Virus Service

This Service provides Buyers with anti-virus checking for web browser (http), and secure web browser (https) traffic. When the Buyer's users request an executable file from a site on the Internet, the file is inspected against the current antivirus definition file. If no virus is detected, the file is passed to the requestor. If a virus is detected, the file will be blocked and deleted.

Antivirus definition files are kept up to date by regular downloads direct from the antivirus servers. The Service is subject to maximum file size and compressed archive limits. Within these limits, the Buyer can specify a maximum file size to be scanned.

2.2.10.4 Firewall Identity Awareness

This Service allows Buyers to control explicitly which groups and therefore associated people within an organisation can access on-line resources. A connection is made by the management platform and gateway to the Buyer's active directory server, allowing identity information (users and groups) to be reflected in firewall policy, instead of relying on IP addresses.

Buyers using the Fortinet solution will be responsible for installing collector agents where required, due to the privileges required on the Buyers Active Directory servers.

2.2.10.5 Firewall Application Control

This Service provides granular controls based on the applications people are using, rather than just the websites they are visiting. It should be noted that there are thousands of potential applications, so it is intended that the service is configured using application categories rather than unique applications. Access for individual application can be configured as exceptions using the vendor's specific application list identifiers.

2.2.10.6 Firewall Anti-Bot

This service reduces the post-infection impact of BOT compromise, i.e. when a server/ endpoint within an organisation has been infected. It blocks the communication between the host and internet-based command and control servers. This prevents payloads from being downloaded, malicious commands from being executed, and corporate data from being exfiltrated.

The Fortinet solution configures Antivirus and Anti bot simultaneously and cannot separate the feature.

2.2.10.7 Firewall Threat Emulation

Threat Emulation is available for Fortinet Solutions. It is primarily focused on identifying zero-day attacks. It achieves this using advanced heuristics to understand typical "good traits" coupled with a hard-wired understanding of known "bad traits" in order to identify threat characteristics that don't currently have a written signature.

The table below describes how Fortinet Technology behaves in important areas.

	Fortinet	Palo Alto	Check Point
File Type	Archived: .tar, .gz, .tar.g, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj Executable: .exe, .dll, PDF, Windows Office, Javascript Media: .avi, .mpeg, mp3, mp4	Microsoft Office .doc/docx, .xls/xlsx, and .ppt/pptx; Portable Document Format (PDF); PE Java Applet (jar and class); Android Application Package (APK). Flash email-link Multi-Level-Encoding PE, ai, any, apk, arj, avi, avi-divx, avi-xvid, bat, bmp, bmp-upload, cab Catpart, cdr, chm, cin Class, cmd, cpl, dll, doc Docx, dpx, dsn, dwf, dwg, dxf, edif, emf, encrypted-doc, encrypted-docx encrypted-office2007, encrypted-pdf, encrypted-ppt encrypted-pptx, encrypted-rar encrypted-xls, encrypted-xlsx encrypted-zip, eps exe, exr, flash, flv, gds gif, gif-upload, gzip, hlp hta, ichitaro, iff, iso iwork-keynote, iwork-numbers, iwork-pages, jar jpeg, jpeg-upload lnk, lzh, ma, macapp, mb, mdb, mdi, mif, mkv, mov, mp3, mp4 mpeg, mpkg, msi, msoffice, ocx, pbm, pcl pdf, pgp, pif, pl, png, png-upload, ppt, pptx psd, rar, reg, rla, rm, rpf, rtf, scr, sgi, sh, shk softimg, stp, svg, tar, tdb, tif, tiff, torrent, vbe, wmf, wmv, wri, wsf, xls, xlsx, xpm, zcompressed, zip	pdf, doc, docx, xls, xlsx, ppt, pptx, rtf, dot, docm, dotx, dotm, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, csv exe, tar, zip, rar, Seven-Z, scr, swf, hwp, jar, cab, tgz, pif Check Point can also run Threat Extraction which converts office and PDF docs with active links to pdf format files.
Location of Processing	Canada and Germany. Once registered with the 'European' IP, the files will automatically be send to Frankfurt for further analysis	US (California) and European datacentre in the Netherlands.	Sandboxing is in Israel, Germany and USA

Encryption on route to cloud	Yes	Yes	N/A
SLA for signature	no SLA	within 15 mins	no SLA
Signature update	Automatic via AV update	Automatic via AV update	Signature updates from the Cisco AMP cloud
Will the service Block the new threat as detected?	No. There is a patient zero situation until the new signature is updated.	Yes, after first sight Files can be blocked, forwarded or continued.	Yes files can be detected or blocked.
After initial scan, will subsequent files still be sent for emulation?	No. FortiSandbox cloud will recognise that the file has been uploaded before and respond back instantly with a result negating the need for an upload	Yes. Gateway keeps sending suspect files until update is deployed	N/A
Unlimited no. of scans?	Yes	Yes	Yes
Deployment	In conjunction with gateway and UTM subscriptions	In conjunction with gateway and advanced threat prevention subscription and advanced wildfire subscription.	In conjunction with gateway and UTM subscriptions
Anonymised data	No	Yes	N/A
Configuration	Suspicious or ALL	Granular control over what session information is sent to the cloud, enabling users to maintain compliance with local laws and regulations	Select which file formats (from list above) and protocols.
Protocols & Apps supported	FortiGate Integrated: HTTP, SMTP, POP3, IMAP, MAPI, FTP, SMB, IM and SSL and encrypted equivalent	Supports Applications as opposed to protocols	http, smtp, imap, pop3, ftp, smb
Operating systems supported	Windows® XP, Windows 7 (32 and 64-bit) Windows 10 is on roadmap. No dates yet.	Windows® XP, Windows 7, Android ® and Mac® OS X®	N/A
Portal	Forticloud Portal BT will setup portal to email customer reports	Wildfire Portal BT BT will setup portal to email customer reports	N/A local only
Reports	Reports generated via customer FortiAnalyzer. 1. Number of Files Analysed by FortiCloud Sandbox 2. Malicious Files Detected by FortiCloud Sandbox	For customers using the Panorama management platform, reports are available via Panorama ACC: 1. wildfire activity by file type (malicious and benign) 2. wildfire activity by applications (malicious and benign) For customers using Strata Cloud Manager, various reports are available on Strata Cloud Manager itself.	

Logging	If threat emulation is selected the customer must be aware that all anti virus event logs will be forwarded to Fortinet. Av logs also contains sandbox logs that get forwarded to Forti sandbox cloud service.	Critical event logs will be forwarded to Panorama or Strata Cloud Manager depending on what management system has been opted for.	
Email notification/alerts	Yes	Yes	Yes

2.2.10.8 Advanced Threat Prevention (Palo Alto)

Advanced threat Prevention adds an additional layer of insight and security for NG Firewall users. Advanced threat Prevention scans IP addresses, blocking or granting access to web and application-based content after a complete analysis of the IP address reputation.

2.2.10.9 Advanced URL Filtering (Palo Alto)

This Service allows the customer to block access to Internet sites which it deems to be undesirable. Internet sites are arranged into groups which are regularly updated by the vendors; the Customer may choose to block or restrict access to any or all groups.

Upon trying to access a blocked / restricted site, the end user will receive an appropriate (customer definable) message to advise either:

the request has been completely blocked, or

to confirm adherence to an acceptable use policy (or similar warning). Upon acceptance, the page will be delivered.

Reporting capability for URL filtering is dependent upon the firewall technology deployed – please discuss with account team and relevant BT subject matter experts.

In the event of any change in the customer's policy, BT will implement the necessary alterations via the standard configuration management process.

2.2.10.10 Advance Wildfire (Palo Alto)

Wildfire is a cloud-based service that provides malware sandboxing and fully integrates with the vendor's on-premises or cloud-deployed next-generation firewall (NGFW) line. The firewall detects anomalies and then sends data to the cloud service for analysis.

2.2.10.11 Prisma Access Agent (Palo Alto)

Prisma Access Agent (replaced GlobalProtect) from Palo Alto Networks®, is a next-generation network access client for endpoints: it extends security to mobile and remote users.

2.2.10.12 NGTX (Check Point)

NGTX from Check Point is a cloud-based service that provides the following UTM features within the same, bundled licence: IPS, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam and Application Control.

2.2.10.13 NGTP (Check Point)

NGTP from Checkpoint offers Threat Emulation in addition to those UTM features offered with NGTX.

2.3 Managed Service Tiers

Buyers will choose a service level from the Managed Services (MS) 3 tiers of differentiated service, these are Managed Service MS1, MS2 and MS3; which increase in levels of the Supplier proactivity and tailoring for our Buyers.

2.3.1 Initial Set-up

The Supplier will provide means by which Buyer orders for one or more managed services may be captured and progressed through to delivery. The Buyer will be kept informed throughout the delivery process which will be managed to ensure that Buyer committed delivery dates are accurately forecast and achieved.

