COMCAST ENTERPRISE SERVICES
PRODUCT-SPECIFIC ATTACHMENT
UNIFIED THREAT MANAGEMENT (UTM)

ATTACHMENT IDENTIFIER: UTM, Ver. 1.0

The following additional terms and conditions are applicable to Sales Orders for Comcast's UTM Services:

DEFINITIONS

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

"**Architectural Confirmation Document**" or "**ACD**" means the document containing the initial configuration for the Service, as agreed to by Customer and Comcast.

"Base Service" means the Comcast-provided SD-WAN service or ActiveCore℠ Router Service by which the Service is provided.

"Comcast Data" means any and all data provided to Customer by Comcast, Comcast's Affiliates, or Comcast's vendors or that is collected by Customer or its subcontractors on Comcast's behalf.

"Comcast Systems" means applications, websites, computing assets, systems, databases, devices, products, or services owned or operated by or for Comcast (including the ActiveCoreDX and Advanced Security Customer portals), but excluding any Customer Systems.

"Customer Devices" means computing, storage, or networking devices operated by or on behalf of Customer that Process Comcast Data or that are used to access Comcast Systems.

"Customer System" means any Customer or its subcontractors' applications, websites, computing assets, systems, databases, devices, products, or services that process Comcast data.

"Estimated Availability Date" means the target date for delivery of Service.

"Information Security Standards" means prescribed for use by the National Institute of Standards and Technology, aligned with the International Organization for Standardization/International Electrotechnical Commission 27000 series of standards.

"Process" and its cognates means any operation or set of operations that is performed on information, including collection, storage, transmission, disclosure, erasure, and destruction.

"Service(s)" means UTM service(s).

"**Underlay Service**" means the internet connectivity over which the Service operates.

ARTICLE 1. SERVICES

This attachment shall apply to UTM Services. A further description of these Services is set forth in Schedule A-1 hereto which is incorporated herein by reference.

ARTICLE 2. PROVIDER

The Services shall be provided by Comcast Business Communications, LLC ("Comcast").

ARTICLE 3. PROVISIONING INTERVAL

Following the Customer's acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Service on or about the Estimated Availability Date; provided, however, that Comcast's failure to provision Services by the Estimated Availability Date shall not constitute a breach of the Agreement.

ARTICLE 4. SERVICE COMMENCEMENT DATE

The Service Commencement Date shall be the date Comcast informs the Customer that the Service is available and performing in accordance with the "Performance Standards" set forth in Schedule A-1 hereto ("Availability Notification").

ARTICLE 5. TERMINATION CHARGES

In the event that Service is terminated on or following the Service Commencement Date but prior to the end of the applicable Service Term, Customer shall pay Termination Charges solely on the underlying Comcast-provided Underlay Service and Base Service, if any, as provided in the applicable PSA(s).

ARTICLE 6. ADDITIONAL INFORMATION

If the Customer's Underlay Service is provided by a third-party, Customer's Base Service must be interconnected with such third-party provided Underlay Service in accordance with the applicable PSA.

ARTICLE 7. CUSTOMER PORTAL

Comcast provides the Customer with a password-protected web portal to access information regarding the Customer's Service. Customer may have the option to use the portal to enter changes to the Customer's UTM configuration, subject to the availability of the configuration service, as determined by Comcast.

ARTICLE 8. TECHNICAL SPECIFICATIONS AND PERFORMANCE STANDARDS

The technical specifications and performance standards applicable to the Service are set forth in Schedule A-1 hereto.

