Services Schedule: Cloud Security Services ("CSSs")

This document forms part of, and applies only to the extent incorporated into, an applicable Statement of Work ("SOW"). The sub-sections herein explain the CSSs that are provided for Customer's Cloud Services environment(s), but only to the extent such services and activities are expressly included in an applicable SOW or expressly included in a CO. Syntax may update this Services Schedule from time to time by updating the linked version of this document, and the then-current linked version will apply.

Quick links to sections in this document:

Responsibilities Abbreviations

Below are explanations for the abbreviations used in the "Syntax" and "Customer" columns in the RACI tables within the sub-sections.

Responsibility	Abbr.	Description
Responsible	R	The Party performing the activity.
Accountable	A	The Party who oversees and approves the activity.
Consulted	C	Any Parties whose opinions should be considered when performing the activity
Informed	I	Any Parties who must be made aware that the activity is being performed.
N/A	AD	Additional Service (additional charges apply; may require a Change Request or separate SOW). As requested, services that require additional planning or a consulting component in order determine scope, effort, and costs. These services may be charged on a Time and Materials basis.

Note: The table(s) below indicates the responsibilities and services that Syntax provides as part of the standard Services, unless otherwise specified in the Notes column. Any responsibility or service not specifically identified below is not included in the standard Services and is the responsibility of Customer.

1. Managed Detection and Response ("MDR")

Syntax will provide Managed Detection and Response services to Customer for security protection of Customer's workstations and servers ("endpoints"). This Service is a cloud-based foundational strategy that is designed to deliver increased security and protection to Syntax customers. Primary elements include, but are not limited to, the following: simplified rollout, endpoint protection from malware, user behavior analytics, system behavior analytics, roaming protection and policy enforcement, and comprehensive network protection. This Service includes Security Operations Center ("SOC") services for monitoring and threat remediation, and serves to minimize the threats from zero (0) day attacks, insider threats, known security exploits, and ransomware events on Customer's in-scope endpoints.

MDR RACI for all Cloud Services except Co-Managed

(Syntax- or Customer-provided environments for AWS, Azure, GCP, and OCI; also, Syntax Enterprise Cloud)

Item	Description	Syntax	Customer	Notes
1.0	**Setup and Endpoint Management**			
1.0.1	Provide licensing	R, A	I	
1.0.2	Deploy agent	I	R, A	Not applicable with Microsoft Defender for Endpoint
1.0.3	Perform ongoing updates, tuning, and optimization on Syntax Security Platform	R, A		
1.0.4	Perform ongoing updates, tuning, and optimization on Customer's Microsoft Tenant	C, I	R, A	Microsoft Defender only
1.0.5	Provide 24x7 SOC monitoring	R, A	C, I	
2.0	**Incident Response/IoC**			

Item	Description	Syntax	Customer	Notes
2.0.1	Provide remediation plan for OS, network, and identity-related Incidents on Syntax-Managed Security Devices – Critical (P1) and High (P2) only	R, A	I	
2.0.2	Engage CIRT	C, I	R, A	AD *(see Responsibilities Abbreviations on page 1)*
2.0.3	Provide support of CIRT requests for information for Syntax-Managed Security Devices	R, A	C, I	
2.0.4	Provide support of CIRT requests for information non-Syntax-Managed Security Devices	C, I	R, A	AD *(see Responsibilities Abbreviations on page 1)*
3.0	**Malware Analysis**			
3.0.1	Conduct malware analysis on Syntax-Managed Security Devices	R, A	C, I	
3.0.2	Provide notification of P1 and P2 OS and network security events on Syntax-Managed Security Devices	R, A	I	Excludes the following: • OS and network security events (non-managed endpoints) • Security events above the OS for Syntax-Managed Security Devices • Security events above the OS (non-Syntax-Managed Security Devices) Additional charges apply if Customer wants Syntax to be R, A for the above-listed items
3.0.3	Acknowledge tickets for P1 (Critical) events within 24 hours	C, I	R, A	
3.0.4	Acknowledge tickets for P2 (High) events within 2 business days	C, I	R, A	