Prior to raising an order, the Supplier will liaise with the Buyer to produce a quotation for the service requested. The Supplier will only proceed with the service order once this quote has been produced and agreed with the customer. It will be the responsibility of the Supplier's Pricing Desk to produce the quotation using the relevant Pre-Sales Questionnaire (PSQ), which will be produced by the Sales team to capture the customer's service requirements

2.3.1.1 Managed Service (MS)1

SUPPLIER OBLIGATIONs

Order Capture, the Supplier will:

- Provide the Buyer with access to the BT Web Portal
- Provide standard good practice templates that describe the service in terms of architecture and initial policy; the Buyer will be invited to select the appropriate template during the pre-order stage. The Supplier will deliver the service against the templates. The Buyer may not alter the service from that described by these templates until commissioned and handed over to in-life management, at which point they may raise policy change requests which BT will implement in accordance with the change control process and with due regard for the level of service being delivered.
- The Supplier may provide the Buyer with Professional Services at an additional Charge, at their request, to assist them in the creation of their CSP(s). The responsibility for the CSP(s) will remain with the Buyer.

Service Delivery, the Supplier will:

- Ensure all necessary information is captured for the service implementation and its transition into management by the Supplier Security operations teams. This may be captured at different points in the order journey; delays receiving this information may in turn delay service delivery.
- Validate the completion of the submitted order, identify missing or conflicting information, and summarise the details of the order back to the Buyer. The Supplier will request the Buyer confirm that they have ordered the correct number of licences to serve their requirements.
- Based on standard delivery plans and supplier lead times, provide a date on which delivery of the service (or each part of the service, including to each site) is due to start ("Customer Committed Date (CCD)") and will use commercially reasonable endeavours to meet any CCD.
- Set up the Buyer and billing accounts.
- Co-ordinate the delivery of the Associated Services and its commissioning.
- Liaise with the Buyer and third-party suppliers of Buyer equipment suppliers as required, and handover the overall service into in-life management.
- The Supplier will commission the Associated Services remotely in accordance with the policy selected by Buyer.
- Once commissioned the Buyer is responsible for defining their ongoing policy beyond that specified by the default template, raising change requests on the Supplier, via the BT Security Change Manager Portal, as necessary to evolve the policy in line with their business need.
- Update the Buyer by email at each stage of this service delivery process: Order acknowledgement: CCD, Service delivery; and start of billing.
- Chargeable option to upgrade to a Managed Security Project Management Plus or Premium service.
- Provide a Security Policy Document, to capture the Buyer's Security Policy applicable to the service order. If applicable, the Suppli will contact the customer to arrange a call to complete the CSP with them.
- Start billing at the end of Initial Setup; Initial set-up is charged in arrears, whilst Controlled deployment, Monitoring and management, and Continuous improvement charged in advance.

Post Implementation checks, the Supplier will:

- Conduct a series of standard tests on the Service, at dates agreed with the Buyer to ensure that it is configured correctly; and on the date that we have completed these activities confirm and notify the Buyer through email the Service Start Date.

- Provide a technical description of the service being provided, together with information on the Supplier points of contact, the services provided, the Buyer account IDs and their regional first line the Supplier's Helpdesk details. It will also explain how to use the service, view reports, raise change requests and faults, etc. This will be available from the BT Web Portal.

BUYER OBLIGATIONS

Before the Service Start Date and, where applicable, throughout the provision of the BT Security Managed Service, the Buyer will:

- Select appropriate policies to use as their CSP(s) when they place the Order and ensure that the standard policies, they select meet their requirements.
- Raise change requests on the Supplier, via the BT Web Portal, as needed to modify this policy in accordance with the change control process, and in line with the defined scope of the service.
- Purchasing enough licences to meet the requirements of the service and comply with any end user licence agreements. It is the Buyer's responsibility to notify the Supplier if licence requirements change.
- Complying with instructions that the Supplier provides to the Buyer in order to operate the service.
- Maintain MPLS / Internet access circuit bandwidth if applicable for associated service, including provision for in-band management access from the BT SOC, and ensure that Associated Services are able to receive updates, such as Vulnerability signatures, directly over the Internet, or over an alternative path agreed with the Supplier for that purpose;
- To modify on-site router and networking appliances to ensure appropriate traffic is directed to the Supplier provided services.
- Ensure compliance with local regulations, including any export/import/usage regulations for all countries.
- Provide the Supplier, and keep the Supplier updated, with the names and contact details of the various Buyer Contacts authorised to act on their behalf for BT Security Managed Service management matters including in respect of:
- Management of Incidents.
- Issues identified by BT as a result of monitoring the Associated Services.
- Signature updates.
- Accessing logs.
- Site access by BT or a third party acting on behalf of the Supplier.
- Managing resets and privileges to the BT Web Portal.
- Vulnerability notification and patching.
- Modification of the CSP(s).

- Retain responsibility for the CSP(s).

SERVICE LEVEL TARGETS AND CREDITS

The Supplier will use commercially reasonable endeavours to achieve the date provided to the Buyer. However, no SLA payments are payable for late delivery of the service.

Lead Times. The standard lead-time is set out below, lead times for a working solution assume any associated network is already in place.

Service delivery (Virtual / Cloud services only)	Delivery of the components in accordance with the order and pre-defined architectural and policy templates.	10 days (or shorter where possible)	From the validation and acceptance of the order-on-order entry systems.
Specific Country Issues	For some countries there may be delays due to clearance through Customs, or where export and import licensing are required.	Up to 45 days on top of standard lead time	Typically apply to non-EU / USA locations.
Buyer checks	Verification that the service is operating in line with contract and design templates.	48 hours	

Note: all days quoted are business days.

2.3.1.2 Managed Service (MS)2

SUPPLIER OBLIGATIONS:

As above, and in addition the Supplier will:

- Appoint a named BT Project Manager to be the Buyer's single point of contact during the Initial Setup. The BT Project Manager will undertake any activity remotely and will not visit the Buyer's Site.
- Provide industry/scenario policies to use as the Buyer's CSPs.
- The Buyer may request the services of a named BT Project Manager who will be available to attend meetings at the Buyer's Site, for an additional charge, depending on their location for the Initial Setup phase.
- Comply with all reasonable health and safety rules, regulations, and security requirements that apply at a site and are notified to us.
- Apply SLA credits for late delivery of the service.

2.3.1.3 Managed Service (MS)3

SUPPLIER OBLIGATIONS:

As above, and in addition the Supplier will:

- Provide a named BT Project Manager who will be available to attend meetings at the Buyer's Site depending on their location, for the duration of the Initial Set-up.

2.3.2 Controlled Deployment

Following the initial set up of services, the Supplier will work with the Buyer during a defined period (typically between 2 and 30 days, dependent on Service Level and the services taken), for Buyer testing and optimisation to ensure rules and policies are tuned to achieve desired outcomes, before bringing the service under the Supplier's Management.

The table below outlines the number of Simple Service Requests (SSR) that are allowed during the initial Controlled Deployment period.

Further details of what constitutes a SSR (as well as a Complex Service Requests, or CSR) can be found in Section 2.3.4.3 of this document.

MS Level	MS1	MS2	MS3
Number of Changes Allowed	6 SSR	8 SSR	10 SSR

If the Buyer wants more than the allocation of 6/8/10 changes during this timeframe, the Buyer will be asked to specify the changes they wish to implement during the Controlled Deployment phase up to the allocated amount and all remaining changes above this number will be submitted to the Supplier once this phase has completed and the service is operational. This will then be subject to an allocation of 6/8/10 change per month, according to the manged service level purchased.

2.3.2.1 Managed Service (MS)1

SUPPLIER OBLIGATIONS

The Supplier will:

- Start Controlled Deployment as soon as the initial set-up phase has been completed bringing the service under BT Operational control.
- The Project Manager will inform the Buyer via email of the start and end of the Controlled Deployment period.
- Provide user guides for access to the BT Web portal including how to make policy changes, how to request technical resource, access to reports and the operational Buyer handbook.
- Provide a 48-hour period for the Buyer to test the security policy rules provided at the initial set up phase.
- Review any Buyer issue reported within the 48-hour period and time to resolve agreed. Any issues with the Service will be directed via the Service Desk and triaged to make sure they are contractually within the scope of the service the Buyer has purchased. Any issues requiring CSP Changes will be directed to the Technical Implementation Manager.
- If the change request is outside the scope of work contractually agreed, the new change request will be treated as a new work request and be subject to appropriate timescales. During Controlled Deployment, only Standard/Simple Changes are within scope. All Complex Changes are outside the scope.

- Complete checks to ensure everything is in place to process Monitoring and Management.
- Allocate a BT Security Optimisation Manager who will review Buyer service requirements twice a year.
- The Technical Implementation Manager will notify the Buyer of the date of completion of the Controlled Deployment CSP Optimisation.