ARTICLE 9. INFORMATION SECURITY REQUIREMENTS

9.1 Access to Comcast Systems. Customer must meet the following requirements with respect to its access to any Comcast Systems:

(i) Customer must use reasonable identity and access management processes that meet or exceed Information Security Standards;

(ii) Customer must use unique user/system identities and must prohibit the use of shared, default, or temporary credentials;

(iii) Customer must terminate the access of any end user or, if unable to terminate directly, must notify Comcast within twenty-four (24) hours, if an end user no longer needs access to a Comcast System;

(iv) Customer devices must lock after a reasonable period of inactivity and must disable upon repeated, failed access attempts;

(v) Customer must periodically conduct user access reviews no less frequently than every six (6) months and must cooperate with any access reviews conducted by Comcast;

(vi) Customer may only access Comcast Systems to the extent necessary to Process Comcast Data;

(vii) Customer must comply with all security requirements when accessing Comcast Systems, which may include Comcast virtual private networks, transport encryption, and multi-factor authentication;

(viii) Only approved connections to a Comcast System using the Comcast approved protocols and services may be used;

(ix) Upon request, Customer must document the ports, rules, and protocols acceptable to Comcast; and

(x) Comcast may suspend or terminate access to a Comcast System without notice and without penalty.

9.2 Maintenance. If the Services require the reconfiguration of Customer Systems or Comcast Systems for maintenance or support, when such configurations are no longer necessary or upon Comcast request, Customer must revert such reconfigurations. To the extent that only Comcast can make such reconfigurations, Customer must inform Comcast and assist Comcast in making such reconfigurations.

9.3 Customer Devices. Customer must implement and maintain reasonable security standards for all Customer devices that meet or exceed Information Security Standards, including but not limited to timely patch management, and (a) usage of next generation threat detection or (b) real time anti-virus monitoring and updates and full scans (including system and boot files) as frequently as recommended by Information Security Standards. All Customer devices must be owned or leased and managed by Customer or its subcontractors. Customer must only Process Comcast data or access Comcast Systems from Customer Devices or devices provided by Comcast. Customer must maintain device management controls for all mobile Customer Devices with access to a Comcast System. Such controls must include the ability to wipe the device remotely.

9.4 Customer End Users. Customer is responsible for the acts and omissions of all end users. Customer must ensure that end users do not retain any Comcast data, any Comcast device, or access to any Comcast System at the request of Comcast.

COMCAST ENTERPRISE SERVICES
PRODUCT-SPECIFIC ATTACHMENT UNIFIED THREAT MANAGEMENT

SCHEDULE A-1
SERVICE DESCRIPTIONS, TECHNICAL SPECIFICATIONS AND PERFORMANCE STANDARDS

Comcast's UTM Service will be provided in accordance with the service descriptions, technical specifications, and performance standards set forth below:

1. Service Descriptions

UTM is a comprehensive security service that can be delivered via the cloud or Comcast Equipment located at the Customer premises, as requested by Customer.

The Service is available in the below product tiers, which may include all or a subset of the listed features:

Basic Service:

A. Next Generation Firewall
   i. Source, destination, application/protocol enforcement

B. Web Filtering
   i. Based on automatic security intelligence tools and targeted threat analysis, real-time updates designed to enable Customer to apply granular policies that filter web access based on content categories

Advanced Service (in addition to A and B above):

C. Intrusion Prevention Service (IPS)
   i. Implements a database of thousands of signatures, designed to stop attacks that evade conventional firewall defenses

Enterprise Service (in addition to A, B, and C above; requires Advanced Customer Care):

D. Denial of Service (DOS) Protection
   i. Helps prevent attackers bringing down a machine or network resources by overwhelming services using a flood of traffic

E. Anti-Virus Service
   i. Employs advanced virus, spyware, and heuristic detection engines designed to protect endpoint security agents, to help prevent both new and evolving threats from gaining access to your network's content and applications

F. Malware Service
   i. Cloud-based threat analysis service that provides analysis and helps prevent for zero-day exploits and malware

G. Data Loss Prevention
   i. Data loss prevention software detects potential data breaches/data ex-filtration transmissions and helps prevent them by monitoring, detecting and blocking sensitive data

2. Service Requirements

In order to provide the Service to a Customer's Service Location, the Service Location must have an Underlay Service and Base Service. With respect to the Underlay Service, Comcast supports the Service over Comcast Ethernet Dedicated Internet (EDI) Service, Comcast Business Internet Service, or internet connectivity services provided by a third-party service provider. If the Base Service or Underlay Service is terminated at a Service Location or unavailable for any reason at any time, the Service at said Service Location will be inoperable.