MDR RACI for Co-Managed Cloud Services only

(e.g., AWS/Azure Co-Managed Cloud Services)

Item	Description	Syntax	Customer	Notes
1.0	**Setup and Endpoint Management**			
1.0.1	Provide Syntax with access for installing, deploying, and maintaining CSS software	C, I	R, A	
1.0.2	Provide licensing	R, A	I	
1.0.3	Deploy agent (Co-Managed Devices)	R, C, I	A	Professional Services fees apply; Work performed will be billed against Cloud Support Retainer
1.0.4	Provide ongoing updates, tuning, and optimization (Co-Managed Devices)	R, A	R, I	
1.0.5	Provide 24x7 SOC monitoring	R, A	C, I	
2.0	**Incident Response/IoC**			
2.0.1	Provide remediation plan for OS, network, and identity-related Incidents on Syntax-Managed Security Devices – P1 (Critical) and P2 (High) only	R, A	I	
2.0.2	Engage CIRT	C, I	R, A	AD *(see Responsibilities Abbreviations on page 1)*
3.0	**Malware Analysis**			
3.0.1	Conduct malware analysis on Co-Managed Devices	R, A	R, C, I	
3.0.2	Provide notification of P1 and P2 OS and network security events on Co-Managed Devices	R, A	I	Excludes the following: • OS and network security events (non-managed endpoints) • Security events above the OS for Co-Managed Devices

Item	Description	Syntax	Customer	Notes
				• Security events above the OS (Co-Managed Devices) Additional charges apply if Customer wants Syntax to be R, A for the above-listed items
3.0.3	Acknowledge tickets for P1 (Critical) events within 24 hours	C, I	R, A	
3.0.4	Acknowledge tickets for P2 (High) events within 2 business days	C, I	R, A	

2. Vulnerability Monitoring ("VuMo")

Syntax will perform vulnerability monitoring for Customer's Endpoints when capable. This Service includes SOC services for P1 and P2 events only.

VuMo RACI for all Cloud Services except Co-Managed

(Syntax- or Customer-provided environments for AWS, Azure, GCP, and OCI; also, Syntax Enterprise Cloud)

Item	Description	Syntax	Customer	Notes
1.0	**Network-based Vulnerability Scans**			
1.0.1	Conduct periodic scans (no login to box) to identify risks on Syntax-Managed Security Devices	R, A	I	Monthly
1.0.2	Conduct periodic authenticated scans on Syntax-Managed Security Devices	R, A	I	AD *(see Responsibilities Abbreviations on page 1)*
1.0.3	Provide necessary access credentials for authenticated scans	C, I	R, A	
1.0.4	Provide image for network scanner	R, A		
1.0.5	Provide hardware based on vendor requirements for deployment of network scanner VM(s) as specified	C, I	R, A	
1.0.6	Provide necessary connectivity for access to network scanner	C, I	R, A	
1.0.7	Conduct database scans	R, A	I	AD *(see Responsibilities Abbreviations on page 1)*
1.0.8	Conduct OWASP scans	R, A	I	AD *(see Responsibilities Abbreviations on page 1)*
1.0.9	Conduct application scans	R, A	I	AD *(see Responsibilities Abbreviations on page 1)*
1.0.10	Acknowledge tickets for P1 (Critical) vulnerabilities within 24 hours	I	R, A	
1.0.11	Acknowledge tickets for P2 (High) vulnerabilities within 2 business days	I	R, A	
2.0	**Setup and Management of Real-time Vulnerability Detection**			
2.0.1	Deploy agent on Syntax-Managed Security Devices – in Customer owned cloud tenant	C, I	R, A	
2.0.2	Deploy agent on Syntax-Managed Security Devices – Syntax provided tenant	R, A	C, I	Only if Syntax is responsible for OS management
2.0.3	Configure and maintain agent	R, A		
2.0.4	Provide agent licensing	R, A		
3.0	**Remediation Plans**			
3.0.1	Provide remediation plan for Network and OS vulnerabilities for Syntax-Managed Security Devices - P1 and P2 only	R, A	I	
3.0.2	Provide remediation plan for Network and OS vulnerabilities for non-Syntax-Managed Security Devices - P1 and P2 only	R, A	I	AD *(see Responsibilities Abbreviations on page 1)*
3.0.3	Manage OS remediation plan - P1 and P2 only (Syntax-Managed Security Devices)	R, A	C, I	
3.0.4	Manage OS remediation plan for non-Syntax-Managed Security Devices - P1 and P2 only	R, A	I	AD *(see Responsibilities Abbreviations on page 1)*
4.0	Conduct White or Gray Box Penetration Tests	R, A		AD *(see Responsibilities Abbreviations on page 1)*