BUYER OBLIGATIONS

The Buyer is responsible for the following:

- Carrying out the Controlled Deployment CSP Optimisation within the Controlled Deployment 48-hour test Period.
- Reading the BT Web Portal user guides to understand the correct process to report, faults, access reports and raise change controls.
- Raise any changes they require to the CSP as a result of the Controlled Deployment CSP Optimisation through the CSP Change Management Process.
- The Buyer will notify the Supplier when they have completed the Controlled Deployment CSP Optimisation. If they do not provide the Supplier with such Notice by the end of the Controlled Deployment CSP Optimisation Period, the Controlled Deployment CSP Optimisation will be deemed to have been completed by them.

2.3.2.2 Managed Service (MS)2

SUPPLIER OBLIGATIONS

As above, and in addition, the Supplier will:

- Provide a specific timeframe for the Buyer to work in conjunction with the Supplier to fine tune their policy (for example changes to data sources, rules, and configurations).
- If the change request is outside the scope of work contractually agreed, the new change request will be treated as a new work request, submitted to the Supplier via the change management process (where the Supplier is responsible for managing the changes) and be subject to appropriate timescales.
- Allow a testing and fine-tuning period up to 30 calendar days for the MS2 level service, not including a BT managed Security Information & Event Management (SIEM) solution.
- Allocate a BT Security Optimisation Manager who will review the Buyer's service quarterly.

BUYER OBLIGATIONS

As above, and in addition, the Buyer is responsible for the following:

- Providing a named contact to work with the Supplier over the specified timeframe to test and fine tune the service.
- All communication will be via the Service Desk.
- Raising a change control for any requirement that is either outside the contractual scope of the MS 2 level service or is a chargeable additional service or feature.

2.3.2.3 Managed Service (MS)3

SUPPLIER OBLIGATIONS

As above, and in addition, the Supplier will:

- Allocate a BT Security Allocate a BT Security Optimisation Manager, who will review the Buyer's service on a time period agreed with the Buyer but not more frequently than once a month.

BUYER OBLIGATIONS

As above, and in addition, the Buyer is responsible for the following:

- Providing a project manager and technical team to work with the Supplier over the specified timeframe to test and fine tune the service.
- Making sure all communications are directed to the assigned the Supplier personnel during this timeframe.
- Raising a change control for any requirement that is new and not within the existing contractual scope.

2.3.3 Monitoring and Management Overview

The Monitoring and Management service features can be characterised as real time (24x7) through to weekly regular service activities that are in place once In Life Service commences.

2.3.3.1 Manage Service Incidents

The Supplier will act as the single point of contact through to resolution of incidents related to the security services that BT are supplying to the Buyer. A service incident is defined as an unplanned interruption to, or the reduction in the quality of the security service. Failure of a resilient component that has not yet affected service is also an incident.

Service Management Boundary

- The Supplier will manage incidents that explicitly relate to the service being provided by the Supplier.
- The Supplier will have no responsibility for managing incidents outside of this service boundary, including Buyer servers and end client devices other than when contracted to the service provided

- Where the Supplier deploys shared infrastructure as part of the service, the Supplier will manage incidents affecting that infrastructure

2.3.3.1.1 Managed Service (MS)1

SUPPLIER OBLIGATIONS

The Supplier will:

- Ensure the Buyer has a copy of their MFS Service Handbook with appropriate information on the following:
    - Service Monitoring and Management Features
    - Managing Service BT Contacts
    - BT Contacts and Systems
    - Managing Service Incidents
    - Vulnerability Management & Patching of Managed Devices
    - Signature Updates
    - Log Capture
    - Continuous Improvement
    - Licensing and Vendor Support Agreement
    - My Account Portal Tool and Security Hub Information
    - Change Management
    - Service Level Agreements
    - Security Threat Intelligence and Reporting
- Proactively identify and action any incidents using the Supplier's monitoring tools.
- Accept communication from designated Buyer contacts via the Security Hub portal. In the event that the Buyer is unable to raise a fault on the BT Web Portal, then a phone option will be available.
- Accept Security Service incident reports from the Buyer's designated IT Service desks via the BT Web Portal.
- All communications with the Service Desk via the Security Hub Portal will be in English, unless specifically agreed otherwise.
- The Service Desk that will action the Incident notifications is available 24x7x365 and is staffed by security trained professionals.
- Raise tickets to track all reported incidents and use structured questions and remote diagnostic/ monitoring tools to validate the Incident and determine appropriate remedial action.

- Aim to resolve common incidents within the helpdesk environment, advising Buyers of remedies within their own control, or using administrative tools to effect a resolution remotely.
- Escalate internally to such specialist groups as may be necessary if it is not possible to address the Incident within the helpdesk. At the Supplier's discretion, the Supplier may engage and coordinate third party support.
- the Incident will be assessed in accordance with the criteria set out in the table below:

Priority	Description
P1	Serious impact and Incident cannot be circumvented, typically where the Associated Service is completely down / unavailable; for example: a Site is isolated or there is a complete loss of service to a Site or critical business functions are prevented from operating.
P2	Large impact on a portion of the Associated Service and cannot be circumvented, causes significant loss of the Associated Service, but the impacted business function is not halted; for example: there is a complete loss of primary link, and the BT backup link (if provided) is invoked, or business functions are disrupted but not prevented from operating.
P3	Small impact on the Associated Service or where a single User or component is affected, and it causes some impact to the Buyer's business; for example: there is an intermittent or occasional disturbance which does not have a major impact on the Associated Service or where a temporary work around has been provided.
P4	Incident minor or intermittent impact to a non-operational element of the Associated Service; for example: a temporary failure of reporting or billing.
P5	Incident has no direct impact on the Associated Service. Records normally kept for Incidents are used for information purposes. Example: to track upgrades, to obtain a Reason for Outage report (RFO), for planned outages or for enquiries as well as Buyer provoked Incidents.

- Maintain up to date support contracts covering the appliances and services provided.
- Review the status of the incident and: a) amend the initially assigned priority as necessary, if for example the impact is found to be broader that first believed; b) escalate via vendor Firewall support ticket and allocated Vendor technical contacts.
- Maintain backup configurations to allow service to be fully restored following hardware swap out, or failover of service to an alternative means of delivery.
- Keep the Buyer informed at regular intervals throughout the course of an Incident. This will be by means of updates posted on the BT Web Portal.

BUYER OBLIGATIONS

The Buyer is responsible for the following:

- Notify all Incidents to the Service Desk directly or via the BT Web Portal.

- Ensure that the Supplier has up to date contact points and provide the name and contact details for a nominated representative responsible for liaising with the Supplier regarding the service.
- Advise the Supplier if the nominated representative changes and ensure that BT has the current details of the nominated representative.
- Provide the Supplier with access to the Buyer's site(s) during business hours or as otherwise agreed, to enable the Supplier to resolve the incident.
- Be responsible for the physical environment, and provision of power to any Buyer appliances, in accordance with the specifications advised by the Supplier
- Unless explicitly within the scope of a Buyer service agreement with the Supplier, be responsible for local and wide area network connectivity and necessary switch/router configuration to deliver required traffic to and from the services and appliances being managed by the Supplier; this includes any management connectivity (at the Buyer site) to the appliances in question.
- Ensure that end users report incidents to the Buyer contact point and not directly to the Supplier.
- Agree that if an incident is caused directly by the Buyer, then the Supplier reserves the right to pass on any charges for time and materials spent responding to the incident.

Service Targets for Incident Management

Priority	Target Progress Update			Target Restoration Time
	MS1	**MS2 and MS3**		
P1-P5	Whenever a progress update is available	Confirmation of Incident within 15 minutes following this and first update 30 minutes of the Incident being reported and then at intervals as follows:	follow up if the Buyer does not respond to BT questions at intervals as follows:	
P1		every 20 minutes	every 2 hours	5 Hours
P2		every 40 minutes	every 4 hours	12 Hours
P3		every 2 hours	every 12 hours	24 Hours
P4		every 4 hours	every 24 hours	72 Hours
P5		every 6 hours	N/A	N/A

- The Supplier will aim to provide the Buyer with an update on the progress of an Incident in accordance with the table above.
- The Supplier will not provide a progress update while the Supplier is waiting on input or feedback from the Buyer.

- The Supplier will aim to restore the Associated Service affected by the Incident within the period set out in the table above.
- The progress update times, and restoration times are targets only and the Supplier will have no liability for failure to meet them.

2.3.3.1.2. Managed Service (MS)2

As above, but with the addition of the following:

- If the Buyer notifies the Incident to the Service Desk directly, they will have the option of communicating in the languages agreed with the Supplier. If the Service Desk is required to escalate the Incident within the Supplier or to a third-party vendor, then the Buyer may be required to communicate in English only.

2.3.3.1.3. Managed Service (MS)3

As above, but with the addition of the following:

- The Buyer will agree with the Supplier whether the Buyer report Incidents to the Service Desk directly or via the BT Web Portal or to the regional Security Operations Centre.

