CyFlare Solution Terms

Effective February 9, 2024

The following solution-specific scope and terms ("Solution Terms") apply to Services purchased by the Customer ("Customer" or "you") in a signed quote or SOW. These Solution Terms are issued pursuant to the Master Service Agreement ("MSA") between the Customer and CyFlare Security Inc. ("CyFlare") and are subject to the terms and conditions specified below. Any term not otherwise defined herein shall have the meaning specified in the MSA.

General Assumptions

CyFlare's pricing, schedule, and scope of services are based on these assumptions:

- CyFlare will assign a **Customer Success Manager ("CSM")** who will be your focal point for the engagement.
- You will identify a **liaison** who will be CyFlare CSM's focal point (e.g., scheduling, documentation collection, status reporting, and issue resolution)
- You will share existing, relevant documentation with CyFlare (preferably in electronic formats)
- You will not share regulated data (e.g., PHI, PII, or CHD) with CyFlare unless it is necessary for the services CyFlare provides. If you expect CyFlare to encounter regulated data while working with you (e.g., during pen tests), you will inform CyFlare in advance. CyFlare will protect the non-public information you share with it.
- You will provide remote access to networks, systems, and documentation to CyFlare to perform its services.
- XDR per-user licensing assumes an asset ceiling of three times the licensed user count. For example, if 10 XDR users are licensed, a maximum asset count of 30 will be expected. Assets are considered IP addresses are seen by our XDR platform. CyFlare reserves the right to shape service or adjust license counts if the maximum threshold is consistently surpassed for three consecutive months.

Change Management

We will follow this process if either party needs to make a change to CyFlare's Services:

- CyFlare will create a written Change Request (CR), including a change description, rationale, and impact.
- CyFlare will review the CR with your liaison. We may mutually agree to investigate the CR further to determine the impact on the Service price and schedule.
- After further investigation, CyFlare will update the CR documentation.
- We may mutually agree to reject or execute the CR. However, both parties must sign the CR for it to be considered executed.

Acceptance and Authorization

- These Solution Terms are subject to the terms and conditions of the separately executed Master Services Agreement (the "MSA").

CyFlare Security Inc.
21 Goodway Drive, Suite A4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

Scope of Services

CyFlare shall provide the following:

CyFlare ONE XDR Complete and Initiate

1. Provide a named Customer Success Manager (CSM) to you
2. Provide a named Systems Engineer (SE) to you
3. Provide you and your Customer's access to CyFlare ONE Platform
4. Execute on end customer-specific Incident Response plan as created in the ONE platform by you.
5. Monitoring of Customer-deployed tenants, sensors, connectors, and log senders
6. Review initial events received and work with the Customer to tune the solution using a Customer-supplied context builder
7. Monitor, investigate, and provide cases to Customers per the subscribed Service Level Agreement (24/7/365 monitoring based on XDR default CyFlare aligned detections)
8. NOTE: Custom rules or Customer-created alerts that do not have an MITRE ATT&CK Framework ID may be subject to professional service fees for developing IR playbooks for those custom rules
9. Join end-customer calls as requested in support of XDR platform tenants
10. Create filtering/exclusion rules required within the XDR platform
11. Implement correlation rules as needed and subject to limits stated within the CyFlare Service Level Agreement located at: https://www.cyflare.com/legal/.
12. For XDR Complete Only: Enable Network Traffic Analysis functionality with related security detections (when the network sensor is deployed)
13. For XDR Complete Only: Enable core CyFlare XDR Defined Automation use cases identified in Table 1 below

Table 1

Service	Use Cases		Common CyFlare Response Actions	Typical Integrations
mXDR	**Use Case 1**	**Firewall Policy Update:** Integration to make routine changes, such as adding an IP address to a blacklist or querying the whitelist.	• Write blacklist • Read the blacklist (to see if it already had been added) • Update geo-blocking from CKB (potential)	JUNIPER NETWORKS, Check Point SOFTWARE TECHNOLOGIES LTD., CISCO, paloalto NETWORKS, FORTINET
	Use Case 2	**Network Isolation:** Integrates with networking tools and platforms to isolate or remove a device from the network.	• Get/terminate sessions • Quarantine/unquarantine address • Add/remove IP to address set	SONICWALL, CLOUDFLARE, Cisco ISE, JUNIPER NETWORKS