VuMo RACI for Co-Managed Cloud Services only

(e.g., AWS/Azure Co-Managed Cloud Services)

Item	Description	Syntax	Customer	Notes
1.0	**Network-Based Vulnerability Scans**			
1.0.1	Provide Syntax with access for installing, deploying, and maintaining CSS software	C, I	R, A	
1.0.2	Conduct periodic scans (no login to box) to identify risks (Co-Managed Devices)	R, A	I	Monthly
1.0.3	Conduct periodic authenticated scans (Co-Managed Devices)	R, A	I	AD *(see Responsibilities Abbreviations on page 1)*
1.0.4	Acknowledge tickets for P1 (Critical) vulnerabilities within 24 hours	I	R, A	
1.0.5	Acknowledge tickets for P2 (High) vulnerabilities within 2 business days	I	R, A	
2.0	**Real-time Vulnerability Detection**			
2.0.1	Provide Syntax with access for installing, deploying, and maintaining CSS software	C, I	R, A	
2.0.2	Deploy agent (Co-Managed Devices)	R, A	C, I	Professional Services fees apply; **Customer is responsible for allowing the agent to be deployed;** Work performed will be billed against Cloud Support Retainer
2.0.3	Configure and maintain agent	R, A	C, I	**Customer is responsible for allowing the agent to be configured and maintained;** Work performed will be billed against Cloud Support Retainer
2.0.3	Provide agent licensing	R, A		
3.0	**Remediation Plans**			
3.0.1	Provide remediation plan for Network and OS vulnerabilities (Co-Managed Device) – P1 and P2 only	R, A	C, I	Excludes the following: • OS and network security events (non-managed endpoints) • Security events above the OS for Co-Managed Devices • Security events above the OS (Co-Managed Devices) Additional charges apply if Customer wants Syntax to be R, A for the above-listed items
3.0.2	Manage remediation for vulnerabilities related to Managed Applications – P1 and P2 only	C, I	R, A	Professional Service Fees apply; If Service is M-IaaS only, then Customer is R, A; Work performed will be billed against Cloud Support Retainer
3.0.3	Manage remediation for vulnerabilities related to Third-Party / Customer-Owned Applications	C, I	R, A	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer

3. Cloud Security Posture Management ("CSPM")

(***Note:*** This service is only applicable to AWS, Azure, GCP, and OCI; does not apply to Syntax Enterprise Cloud.)

Syntax will provide CSPM services to Customer. Potential policy (based on, e.g., CIS standards) violations and security issues regarding Customer's cloud environment will be sent to the Syntax Security Operations Center ("SOC"). When a potential issue is detected, the system may record additional information, generate an alert and forward that alert to the SOC where an Incident will be created and acted upon in an attempt to remediate the alert. As with many cloud environments, subtle changes to cloud configuration can result in unexpected results. The SOC will consult with Customer in required cases to determine if a posture management configuration

change will potentially impact the Production environment and, if required, create a remediation plan to remediate that CSPM-specific Incident. The work required to create a remediation plan will be charged to Customer on a time and materials basis.