2.3.3.2 Monitoring

The Supplier will monitor the performance of the Associated Services against parameters that BT deems appropriate depending on the nature of the relevant Associated Service.

2.3.3.2.1. Managed Service (MS)1

SUPPLIER OBLIGATIONS

The Supplier will:

- Monitor the performance of the Associated Services at 6-month intervals and, where possible, provide warning to the Buyer through the BT Web Portal of impending issues that may affect an Associated Service and that the Supplier identifies as a result of the monitoring. The Supplier may not identify all impending issues.
- Check that the Associated Services are operating correctly by:
    - **Appliance reachability**: Polling the Security Appliance to check it is powered on and has network connectivity. If the Security Appliance is not powered on or does not have network connectivity, the SOC will investigate and either take appropriate action or recommend action that the Buyer is required to take
    - **Security Appliance Status:** The Supplier will test at regular intervals at the Supplier's discretion as follows:
        - Resource status: conduct one test per Resource per Security Appliance such as CPU and RAM.

        - Physical status: conduct one test per physical attribute per Security Firewall such as temperature, where applicable to the Security Appliance.
        - Compare test results against standard vendor thresholds and notify any variances to the SOC. The SOC will investigate and either take appropriate action or recommend action that you require to take.
    - **Application update status**: on UTM / Intrusion Detection Service (IDS) / URL Filtering and other applications selected as part of the Associated Services.

BUYER OBLIGATIONS

The Buyer will:

- Provide networking diagrams and details at the point of sale to allow the Supplier to identify the most appropriate route/mechanism for implementing proactive monitoring.
- The Buyer will ensure that the Buyer or third parties, as required, configure routing/permissions on platforms or Associated Services to allow the Supplier to carry out the monitoring.
- The Buyer is responsible for resolving the issues that the Supplier provides the Buyer warning of.

2.3.3.2.2. Managed Service (MS)2

In addition to MS1:

- Both the Supplier and the Buyer will agree a process for the Supplier to contact the Buyer when it identifies an issue that impacts the Associated Services.
- The Supplier will utilise historic and current metrics captured via the monitoring of the Associated Services to forecast issues that may impact the performance of the Associated Services and make recommendations to the Buyer either through reporting on the Security Hub Portal or by e-mail, as agreed by the Buyer.
- In addition to the MS! checks carried out by the Supplier checking that the Associated Services are operating correctly, BT will check that the Associated Services are operating correctly by:
    - **Monitoring Applications** under the relevant Associated Services against parameters set by the Supplier.
    - **Associated Service** usage and capacity management reporting.

2.3.3.2.3. Managed Service (MS)3

In addition to MS2:

The Supplier will provide comprehensive monitoring of the end-to-end service, by checking that the appliance is functioning correctly in the following ways:

- The Supplier will carry out capacity management performance estimation of the Associated Services.
- In addition to the MS1 checks carried out by the Supplier checking that the Associated Services are operating correctly, the Supplier will check that the Associated Services are operating correctly by:
    - **Password management:** the SOC will configure a complex password, meeting the Buyer's security policy. They will also review and update them manually yearly or half-yearly.
    - **Certificate expiry monitoring.** The Buyer is responsible for updating certificates.

2.3.3.3 Signature Updates

The Supplier will work with Firewall Vendors to check Buyer Firewalls have correct version of Unified Threat Management (UTM) signature updates. The BT Security Optimisation Manager (SOM) will contact the Firewall vendor and obtain the most recent and appropriate UTM software version for the Buyer's Firewall and check this against the actual software version.

2.3.3.3.1 Managed Service (MS)1, (MS)2 and (MS) 3

SUPPLIER OBLIGATIONS

The Supplier will:

- Apply Signature updates at a time convenient to the Supplier, using reasonable endeavours within 14 days of the vendor release.
- If the Supplier is aware that the Buyers' Associated Services will have downtime or that the Signature Update will cause an impact on the Associated Services, both the Supplier and the Buyer will agree an appropriate time within Business Hours for the Signature Update to be applied.
- Where possible, identify and apply an automated method for applying Signature Updates unless this may impact the Associated Services.
- Check Signature Updates are the most recent version.
- If the Supplier requires to apply a Signature Update manually, both of us will agree an appropriate time within Business Hours for the Signature Update to be applied.
- Request that if the Signature Update is applied outside Business Hours, the **Supplier may invoice the Buyer for an additional Charge.**

BUYER OBLIGATIONS

The Buyer will:

- Consent to the Supplier applying the Signature Updates automatically.
- Where implementation necessitates impact to service, agree a suitable and appropriate time when the signature file can be applied.
- Request or authorise the Supplier to reverse the Signature Update if it causes an Incident in the Associated Service.

2.3.3.4 Logging

The Supplier will implement a logging capability on Associated Services where the standard design of the Associated Services allows the capture of logs through standard process.

At the Supplier's discretion, a minimum log set will be captured and stored to enable the Supplier to offer effective management of Associated Services and the captured logs will be made available to Buyers if requested.

2.3.3.4.1 Managed Service (MS) 1

SUPPLIER OBLIGATIONS

The Supplier will:

- Store Audit and Alert logs within an appropriate secure the Supplier environment outside of the Buyer's environment on a rolling 13-month basis, where appropriate.
- Store Operational logs within an appropriate secure the Supplier environment outside of the Buyer's environment on a rolling 1-month basis, where appropriate.
- Make available the previous 60 days' Audit and Alert logs to the Buyer on their request. If they require access to the logs outside of the previous 60 days, the Supplier will make them available to them at an additional Charge.
- Make available the previous 1-month's Operational logs to the Buyer on their request.
- Use reasonable endeavours to transmit and store the logs securely.
- Store the logs in their raw state or compress them if appropriate.

BUYER OBLIGATIONS

The Buyer will:

- Confirm their specific logging requirements at the time of placing the Order. The Supplier may raise a Charge for any of the Buyer's specific requirements that the Supplier deems are non-standard.

- If requested by the Buyer and subject to an additional Charge, logs may be sent to and stored in a repository on their Site or third-party premises based on a design that is agreed with the Supplier:
    - Confirm their specific logging requirements at the time of placing the Order. The Supplier may raise a Charge for any of their specific requirements that the Supplier deems are non-standard.
    - The Supplier will not be responsible for the logs while they are sent to or stored in such a repository.
    - Take any action necessary in a timely manner to enable the logs to be routed to the repository as agreed with the Supplier.
    - Ensure that they or the nominated third party use reasonable endeavours to secure the repository appropriately.

2.3.3.4.2 Managed Service (MS)2

In addition to MS1:

- The Supplier will make available the previous 120 days' Audit and Alert logs to the Buyer on their request. If they require access to the logs outside of the previous 120 days, the Supplier will make them available to the Buyer at an additional Charge.
- The Supplier will make logs available to:
- The Buyer, or third-party technologies (e.g. SIEM), where appropriate as agreed with the Buyer.
- Other Supplier services (BT SEIM, Cyber Services, etc.) that the Supplier is providing to the Buyer that do not form part of the Contract where appropriate as agreed with them.

2.3.3.4.3 Managed Service (MS)3

In addition to MS2s:

- The Supplier will make available Audit and Alert logs to the Buyer on their request for a rolling 13-month period.

2.3.3.5 Licensing Management

The Supplier will ensure all software licences and any required vendor support contracts are placed and renewed for the term of the Buyer's contract with the Supplier.

2.3.3.5.1 Managed Service (MS)1

SUPPLIER OBLIGATIONS

The Supplier will:

- Provide and deploy licences for the services identified as being within the service boundary

- Manage licence and maintenance renewal contracts for the duration of the contract period.
- Where Security Appliances are virtual Security Appliances, such as a virtual firewall, that are located on the Buyer's or a third-party platform, the Supplier will not provide licences or vendor support agreements for the host platform.
- The Supplier is responsible for ensuring software licences and any required vendor support agreements are renewed for the term of the Contract.
- Prior to end of a contract term, unless the Buyer notifies BT of a cease, service contracts will be renewed by one year (at a time). If the Buyer subsequently cancels within the one-year period, they will be liable for all costs incurred.
- Renew licences and maintenance contracts without disruption to service for the contractual term.
- Validate that Buyers have ordered the correct number of licences to serve their requirements, in accordance with any related vendor commercial terms and information provided by Buyer.

BUYER OBLIGATIONS

The Buyer will:

- Identify and maintain the name and contact details for a nominated site representative where a fault results in the need for the Supplier (or 3rd parties acting on behalf of the Supplier) to access a site for completion of a maintenance site visit.
- If the Supplier determines that the Buyer has not ordered sufficient licences, the Supplier will notify the Buyer who will seek to rectify the situation within 30 days of the date of notification.
- Confirm to the Supplier any change in the number of users or devices requiring licensing as part of the contract.
- Be responsible for ensuring compliance with applicable law, including obtaining (if required) local import and user licences and the written authority from all respective authorities, particularly for countries where the use and import of encryption software and devices may be restricted.