CyFlare Security Inc.
21 Goodway Drive, Suite A4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

	Use Case 3	**Disable/Enable User Account**: This response action is invoked when there is a high probability the account or device has been compromised. To safeguard against account takeover and additional compromise, a user account can be disabled until properly investigated	• Enable User Account • Lock User Account (permanently or for X amount of time)	The threat stops here. okta Google Cloud IAM Active Directory G Suite CYBERARK
	Use Case 4	**Email Integration:** Integrate to recall confirmed or potential phishing emails from mailboxes to minimize the risk of interacting with malicious URLs	• Quarantine email from mailbox(es)	mimecast TREND MICRO Office 365 Symantec

CyFlare ONE XDR Connect

1. Provide a named Customer Success Manager (CSM) to you
2. Provide a named Systems Engineer (SE) to you
3. Provide you and your customers access to CyFlare ONE Platform
4. Support the SIEMs defined in ***Table 2 (see next page)*** for monitoring and response actions via API Integration
5. Schedule regular integration sessions as needed for the first 30 days
6. Execute on end customer-specific Incident Response plan as created in the ONE platform by you
7. Regular Monitoring of API Connector status
8. Review initial events received and work with the Customer to tune the solution using a CUSTOMER-supplied context builder.
9. Monitor, investigate, and provide cases to customers per the subscribed Service Level Agreement (24/7/365 monitoring).
    1. NOTE: Custom rules or Customer-created alerts that do not have an MITRE ATT&CK Framework ID may be subject to professional service fees for developing IR playbooks for those custom rules.
10. Join end-customer calls as requested.
11. Consult only on creating filtering/exclusion rules required within the SIEM platform
12. Consult only on implementing correlation rules as needed

CyFlare Security Inc.
21 Goodway Drive, Suite A4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

13. If leveraging a Customer-provided SIEM solution, CyFlare will process all detections that are tagged with a MITRE ID.
    a) Detections sourced without a MITRE ID will be processed and visualized within the CyFlare ONE Platform.

Table 2

SIEM Vendor	Response Actions Available	Ingest Detections
Stellar Cyber	Yes	Yes
AlienVault	Yes	Yes
Rapid7 InsightIDR	Yes	Yes
Arcsight	Yes	Yes
Devo	Yes	Yes
Elastic	Yes	Yes
FireEye Helix	Yes	Yes
Fortinet FortiSIEM	Yes	Yes
Google Chronicle	Yes	Yes
LogPoint	Yes	Yes
LogRhythm	Yes	Yes
Logzio	Yes	Yes
McAfeeESM	Yes	Yes
Microsoft Azure Sentinel	Yes	Yes
QRadar	Yes	Yes
RSA NetWitness	Yes	Yes
Splunk	Yes	Yes
Sumologic	Yes	Yes
Symantec ICDX	Yes	Yes
Vectra	Yes	Yes
Humio	Yes	Yes
Nozomo Networks	Yes	Yes

Table 3

Feature / Benefit	mXDR Connect	mXDR Initiate	mXDR Complete
Onboarding and Deployment Assistance	ü	ü	ü
Unlimited Incident Response	ü	ü	ü
24x7 SOC Monitoring	ü	ü	ü
XDR / SIEM Platform	BYO	ü	ü
Advanced SLA	ü	ü	ü
CyFlare ONE Platform	ü	ü	ü
97% True Positive Rate Target	ü	ü	ü
UEBA, Machine Learning Detection Engines	BYO	ü	ü
Threat Containment & Response Automation	ü	-	ü
Log Storage Retention	-	90 Day Standard Optional 12 months Extended Log Retention	90 Day Standard Optional 12 months Extended Log Retention
Network Traffic Analysis / Network Detection & Response	-	-	ü