Syntax will provide licenses as well as install and configure the CSPM solution within a Syntax managed services provider ("MSP") tenant and provide the CSPM services for Customer's cloud environment (either Customer-owned or Syntax-provided tenant). Upon Go-Live of the CSPM, the SOC will be responsible for Incident management and respond to Customer for defined P1 and P2 Production events. A Production event is defined by notifications in the CSPM policy. Syntax will provide Incident management only through the pre-defined contact methods to Customer 24x7 in accordance with Customer's SOW.

CSPM RACI for all Cloud Services except Co-Managed

(Syntax- or Customer-provided environments for AWS, Azure, GCP, and OCI)

Item	Description	Syntax	Customer	Notes
1.0	**Setup**			
1.0.1	Create CSPM Tenant	R, A		
1.0.2	Create Cloud User / Role / Permissions	R, A	C, I	User must be created in each Cloud tenant
1.0.3	Enable CSPM access from Cloud Tenant – Customer-owned tenant	C, I	R, A	
1.0.4	Enable CSPM access from Cloud Tenant – Syntax-provided tenant	R, A	C, I	
2.0	**Connectors**			
2.0.1	Configure Cloud Connectors	R, A	C, I	
2.0.2	Configure Role-Based Access Control	R, A	C, I	
2.0.3	Manage Access for Cloud User Accounts	R, A	C, I	
2.0.4	Assign roles to users	R, A	C, I	
2.0.5	Tag Connectors	R, A	C, I	
3.0	**Access Control**			
3.0.1	Configure Risk Insights	R, A	C, I	
4.0	**Inventory**			
4.0.1	Monitor Resource Inventory	R, A		
4.0.2	Remediate resource misconfiguration	R, A	C, I	
4.0.3	Monitor instance vulnerability details	R, A	C, I	
4.0.4	Remediate Critical (P1) and High (P2) instance vulnerabilities on Syntax-Managed Security Devices	R, A	C, I	
4.0.5	Remediate Informational Low and Medium vulnerabilities	R, A, C	C, I	AD *(see Responsibilities Abbreviations on page 1)*
5.0	**Posture**			
5.0.1	Conduct Posture - Control Evaluations	R, A	C, I	
5.0.2	Conduct Posture - Control Evaluations - Remediation	R, A	C, I	
5.0.3	Conduct Posture - Infrastructure as Code Evaluations	R, A	C, I	
5.0.4	Conduct Posture - Syntax-Provided Infrastructure as Code Evaluations - Remediation	R, A	C, I	
5.0.5	Conduct Posture - Customer-Provided Infrastructure as Code Evaluations - Remediation	C, I	R, A	AD *(see Responsibilities Abbreviations on page 1)*
5.0.6	Manage Posture - Cloud Posture Resources	R, A	C, I	
5.0.7	Manage Posture - Cloud Posture Resources - Remediation	R, A	C, I	
6.0	**Policy**			
6.0.1a	***AWS Monitoring*** Define Compliance Policies	R, A	I	CIS Amazon Web Services Foundations, AWS Best Practices, AWS Lambda Best Practices, AWS Database Best Practices
6.0.1b	***Azure Monitoring*** Define Compliance Policies	R, A	I	CIS Microsoft Azure Foundations, Azure Data Service Best Practices, Azure Best Practices, Azure Function App Best Practices
6.0.1c	***GCP Monitoring*** Define Compliance Policies	R, A	I	CIS Google Cloud Platform Foundation, GCP Cloud Functions Best Practices, GCP Best Practices, GCP Cloud SQL Best Practices, GCP Kubernetes Engine Best Practices

Item	Description	Syntax	Customer	Notes
6.0.1d	***OCI Monitoring*** Define Compliance Policies	R, A	I	CIS OCI Foundation Benchmark, OCI Best Practices
6.0.2	Define Custom Policies	R, A	C, I	Associated with system- or user-defined-controls
6.0.3	Define Custom Control Permissions	R, A	C, I	
6.0.4	Manage Exceptions - Connectors and Tags	R, A	C, I	AD *(see Responsibilities Abbreviations on page 1)*
6.0.5	Manage Exceptions - Build Time Controls	R, A	C, I	AD *(see Responsibilities Abbreviations on page 1)*
6.0.6	Manage Exceptions - Run Time Controls	R, A	C, I	AD *(see Responsibilities Abbreviations on page 1)*
7.0	**Incident Response and Remediation**			
7.0.1	Configure Rule-Based Alerts (Egress to SOC)	R, A		Alerts into Syntax SOC
7.0.2	Configure SOC Actions	R, A		SOAR/TEA/VORTEX Implementation
7.0.3	Manage SOC Rule base	R, A		
7.0.4	Manage SOC General Alerts	R, A		Alerts into Syntax SOC