2.3.3.5.2 Managed Service (MS1 and (MS)3

In addition to MS1:

- Where the Buyer selects the Supplier Takeover delivery model as part of an Associated Service, they will:
    - Provide access to the Supplier to any licence user centre, existing vendor support agreements, authorisation code(s) or other information required by specific vendors and provided at the time of provision for registering products.

- Provide the Supplier read and write access to Buyer owned vendor portals for licence and support accounts where there is an operational requirement including raising a vendor support request.
- Pay the Supplier any vendor charges to reinstate any lapsed software licence agreements or vendor support agreements.

2.3.3.6 Reporting

The Supplier will offer a secure Web Portal which provides inventory and Buyer reporting for the services the Buyer has purchased from the Supplier's Security, and which can drill down into the associated service dashboards. This will include:

- A dashboard tailored to the security services that the Buyer has bought.
- Inventory information so that the Buyer can easily view their Supplier's Security capability/ estate.
- Provide access to a Dashboard for the Security Component for the Buyer to drill down and see more detailed dashboards relating to that service.

2.3.3.6.1 Managed Service (MS)1, (MS)2 and (MS)3

SUPPLIER OBLIGATIONS

The Supplier will:

- Provide the Buyer with an inventory of the Associated Services and reporting for the BT Security Managed Service and the Associated Services via the BT Web Portal including:
  - A dashboard tailored to the Associated Services purchased, such as IPS signature effectiveness e.g. hits per rule.
  - Inventory information the Supplier deems appropriate such as details of hardware, firmware, and operating systems.
- Provide the Buyer's nominated personnel with access to the BT Web Portal, where they can view their service performance data. The BT Web Portal has a number of standard reports built into it, including:
- Usage and capacity management of the Associated Services.
- End of life and end of service of Security Appliances, firmware, and operating systems.
- Vulnerabilities and implementation of Patches of Security Appliances.
- Top attack categories
- Top attack vectors
- Threat feed

BUYER OBLIGATIONS

The Buyer will:

- Identify and provide the name and contact details for a nominated representative responsible for liaising with the Supplier and managing resets and privileges to the BT Web Portal.
- Advise the Supplier if the nominated representative changes and ensure that the Supplier has the current details of the nominated representative.

2.3.4 Continuous Improvement

Regular reviews will be held with the Buyer to agree the ongoing satisfactory performance of the service. The Continuous Improvement offering can be characterised as regular reviews to optimise services, and covers the following aspects:

- Service reviews
- Security policy reviews
- End of life reviews
- Vulnerability management review and patching of managed appliances
- Change management

These are documented in the following sections, some are combined within a section where it naturally sits alongside another element such as service review and security policy review.

2.3.4.1 Service, Security Policy and End of Life Review

The Supplier will provide a service and security policy review at an agreed interval which will depended on the service option the Buyer has subscribed to.

- **Service reviews** will focus on the performance against KPIs and SLAs, including a review of event generation threshold parameters, to reduce false positives, for example, to only process Trouble Tickets for "very high" events.
- **Security Solution** review will focus on the effectiveness of the rules applied to the business environment and review the need to further tune and amend the rules to optimise the service reflecting changes in the business environment, covering items such as volume and false positives, trends in threats detected etc.
- **End of life** review will focus the Notification of end of life events, to advise any forthcoming service replacements or upgrades that may be required.

2.3.4.1.1 Managed Service (MS) 1

SUPPLIER OBLIGATIONS

The Security Optimisation Manager will carry out a review six monthly to include:

- A review focussing on the performance of the BT Security Managed Service and Associated Services against Service Levels and Service Targets.
- An end-of-life review. The Security Optimisation Manager will provide the Buyer with a report summarising the Virtual Firewall, applications and software that are managed by the Supplier on their behalf as part of the Associated Services that will go end of life within the following six months and take them through the renewal options that are available.
    - The Security Optimisation Manager will provide the Buyer with a report on the review via the BT Web Portal.
    - If requested by the Buyer and if agreed to by the Supplier, both of us may hold a conference call to discuss the report.

BUYER OBLIGATIONS

The Buyer will:

- If the Supplier has agreed to participate in a conference call the Buyer will ensure that any report the Security Optimisation Manager provides the Buyer with will be reviewed by suitably qualified personnel who are participating in the conference call prior to the conference call taking place.
- Take appropriate action to address issues as recommended by the Security Optimisation Manager.

2.3.4.1.2 Managed Service (MS)2

SUPPLIER OBLIGATIONS

In addition to MS1:

- The Security Optimisation Manager will carry out a review quarterly as follows:
    - A review focussing on the performance of the BT Security Managed Service and Associated Services against Service Levels and Service Targets.
    - A review of their CSP(s) focussing on the effectiveness of the rules applied to the CSP(s) and the need to fine tune or amend the rules of their CSP(s).
    - An end-of-life review summarised as per MS1.

BUYER OBLIGATIONS:

As above, and in addition, the Buyer will:

- Take appropriate action to address issues in respect of fine tuning or amending the Buyer CSP(s) as recommended by the Security Optimisation Manager.

2.3.4.1.3 Managed Service (MS)3

SUPPLIER OBLIGATIONS

As above, and in addition, the Supplier will:

- The Security Optimisation Manager will carry out a review at intervals agreed by the Supplier and the Buyer, but not less than monthly as follows:
    - A review focussing on the performance of the BT Security Managed Service and Associated Services against Service Levels and Service Targets.
    - A review of their CSP(s) focussing on the effectiveness of the rules applied to the CSP(s) and the need to fine tune or amend the rules of their CSP(s).
    - An end-of-life review summarised as per MS1.
    - The Security Optimisation Manager will provide the Buyer with a report on the review via the BT Web Portal or direct to them by e-mail, if agreed by the Supplier and the Buyer.
    - If requested by the Buyer and if agreed to by the Supplier, both may hold a conference call to discuss the report, or the Supplier may attend a meeting at their Site depending on their location to discuss the report with them.

BUYER OBLIGATIONS

- If the Supplier has agreed to participate in a conference call or attend a meeting at their Site, the Buyer will ensure that any report the Security Optimisation Manager provides them with will be reviewed by their suitably qualified personnel who are participating in the conference call or attending the meeting prior to the conference call taking place.

2.3.4.2 Vulnerability Management Review & Patching of Managed Appliances

The Supplier will identify, and dependent on service level, can apply a single secure coordinated process for implementing patches to reduce risk of known vulnerabilities on Buyer appliances. The Supplier will rank all Patch updates as priority ranking in accordance with the CVSS (Common Vulnerability Scoring System) and aims to have the Patches ready for implementation as follows:

CVSS Score	Vulnerability Level	Target notification to the Buyer that the Patch is available from vendor, BT has tested the Patch and the Patch is ready for implementation
0 – 4.9	Low	Discretionary
5.0 – 6.9	Medium	MS3, Discretionary during next patch cycle (3-6 months)
7.0 – 8.9	High	MS2, 28 days maximum
9.0 – 10	Critical	MS1,14 days maximum

Vulnerability Management and Patching of Security Appliances will only be available while the Security Appliance is supported by the vendor.

All communications in respect of Vulnerability and Patching of Security Appliances will be through the BT Web Portal.

2.3.4.2.1 Managed Service (MS)1

At the MS1 level the Supplier will patch the Firewalls with a CVSS vulnerability of 9 and above. The patching process is as below.

SUPPLIER OBLIGATIONS:

The Supplier will:

- Receive a daily feed which highlights all known new vulnerabilities.
- Review this list to identify those vulnerabilities which may impact the Buyer's managed Firewalls.
- Inform the Buyer of any vulnerabilities through the BT Web Portal.
- Not assess the configuration or contextual exposure of any Security Firewalls to the Vulnerability.
- Use reasonable efforts to obtain a Patch for the Vulnerability from the Security Appliance vendor and will then test the Patch for implementation and the Supplier's ability to roll-back the software to the level prior to implementing the Patch. Once testing is complete, the Supplier will advise the Buyer that the Patch is available for implementing and provide additional information, where available, to support them in deciding whether to install the Patch or not.
- Implement Patches with a High CVSS score (7.0- 8.9) or a Medium CVSS score (5.0-6.9), on the Buyer's request, at an additional Charge.
- Implement a Patch for a Vulnerability with a Critical CVSS score (9.0-10), subject to the Buyer's agreement and also agreeing an implementation time slot with them.
- Specify an implementation window for the Supplier to implement the Patches which will be typically a weekly six-hour window outside of Business Hours for the Site where the Security Appliance is situated.
- Apply the Patch in the specified implementation window and confirm to the Buyer via the BT Web Portal when the Patch has been implemented.
- Roll the Patch back upon the Buyer's request in the event that they detect undesirable side-effects. Any activity by the Supplier required to resolve issues resulting from the implementation of a Patch is not covered by the Vulnerability Management and Patching and the Supplier will invoice the Buyer for reasonable additional Charges.