3. Technical Specifications

3.1 Universal Customer Premise Equipment (uCPE): Comcast will provide robust, flexible, high powered uCPEs based on x86 hardware that is service agnostic and can deploy Virtualized Network Functions ("VNFs") as needed based on Customer requirements.

3.2 In the UTM Cloud offering, an IPSEC tunnel will be provisioned from the Customer Service Location(s) (single or multiple sites) as defined in the ACD. All traffic destined to the Internet is inspected in the UTM cloud, and egresses from that location. Local internet breakout is not a connectivity service and is solely a route configuration inside the uCPE to allow the local host to access the internet.

3.3 **IP Address Allocation.** The uCPE will use a single IP address provided from the Underlay Service.

4. Service Delivery and Service Management

4.1 Kick-off call: Comcast will sponsor a kick-off call with the Customer to explain the Service delivery process.

4.2 Technical interview: Comcast will engage Customer in one or several interviews related to Customer's network design initiatives. Comcast will document the technical information discovered through the interview process into an Architectural Confirmation Document and the Customer will review and confirm that the ACD is accurate. The ACD will be available via the Portal.

4.3 Install, Test, and Turn-up: Customer's Service will be installed with a standard set of pre-configured policies and Comcast will test the Services.

4.4 On-Going Solution Support: If Comcast or a Comcast vendor develops software updates and/or security patches for Comcast's or such vendor's equipment which Comcast uses to provide the Services, Comcast will upload such software updates and/or security patches to the applicable equipment to the extent Comcast determines, in its sole discretion, that such software updates and/or security patches are necessary. Updates or patches that are viewed as critical may require immediate action with a maintenance window. For the avoidance of doubt, Comcast shall have no obligation to develop software updates or security patches and its only obligation under this paragraph is to install updates and security patches developed by its applicable vendors to the extent Comcast determines, in its sole discretion, that such software updates and/or security patches are necessary.

4.5 Security Monitoring and Mitigation: The Service is designed to provide Customer notice of potential security threats detected by the Service; provided, however, that (i) the Service's failure to provide any such notice(s) shall not constitute a breach of the Agreement and (ii) Comcast and its affiliates and their respective officers, directors, employees, agents, suppliers, licensors, successors, and assigns shall have no liability to Customer for any damages that are alleged to or arise from or are caused by or alleged to have been caused by the failure to provide any such notice(s). Furthermore, Customer acknowledges and agrees that (a) Comcast will not make changes to Customer's configurations or security settings for the Services (including in response to any potential security threats of which Comcast has notified Customer) and (b) Customer maintains overall responsibility and liability for maintaining the security, confidentiality, and reliability of Customer's network, computer systems, and data, including implementing configuration changes to the Services in response to potential security threats. Customer further acknowledges that the Services are not a guaranty by Comcast to protect Customer's network, computer systems, or data against unauthorized access, malicious code, deleterious routines, threats, cyberattacks, ransomware and/or other techniques, attack vectors and tools employed by computer "hackers" and other third parties (including nation states) to create, exploit, or expose security vulnerabilities. Comcast makes no warranty, express or implied, that any specific or all security threats and vulnerabilities will be detected or mitigated or that the Services will render Customer's network and computer systems safe from intrusions and other security breaches. Comcast makes no guarantees with respect to the detection or blocking of viruses/worms/malware or any other types of attacks and is not responsible for any such malicious data that may be transmitted over the provided network. Comcast makes no warranty that the Services will be uninterrupted or error-free.

5. Advanced Customer Care

This Section 5 is in addition to the other Sections of this PSA and is only applicable to those Customers receiving Advanced Customer Care.

5.1 Advanced Install, Test, and Turn-up: When Comcast installs the Service, the configuration created for the Customer during the Kick-Off Call and Technical Interview will be loaded on the equipment and Comcast will test the Services.