CSPM RACI for Co-Managed Cloud Services only

(e.g., AWS/Azure Co-Managed Cloud Services)

Item	Description	Syntax	Customer	Notes
1.0	**Setup**			
1.0.1	Provide Syntax with access for installing, deploying, and maintaining CSS software	C, I	R, A	
1.0.2	Create CSPM Tenant	R, A		
1.0.3	Create Cloud User / Role / Permissions	R, A	C, I	User must be created in each Cloud tenant
1.0.4	Enable CSPM access from Cloud Tenant	R, A	C, I	
2.0	**Connectors**			
2.0.1	Configure Cloud Connectors	R, A	C, I	
2.0.2	Configure Role-Based Access Control	R, A	C, I	
2.0.3	Manage Access for Cloud User Accounts	R, A	C, I	
2.0.4	Assign roles to users	R, A	C, I	
2.0.5	Tag Connectors	R, A	C, I	
3.0	**Access Control**			
3.0.1	Configure Risk Insights	R, A	C, I	
4.0	**Inventory**			
4.0.1	Monitor Resource Inventory	R, A		
4.0.2	Remediate resource misconfiguration	R, C, I	R, A	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
4.0.3	Monitor instance vulnerability details	R, A	C, I	
4.0.4	Remediate Critical (P1) and High (P2) instance vulnerabilities	R, C, I	R, A	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
4.0.5	Remediate Informational Low and Medium vulnerabilities	R, C, I	R, A	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
5.0	**Posture**			
5.0.1	Conduct Posture - Control Evaluations	R, A	C, I	
5.0.2	Conduct Posture - Control Evaluations - Remediation	C, I	R, A	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
5.0.3	Conduct Posture - Infrastructure as Code Evaluations	R, A	C, I	
5.0.4	Conduct Posture - Syntax-Provided Infrastructure as Code Evaluations - Remediation	C, I	R, A	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
5.0.5	Conduct Posture - Customer-Provided Infrastructure as Code Evaluations - Remediation	C, I	R, A	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer

Item	Description	Syntax	Customer	Notes
5.0.6	Manage Posture - Cloud Posture Resources	R, A	C, I	
5.0.7	Manage Posture - Cloud Posture Resources - Remediation	C, I	R, A	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
6.0	**Policy**			
6.0.1a	***AWS Monitoring*** Define Compliance Policies	R, A	I	CIS Amazon Web Services Foundations, AWS Best Practices, AWS Lambda Best Practices, AWS Database Best Practices
6.0.1b	***Azure Monitoring*** Define Compliance Policies	R, A	I	CIS Microsoft Azure Foundations, Azure Data Service Best Practices, Azure Best Practices, Azure Function App Best Practices
6.0.2	Define Custom Policies	R, A	R, C, I	Professional Service Fees apply; Associated with system- or user- defined controls; Work performed will be billed against Cloud Support Retainer
6.0.3	Define Custom Control Permissions	R, A	R, C, I	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
6.0.4	Manage Exceptions - Connectors and Tags	R, A	R, C, I	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
6.0.5	Manage Exceptions - Build Time Controls	R, A	R, C, I	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
6.0.6	Manage Exceptions - Run Time Controls	R, A	R, C, I	Professional Service Fees apply; Work performed will be billed against Cloud Support Retainer
7.0	**Incident Response and Remediation**			
7.0.1	Configure Rule-Based Alerts (Egress to SOC)	R, A		Alerts into Syntax SOC
7.0.2	Configure SOC Actions	R, A		
7.0.3	Manage SOC Rule base	R, A		
7.0.4	Manage SOC General Alerts	R, A		Alerts into Syntax SOC