BUYER OBLIGATIONS

- The Buyer will assess the suitability for deployment of the Patches that the Supplier advises are available to address notified Vulnerabilities within their specific environment and for any post-implementation testing.
- If the Buyer does not consent to accept and implement a Patch within 14 days of notification by the Supplier of a recommended Patch, or if they request that an installed Patch is reversed out due to their specific undesirable side-effects, the Supplier will be under no further obligation to provide further Vulnerability Management and Patching in respect of that Patch and will not have any liability for potential exposure should a threat subsequently exploit that related Vulnerability

2.3.4.2.2 Managed Service (MS)2

At the MS2 level the Supplier will patch the firewalls with a CVSS vulnerability of 7 and above.

In addition to the provisions of MS 1, the following provisions apply to MS 2.

- The Supplier will implement a Patch for a Vulnerability with a Critical CVSS score and a High CVSS score and latest stable variant of the vendor's general availability code, subject to the Buyer's agreement and also agreeing an implementation time slot with them.
- The Supplier may implement Patches with a Medium CVSS score (5.0 – 6.9), on the Buyer's request, at an additional Charge.

2.3.4.2.3 Managed Service (MS)3

At the MS3 level we will patch the Firewalls with a CVSS vulnerability of 5 and above.

As above, but with the addition of the following:

- The Supplier will implement a Patch for a Vulnerability with a Critical CVSS score, a High CVSS score and a Medium CVSS score and latest stable variant of the vendor's general availability code, subject to the Buyer's agreement and also agreeing an implementation time slot with them.
- The Supplier may implement Patches quicker than the implementation time set out in the table, based on the Buyer's own perceived risk of the Vulnerability, on their request, at an additional Charge.
- As part of the testing carried out on the Patch for implementation, the Supplier will consider the Buyer's known infrastructure and specific Security Appliance features.
- The Supplier will agree its test plan for the Patches with the Buyer.
- CVSS 5.0 - 6.9 will only be implemented when the vulnerability will be impacting.

2.3.4.3 Change Management

The primary goals and objectives of Change Management is to respond to the Buyer's changing business requirements, while maximising value and reducing disruption and re-work and to respond to the business and IT requests for change that will integrate the services with the business needs.

A Change might be needed as a result of a Standard, Complex Contract Affecting and Complex Non-Contract Affecting. Additionally Changes might come from other events such as Incidents, problems, and any Third Party / Partner Planned Engineering Works (PEWs).

CHANGE TYPES

Changes can be segmented into the following categories:

- **Standard/Simple Change** - is an individual pre-approved Change that is low risk, relatively common and follow an agreed set procedure or work instruction. Requests are to be managed via the BT Security Change Manager portal. The Buyer Handbook, provided to a Buyer when the service goes live, sets out how the Buyer can submit these changes. The Buyer Handbook will be issued by the Security Optimisation Manager (SOM) for the Managed Service level they have purchased.
    - **Standard** - the target timeframe is 8 hours and has no additional charge associated.
    - **Urgent** - the target timeframe is 4 hours and has a monthly reasonable use policy associated.
- **Complex Non-Contract Affecting** Change - any Change to a product/solution that is not a Standard Change, or an Emergency Change go through the full assessment, authorisation, and implementation steps of the Manage Service Change process. Requests are to be managed via the My Account Change Manager application tool and the Buyer Handbook provided to a Buyer when the service goes live sets out how the Buyer can submit these changes. The Buyer Handbook will be issued by the SOM for the Managed Service level they have purchased.
- **Complex Contract Affecting Change** - any Change that is not defined in the change catalogue or impacts the Buyer contract will follow the Manage Service Order process.
- **Emergency Change** - is a highly critical, Standard Change that must be implemented as soon as possible specifically to address an issue having an adverse impact to business operations, or to prevent or resolve a Major Incident.

Service Summary

The Supplier will implement changes to the CSP(s) in response to a Buyer's request subject to the following process:

- The authorised Buyer Contact will submit requests to change the CSP(s) through the BT Web Portal, providing sufficient detail and clear instructions as to any changes required.
- The Supplier will check each request for its complexity and assess whether the change should be completed via the CSP Change Management Process or whether it should be handled as a chargeable service, scheduled for delivery within mutually agreed timescales.
- Only policy configuration changes can be made via this method. Changes that require additional hardware, licences, or contractual changes to billing (including changes to ongoing recurring charges) should be progressed via contract change control.
- The responsibility for the Security Policy implemented remains with the Buyer, and BT is not liable for potential or actual breaches arising where BT has correctly implemented Buyer-requested changes.
- The Supplier may provide the Buyer with Professional Services at an additional Charge, at their request, to assist them in writing their change request.

2.3.4.3.1 Managed Service (MS)1

- In respect of the Virtual Firewall, the Buyer is responsible for all aspects of CSP configuration which will include CSP changes.
- The Supplier may provide assistance in rectifying problems relating to misconfiguration of the Virtual Firewall, and BT will charge the Buyer for this on a Professional Services basis at an additional Charge.

SUPPLIER OBLIGATIONS

The Supplier will:

- Provide authorised Buyer representatives with the ability to raise change requests on the Supplier and will only make Changes with an authorized Change Request.
- Simple Changes subject to the Reasonable Use Policy are included in the Charges.
- Complex Change requests will proceed in accordance with Clause 31 (Service Amendment) of the General Terms and the Supplier will charge the Buyer the cost of implementing Complex Changes.
- Communicate the status of change requests via e-mail (including notifications to log in to the relevant system to view) to the Buyer Contact requesting the change and the status will be available also on the BT Web Portal for a period of six months.

- Have overall responsibility for all Changes relating to the Technical Services until the Change is closed.
- Record Changes retrospectively, e.g. where an Incident has meant a piece of hardware needs to be replaced.
- Define and implement measures to avoid unnecessary recurrence of failed Changes.
- Track and monitor Changes throughout their lifecycle to ensure good progress is being made and Changes are implemented correctly and in a timely manner.
- Provide report capability to the Buyer detailing an agreed set of performance metrics.
- Use the standard BT toolset as the primary mechanism for the management of Changes.
- Apply the following "reasonable use" restrictions ("Reasonable Use Policy") for changes to the CSP(s):
    - The Buyer will not raise Standard Change requests more frequently than:
        - 6 per month in respect of MS 1;
        - 8 per month in respect of MS 2; and
        - 10 per month in respect of MS 3;
    - The Buyer will not raise Urgent Change requests more frequently than:
        - 1 per month in respect of MS 1;
        - per month in respect of MS 2; and
        - per month in respect of MS3;
- Where the Supplier's measurements show that change requests are being raised more frequently, BT may, either:
    - Aggregate requests over a period of time, so that they may be implemented more efficiently. In this event there may be some implementation delays.
    - Review requirements and agree with the Buyer an appropriate alternative implementation process and any associated charges.
    - Process the changes permitted under the Reasonable Use Policy in the Target Implementation set out in the table below:

Request	Target Implementation Time: target implementation from acceptance by BT of the Buyer's change request
Urgent Change and Emergency Change	4 Hours
Standard Change	8 Hours

- There is no Target Implementation Time for Complex Changes
- Service Credits will not apply to any CSP(s) change requests.
- Use reasonable endeavours to implement an Emergency Change as quickly as is reasonably practicable. BT will charge the Buyer the cost of implementing an Emergency Change.
- May implement an Emergency Change without the Buyer's approval.

BUYER OBLIGATIONS

The Buyer will:

- Keep the agreed list of representatives current and notify BT of changes.
- Changes received by BT are deemed to be fully approved by the Buyer; responsibility for the impact of BT applying such changes remains with the Buyer.
- Provide sufficient detail and clear instructions as to any changes required and where appropriate use the agreed change manager process to enable the change to be fully assessed.
- Provide an appropriate point of contact for the approval of emergency changes.
- Where appropriate, cooperate with BT to undertake any Buyer activities which are necessary to progress Changes.
- Where access to a Buyer site is required, assist BT with arranging this, and provide an on-site point of contact.
- Carry out post implementation test of a change and confirm that the change has been implemented successfully.
- Confirm closure of changes to the Supplier.

2.3.4.3.2 Managed Service (MS)2

In addition to MS1:

- In respect of the Virtual Firewall, the Supplier will implement the changes by default. The Buyer may choose to carry out the CSP configuration and CSP changes, in which case the provisions in MS1 Level of service will apply.
- The authorised Buyer Contact may submit requests to modify the CSP(s) either through the BT Web Portal or direct to the Security Optimisation Manager.

2.3.4.3.3 Managed Service (MS)3

In addition to MS 2s:

The Supplier will use reasonable endeavours to identify errors or potential unforeseen consequences of the Buyer's requested Simple Changes and Complex Changes and advise them appropriately and will not be liable for any consequence arising from:

- Misspecification of a Buyer's security requirements in the CSP(s)
- Unforeseen consequences of a correctly implemented CSP(s), as specified by the Buyer.