5.2 On-Going Solution Support: Comcast will support Customer's requested configuration changes, in accordance with Comcast's then current configuration change policy (the "Configuration Change Policy"). Upon request, Comcast shall provide Customer with its then current Configuration Change Policy. Any moves, additions, changes, or deletions to the Services shall be requested via the Portal or over the phone. This includes any changes to the Service configuration as initially outlined in the ACD. Comcast has the following configuration change response objectives:

Category	**Objective**
Simple Configuration Change	4 hours
Complex Configuration Change	48 hours

"Simple Configuration Change" includes, but is not limited to, the following changes: addition of static route, bandwidth change (single site), button click changes in Edge configurations, account administration addition, SD-WAN FW entry update or change, SD-WAN NAT entry update or change, SD-WAN device remote restart, Edge type topology designation (Hub/Spoke), information request, IP changes, password reset, remote diagnostics, SD-WAN Quality of Service entry update or change, VLAN update or addition, and traffic steering change.

"Complex Configuration Change" includes, but is not limited to, the following changes: Edge device reconfigured, network schematic or restructuring, business policy change (extensive), SD-WAN software change or upgrade, SD-WAN device profile creation, SD-WAN network services control/create, SD-WAN FW policy creation, SD-WAN NAT creation, SD-WAN Quality of Service creation, SD-WAN device WAN/LAN connection port change, SD-WAN device WAN interfaces configuration, SD-WAN device LAN interfaces configuration, SD-WAN device LAN-side DHCP scoping or configuring, SD-WAN device LAN side DNS scoping or configuring, SD-WAN routing configuration, SD-WAN VPN tunnel configuration, SD-WAN 3rd party VPN tunnel configuration (site to site), and packet capture download packet capture file.

5.3 Security Monitoring and Mitigation: Comcast will have read/write access to the Service. At Customer's request and in accordance with the table above, Comcast will modify the configuration of the Service in accordance with Customer's specifications to attempt to mitigate security events and security threats identified by Customer. Comcast's sole obligation is to implement the configuration settings and configuration changes reasonably requested by Customer. Customer acknowledges and agrees that Comcast will not make changes to Customer's configurations or security settings for the Services (including in response to any potential security threats of which Comcast has notified Customer) except to the extent explicitly directed to do so by Customer in accordance with the terms of the Agreement.

6. Customer Responsibilities

Customers have the following responsibilities related to the installation, support, and maintenance of the Service.

6.1 Provide an operating environment with temperatures not below fifty-five (55) or above eighty-five (85) degrees Fahrenheit. Humidity shall not exceed ninety (90) percent at eighty-five (85) degrees Fahrenheit.

6.2 Provide secure space sufficient for access to one (1) standard, freestanding, equipment cabinet at each of the Customer facilities, no further than fifty feet from the Customer router or switch interface.

6.3 Provide power including UPS AC power equipment, circuit sizing to be determined, if applicable.

6.4 Provide emergency local generator backup service, if applicable.

6.5 Provide access to the buildings and point of demarcation at each Customer Service Location to allow Comcast and its approved Contractors to install Universal Customer Premise Equipment. Provide access to each location for regular (8am - 5pm) and emergency (24 hour) service and maintenance of Comcast's equipment and facilities.

6.6 If interfacing with a third-party IP service, provide, install and maintain a device that is capable of routing network traffic between the Service and the Customer's Wide Area Network.

6.7 Customer must provide a point of contact (POC) for installation, service activation, notices for Service Interruptions, and any maintenance activities.

7. Technical Support and Maintenance

7.1 Technical Support. Comcast provides Customers a toll-free telephone number to the Customer Enterprise Technical Support (ETS) that operates on a 24x7x365 basis. Comcast provides technical support for service-related inquiries. Technical support will not offer consulting or advice on issues relating to customer equipment not provided by Comcast.

7.2 Maintenance. Comcast's standard maintenance window is Sunday to Saturday from 12:00am to 6:00am local time. Scheduled maintenance is performed during the maintenance window and will be coordinated between Comcast and the Customer. Comcast provides a minimum of forty-eight (48) hour notice for non-service impacting scheduled maintenance. Comcast provides a minimum of seven (7) days' notice for service impacting planned maintenance. Emergency maintenance is performed as needed.