4. Additional Information

- Upon Go-Live, Syntax will provide 24x7 SOC coverage in accordance with Customer's SOW.
- Specific tasks for MDR, Vulnerability Monitoring, and CSPM are detailed in the RACIs above.
- Software and license fees for CSSs:
  - ***For Syntax-Managed Services within Syntax-provided environments***, Syntax must provide MDR, Vulnerability Monitoring, and CSPM software that will be used for the Services, and license fees for this software are included in the scope of Customer's SOW.
  - ***For all other public cloud environments***, either Syntax can provide the MDR, Vulnerability Monitoring, and CSPM software, or Customer can provide this software (BYOL, and license fees for this software will be excluded from the scope of Customer's SOW).
- Service Level Agreements ("SLAs"): Without prejudice to any applicable SLAs listed in Customer's SOW, when Syntax is providing the MDR, Vulnerability Monitoring, and CSPM services, the SLAs in the table below will apply according to the "Applicable CSSs" column.
- All Incidents and Service Requests (each, a "ticket") are logged into Syntax's ITSM Portal and are assigned a response Priority Level according to the table below. Customer can access the recorded information within tickets during the Term of Customer's SOW.
- In the event that Syntax notifies Customer of a security issue through the ITSM Portal, Customer shall acknowledge receipt for P1 issues within 24 hours and P2 issues within two (2) business days. If Syntax does not receive acknowledgement within such timeframes, then: (a) additional actions requiring Customer approval or Customer participation may not be taken by Syntax regarding the security issue (ex. Critical patching for "Zero Day" exploit); (b) the related support ticket shall be set to 'waiting for customer'; and (c) Syntax will not escalate the support ticket in accordance with the agreed Incident escalation procedure until Customer responds.

Security Operations Center ("SOC") SLAs				
SOC Operational Availability – 24x7				
Ticket Response Times				
Priority Level	**Event Type**	**Incident Response Time**	**Service Request Response Time**	**Applicable CSSs**
P1 - Critical	Verified imminent threat to Customer Data and/or systems has occurred or is occurring	15 minutes	N/A	MDR, VuMo, CSPM
P2 - High	Indicator of Compromise ("IOC") – An artifact observed on a network or an OS that with a high degree of confidence indicates an intrusion has occurred or is currently occurring	30 minutes	N/A	MDR, VuMo, CSPM
P2 - High	Threat detected but quarantine failed – A malicious file or program was detected that was not successfully deleted or neutralized by the MDR solution	30 minutes	N/A	MDR only
P2 - High	Threat detected by user or system analytics; the MDR detected abnormal behavior based upon: 1) user or system behavior; and 2) known and unknown threat analytics	30 minutes	N/A	MDR only
P3 - Normal	Threat detected and quarantine successful – A malicious file or program was detected that was successfully deleted or neutralized by the MDR solution	2 hours	2 hours	MDR only
P4 - Low	Customer inquiries, features, or research requests	8 hours	8 hours	MDR only

In the event Customer has separately contracted with Syntax for enhanced security services under a separate SOW, the enhanced security services in such SOW shall supersede and replace the CSSs in this Schedule.

4.1. Monitoring and Automation

- **Overview**. Syntax shall deploy a multi-level monitoring and automation solution to facilitate reactive and proactive management of the Entitlements in Customer's SOW. Syntax will configure its monitoring and automation tools in accordance with proven industry standards and practices. All Syntax automation and monitoring infrastructure will be isolated from Customer Workloads.
- **Customer Portal**. The Customer Portal will allow Customer to manage and monitor the Workloads that are being managed according to Customer's SOW. In the Customer Portal, Customer's users can access multiple tools related to configuration management, availability management, performance management, service management (events, Incidents, and Service Requests), security management, and cost management. Customer will have unlimited 24x7 access to the Customer Portal throughout the Term of Customer's SOW. The Customer Portal is considered Syntax-Provided Software.