2.4 Definition of Differentiation between Service Levels

Service Capability	MS1	MS2	MS3
Category of Change available			
Standard	✓	✓	✓
Complex Non-Contract Affecting	✓	✓	✓
Complex Contract Affecting	✓	✓	✓
Emergency	✓	✓	✓

Service Capability	MS1	MS2	MS3
Volume of Standard Changes per month			
6 Standard Changes	✓	×	×
8 Standard Changes	×	✓	×
10 Standard Changes	×	×	✓
Change resource			
Shared 24/7	✓	✓	✓
Delegated Operational resource for Emergency Change Management 24/7	✓	✓	✓
Customer Interaction / contact			
Access to BT Service Desk for visibility of all Changes	✓	✓	✓
Access to nominated BT Change Management team	✓	✓	✓
Language support other than English	×	×	×
Investigation of Customer raised issues relating to Change	✓	✓	✓

Support for Customer requests to assist with Customer-owned Change Management activities	✓	✓	✓
Roles and Responsibilities			
BT Security Change Team BT Security Change Team takes ownership of Standard and Complex change requests. Ensuring the SLAs are met. Their scope of work includes: Monitoring the tracking of Change Requests Ensuring the Change SLAs are met Customer interaction via My Account / Change Tooling Point of contact for all Change Requests Engaging with manufacturers´ specialists (where direct vendor engagement is required) Engagement with subject matter experts where needed Creation of quotes for changes and provided back to the customer Accountable for Change reporting cycles for each Service Layer Accountable for all change execution decisions Customer interact via conference call and My Account	✓	✓	✓
Security Operation Team BT Security Operation Team take ownership of executing changes. Ensuring the SLAs are met. Their scope of work includes: Performing Change execution activities Responsibility of delivery of changes Point of contact for MS3 Layer Service Engaging with manufacturers´ specialists (where direct vendor engagement is required) Engagement with subject matter experts where needed Customer interaction via BT Security Change Team	✓	✓	✓
Reviews			
Bi-annual reporting - list of changes with their resolutions and execution times	✓	✗	✗

Service Capability	MS1	MS2	MS3
Quarterly Reporting - list of changes with their resolutions and execution times	✗	✓	✗
Monthly Reporting - list of changes with their resolutions and execution times	✗	✗	✓
Documentation			
Forward Schedule of Change maintained and visible to the Customer	✓	✓	✓
Tooling			
BT to use standard BT tool for Change Management	✓	✓	✓
Customer has visibility of BT Change Record	✓	✓	✓
Customer has ability to approve through the portal/tool	✓	✓	✓
BT to follow standard process for Change Management	✓	✓	✓
SLA's & KCI's			
Auto-generated monthly service performance reporting on a standard set of Change metrics	✓	✓	✓
KCI (Keeping Customer Informed) Method. Ticketing system, either through automated email push or through web portal / My Account, using BT standard format Contact details via the portal if required for urgent cases	✓	✓	✓
BT will keep the customer informed on our progress when the change status is: work in progress BT will provide a confirmation of the change being raised within 15 minutes: • Standard changes - executed within 8 hours • Complex contract affecting - subject to BT assessment • Complex non-contract affecting - executed dependant on change domain	✓	✓	✓
There will be no status updates while we are waiting on customer input / feedback or outside contracted hours	✓	✓	✓
KPI's			
On time execution - on time execution is a key performance measure. With on time execution, we measure our service change performance, which changes do or do not meet their contractual SLA	✓	✓	✓
Customer experience - Based on recent executed changes we might send a one-click survey to end	✓	✓	✓

customer contacts to capture their feedback based on their experience with us. Customers are presented with a single question relating to their overall experience. This is to gather feedback from the customer to measure how satisfied they are with the way we are handling service issues. The customers are also given an option to leave verbatim. We need customer contact details (email addresses) to where we can sent the change related surveys.			

2.5 Pricing and License Options

- For a given specified service, prices are a mix of One time Charges (OTC), variable recurring and fixed recurring (monthly). Examples are;
    - One Time Charge or Installation charge– initial service installation or subsequent site visit,
    - Variable recurring – policy configuration changes charged per occasion
    - Fixed recurring – service management charges, and hardware
- Where BT provides price quotations, these are valid for 60 days. prices are reviewed monthly to take account of currency fluctuations
- Pricing (via the "Global MSSP DCF" pricing tool) is provided in 3 currencies: UK£, US$, Euros.
- changes to service may be subject to revised charges and potentially revised contracts; the standard 28 days' notice will apply
- No undertaking is given within standard prices to cover refresh of equipment (e.g. for end-of-life), or application upgrades (e.g. for new features).

2.5.1.1 Price Model – Service Wrap

The service wrap charges are a combination of One-Time Charges (OTC) and Monthly Recurring Charges (MRC).

Service Stage	OTC	MRC	Comments
Initial Set-up	X		Charged after Initial Set-Up
Controlled Deployment	X		Charged after Initial Set-Up
Monitoring & Management		X	Monthly recurring in advance
Continuous Improvement & Tuning		X	Monthly recurring in advance

3 Security Requirements

Due to the nature of the service within scope of this service offer, optional Call-Off Schedules 9A (Security: Short Form), 9B (Security: Consultancy), 9C (Security: Development), 9D (Security: Supplier-led Assurance) and 9E (Security: Buyer-led Assurance) are excluded and the **Suppliers standard Security Management Plan applies only**.

Additionally, BUYER'S SECURITY REQUIREMENTS AND ICT POLICY SECURITY REQUIREMENTS within the Call-Off Order Form will be marked with the option **There are no Security Requirements for the purposes of this Call-Off Contract** and SECURITY ASPECTS LETTER will be marked as **not applicable**.

3.1 The Security Management Plan

The Security Management Plan (SMP) defines the security measures that are implemented, and maintained, by BT. BT will maintain the adherence to the contracted security measures.

The plan supports the provision of the services in scope of this service offer and covers the following:

- Our approach to security
- Our information security policy
- External parties
- Human resource security
- Physical and environment security
- Asset management
- Operation of the plan
- The security lifecycle

3.2 Security Accreditation and Governance Standards

Security accreditation and governance standards will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

3.3 Operational Security

Operational security will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

3.4 Asset Protection

Operational security will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

3.5 Cyber Essentials Certification

Cyber essentials certification was a mandatory requirement to secure a place on the framework as a Supplier and to maintain our place on the agreement, all Suppliers must present evidence to Crown Commercial Service (CCS) of their continued certification.

Therefor the option under CYBER ESSENTIALS CERTIFICATION within the Call-Off Order Form under is marked as not applicable and for the purposes of Call-Off Schedule 27 (Cyber Essentials Scheme), clauses 2.1 to 2.4 are not used.

3.6 Staff Vetting Requirements and Background Checks

Staff vetting requirements will be in line with the details defined within the Suppliers Digital Marketplace submission and this Service Definition document and STAFF VETTING REQUIREMENTS within the Call-Off Order Form will be marked accordingly.

Our recruitment process includes pre-employment screening and vetting prior to placement to ensure adequate levels of confidentiality are maintained, screening includes:

- Application for a criminal record check
- Giving us contact details for reference checks
- Health declaration
- CIFAS- Staff Fraud Database check.

Additional checks are made when dealing with particularly sensitive positions (such those involved with sensitive contracts). The normal undertakings signed by individuals at recruitment include non-disclosure provisions and it is a disciplinary offence to misuse any information obtained from Supplier systems. Offenders are subject to disciplinary action up to and including dismissal and may be subject to prosecution, while ensuring compliance with local legislation.

Due to the nature of the service within scope of this service offer, optional Call-Off Schedule 18 (Background Checks) is excluded and in the event that Supplier Staff do not have the necessary clearance required, the Parties will agree an acceptable alternative such as escorted access.

4 Personal Data

Personal data in relation to services in scope of this service offer is divided into 2 areas:

- Managing the contract
- Managing the services

Personal data, where required to be managed, complies with the requirements of clause 17 Data protection and security, within the Framework Core Terms including new Clause 17.7 included via Framework Special Term 13

4.1 Managing the Contract

Joint Schedule 10 (Processing Data) will be completed to define what types of personal date in relation to managing the contract may be held, the nature and purposes of the processing and will confirm The Parties are Independent Controllers of Personal Data.

4.2 Managing the Service

Where personal data is held as part of delivering the service, how this will be managed will be defined, where applicable, within the Suppliers product specific Terms and Conditions that are attached to the Suppliers Digital Marketplace entry for this service offer. The Suppliers Digital Marketplace entry also confirms details of data storage and processing locations specific to this service.

The Supplier, including any Sub-processors of the Supplier, may from time to time use back-office support and system functions which are located or can be accessed by Users from outside of the UK and/or the European Economic Area. Any such processing will be in accordance with Joint Schedule 10 Paragraph 5.5.2, and for the purpose of clause 5.5.2 (a), the Buyer consents to the disclosure and transfer of Data, including Personal Data, as required in order to provide the Service.

4.3 Sub-processing

The Buyer consents to the Supplier's use of Sub-processors in accordance with the Framework Agreement. The Supplier will ensure that data protection obligations in respect of Processing Buyer Personal Data that are broadly comparable to those set out in the Framework Agreement and will be agreed with any Sub-processors.

The Supplier will inform the Buyer of intended changes to its Sub-processors from time to time, either by providing the Buyer with online access to intended changes or by such other means as the Supplier may determine. If the Buyer does not object to the proposed change within 30 days of this notice, the Buyer will be deemed to have authorised the use of the new Sub-processors.

5 Other Service Considerations

The service described in this Service Definition is based on the Supplier's standard offering for this cloud service and the contract is not defined as a Critical Service Contract. It should be noted that the G Cloud 15 Call-Off Order Form has a number of mandatory schedules, optional schedules and Call-Off Order Form options, and this section clarifies the position of these options for this service as provided by the Supplier. The service will additionally be delivered in line with the Supplier Terms and Conditions included within the Suppliers Digital Marketplace submission.

5.1 Modern Slavery, Environmental Requirements and Sustainability

To comply with the reporting requirements to the Buyer as defined within Joint Schedule 5 (Sustainability) the Buyers can access the Suppliers annual Modern Slavery Report, and where required (for lots 1a and 1b only) its Carbon Reduction Plan here Our reports & policies - Responsible business | BT Plc

Optional Call-Off Schedule 25 (Additional Sustainability Requirements) is excluded. The Suppliers approach to sustainability, managing our environment, and our modern slavery policies can be found here Our reports & policies - Responsible business | BT Plc

Optional Call-Off Schedule 26 (Carbon Reduction) is excluded. The Suppliers approach to carbon reduction and our carbon reduction plans can be found here Our reports & policies - Responsible business | BT Plc

5.2 Financial Difficulties

For the purpose of Joint Schedule 7 (Financial Difficulties), the Ratings Agencies listed within Annex 1 (Rating Agencies and their standard Rating System) will be Standard & Poor and Moody's and for Annex 2 (Credit Rating Thresholds) these will be BB+ for Standard and Poor and Ba1 for Moody's.

BT's published ratings are available here

5.3 Guarantee

For the purpose of Joint Schedule 8 (Guarantee), the Buyer does not require a Guarantee from the Supplier to award the contract.

5.4 IPR

For the purpose of Call-Off Schedule 1 (Intellectual Property Rights) **Part A Option A3: Supplier ownership of all New IPR with Buyer rights for the current contract only**; applies and is not further amended on the Call-Off Order Form under INTELLECTUAL PROPERTY RIGHTS.

5.5 Staff Transfer

No staff transfer is required and for the purposes of Call-Off Schedule 2 (Staff Transfer) **Part C: No Staff Transfer on the Start Date** only applies.

5.6 ICT Services

ICT services, where applicable, will be managed in line with the details defined within the Suppliers Digital Marketplace submission and supporting Supplier Terms, and where applicable within this Service Definition document and optional Call-Off Schedule 6 (ICT Services) is excluded, and the option under ICT POLICY within the order form will be marked as not applicable. Any maintenance of the ICT environment, where applicable, will be defined within this Service Definition document and the option under MAINTENANCE OF THE ICT ENVIRONMENT within the Call-Off Order Form will be marked as not applicable.

5.7 Business Continuity and Disaster Recovery

As noted by CCS guidance provided within Framework Schedule 6 (Order Form Template), optional Call-Off Schedule 8 (Business Continuity and Disaster Recovery) is not applicable for services under lots 2a and 2b and is excluded.

5.8 Corporate resolution planning

Due to the nature of the services within scope of this service offer, , which is available only when the Call-Off Contract is not a Critical Service Contract, optional Call-Off Schedule 24 (Corporate Resolution Planning) is excluded.

5.9 Exit Management

Optional Call-Off Schedule 10 (Exit Management) is excluded and at the end of the Call Off Contract Period, the offboarding process will be managed in line with the details defined within the Suppliers Digital Marketplace submission and where applicable within this Service Definition document. The Call-Off Order Form SPECIFIC EXIT MANAGEMENT ASSISTANCE (LOT 1A AND LOT 1B ONLY) and VIRTUAL LIBRARY will both also marked as not applicable.

5.10 Clustering and Leasing

Services will be contracted and invoiced to the Buyers detailed within Framework Schedule 6 (Order Form Template) and as such optional Call-Off Schedule 12 (Clustering) is excluded.

Due to the nature of the services within scope of this service offer, leasing of services is not applicable and as such, optional Call-Off Schedule 22 (Lease Terms) is also excluded.

5.11 Implementation Plan and testing

Due to the nature of the services within scope of this service offer, optional Call-Off Schedule 13 (Implementation Plan and Testing) is excluded and the services in scope will be implemented and tested in line with the details defined within the Suppliers Digital Marketplace submission and this Service Definition document.

5.12 Performance Levels

Due to the nature of the service within scope of this service offer, optional Call-Off Schedule 14 (Performance Levels) is excluded and the service levels provided are as defined within the Suppliers Digital Marketplace submission and this Service Definition document.

5.13 Service Credits

Any service credits for the services within scope of this service offer will be as detailed, where applicable, within this Service Definition document and SERVICE CREDITS within the Call-Off Order Form will be marked accordingly.

5.14 Call Off Schedule 17 (MOD Terms)

Where optional Call-Off Schedule 17 (MOD Terms) is required, this will be based on no additional DEFCONS or DEFFORMS being added within Annex 1 which incurs additional costs to the Supplier.

5.15 Call Off Specification and Deliverables

The services will be delivered in line with the Suppliers Digital Marketplace submission and this Service Definition document and as such, optional Call-Off Schedule 20 (Call-Off Specification) is excluded.

5.16 Call Off Special Terms

Due to the nature of the services within scope of this service offer based on the Supplier's standard offering for this cloud service, no additional call off special terms are introduced into the Call-Off Order Form under CALL OFF SPECIAL TERMS

5.17 Service Request Process

The service request process with be as defined within the Suppliers Digital Marketplace submission and this Service Definition document and SERVICE REQUEST PROCESS within the Call-Off Order Form will be marked accordingly.

5.18 Minimum Commitments

Any MINIMUM COMMITMENT(S) where applicable noted within Call-Off Order Form will be aligned to those as defined within the Suppliers Digital Marketplace submission and Suppliers Price Card where applicable and MINIMUM COMMITMENT(S) within the Call-Off Order Form will be marked accordingly.

5.19 Maximum Liability

The limitation of liability for this Call-Off Contract remains as stated in Clause 14.2 of the General Terms (as that Clause 14.2 has been amended pursuant to Framework Special Term 12 as set out in the Framework Award Form) and is not further amended on the Call-Off Order Form under MAXIMUM LIABILITY.

5.20 Additional Insurances

There is no requirement for additional insurances which will remain as defined within Joint Schedule 3 (Insurance Requirements) and ADDITIONAL INSURANCES on the Call-Off Order Form will be marked as not applicable.

5.21 Product Roadmaps

Any defined product roadmaps, where applicable, will be defined within this Service Definition document and PRODUCT ROADMAP (IF APPLICABLE) within the Call-Off Order Form will be marked as not used.

5.22 Quality Plans

Any defined quality maps, where applicable, will be defined within this Service Definition document and the option under QUALITY PLANS within the Call-Off Order Form will be marked as not applicable.

5.23 Social Value Commitment

Social value is at the heart of our purpose, driving impactful initiatives that address the needs of diverse communities across the UK. Our dedicated Social Value team have a focus on sustainability, community, sponsorship, charity, and the environment.

We're increasing digital inclusion and giving back to local communities through on-the-ground initiatives that make real-world positive changes.

The five pillars of social value at BT are:

- Outreach: no one is forgotten in our social value delivery.
- Improvement: continuous improvement in our delivery.
- Sustainability: our incentives are built to last.
- Engagement: user voice at the forefront and not an afterthought.
- Equity: leveraging our power to mobilise individuals, institutions, and communities

Details and reporting on what we are doing around social value can be found here Social Value At BT | About Us and SOCIAL VALUE COMMITMENT within the Call-Off Order Form will be marked accordingly and no additional bespoke commitments or reporting will be included.

Copyright

Registered office: One Braham, Braham Street, London, E1 8EE

Registered in England no. 1800000

BT is an ISO 9001 Registered Company

Company information

Parent Company: BT Group plc

Company Legal Entity Name: British Telecommunications plc

Company Trading Name: BT

Address: One Braham, Braham Street, London, E1 8EE

Web Address: https://business.bt.com/