CyFlare ONE MDR Complete

1. Provide a named Customer Success Manager (CSM) to you
2. Provide a named Systems Engineer (SE) to you
3. Provide you and your Customer's access to CyFlare ONE Platform
4. Deliver and operationalize end customer-specific Incident Response plan to determine contact procedures and related conditions
5. Review initial events received and work with the Customer to tune the solution
6. Monitor, investigate, and provide cases to Customer or end customers per the subscribed Service Level Agreement (24/7/365 monitoring)
7. Join Customer calls as requested in support of end customers
8. Assist with Incident Response investigations that may require log searching and review to identify related events
9. Provide licensing for SentinelOne or Sophos EDR agents
10. Regularly manage/update agent versions as they become available
11. Enable core CyFlare MDR Defined Automation use cases identified in Table 4 below

CyFlare Security Inc.
21 Goodway Drive, Suite A4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

Table 4

Service	Use Cases		Common CyFlare Response Actions	Typical Integrations
mEDR	**Use Case 5**	**Scan/Remediate/Rollback Endpoint:** Step two after isolation. Scan action will be part of the next steps after isolating the endpoint. Remediate and rollback will be done after contacting the customer and confirming the threat.	• Initiate AV scan • Remediate (clean) threats • Rollback machine	Carbon Black. Symantec CROWDSTRIKE SentinelOne SOPHOS
	Use Case 6	**Isolate/Unisolate Endpoint:** EDR integration to take response action on the endpoint in the event of a confirmed or likely threat.	• Shut down the machine • Isolate from network • Connect to the network	Carbon Black. SOPHOS CROWDSTRIKE Symantec SentinelOne

Table 5

Feature / Benefit	mEDR Connect	mEDR Complete
Onboarding and Deployment Assistance	✓	✓
Advanced SLA	✓	✓
Unlimited Incident Response	✓	✓
24x7 SOC Monitoring	✓	✓
Automatic Threat Response & Containment	✓	✓
CyFlare ONE Platform	✓	✓
97% True Positive Rate Target	✓	✓
Included EDR Software License (SentinelOne or Sophos)	-	✓
Managed Agent Updates	-	✓
Policy Creation & Management	-	✓

CyFlare Security Inc.
21 Goodway Drive, Suite A4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

Table 6

EDR / AEP Platform Vendor	Response Actions Available	Ingest Detections
SentinelOne	Yes	Yes
Sophos	Yes	Yes
Crowdstrike Falcon	Yes	Yes
Bitdefender Gravity Zone	Yes	No
VmWare Carbon Black Cloud	Yes	Yes
VMWare Carbon Black Enterprise EDR	Yes	No
VMWare Carbon Black Endpoint Standard	Yes	No
Carbon Black Defense	Yes	No
Carbon Black Response	Yes	Yes
Carbon Black Protection	Yes	No
Cisco AMP	Yes	Yes
Cybereason	Yes	Yes
Cylance	Yes	Yes
Cynet	Yes	No
Endgame	Yes	Yes
Extrahop	No	Yes
FireEye HX	Yes	Yes
Google Rapid Response	Yes	No
Ivanti	Yes	No
McAfee Active Response	Yes	No
McAfee EPO	Yes	Yes
McAfee Mvision EDR	Yes	Yes
McAfee Mvision EPO	Yes	Yes
Microsoft 365 Defender	Yes	Yes
Microsoft Defender ATP	Yes	Yes
Microsoft Intune	Yes	No
Observe IT	No	Yes
Orca Security	Yes	Yes
Palo Alto Cortex XDR	Yes	Yes
Qualys EDR	No	Yes
RSA Witness EDR	Yes	No
Symantec Endpoint Protection	Yes	No
Trend Micro Security	Yes	No

CyFlare Security Inc.
21 Goodway Drive, Suite A4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

Armis	Yes	Yes
Azure Security Center	Yes	Yes
OpSWAT	Yes	No
ProofPoint TAP	Yes	No
Tanium	Yes	No

CyFlare ONE Cyber Risk Intelligence (CRI)

1) Provide a Customer Success Manager (CSM) to you
2) Provide a Systems Engineer (SE) to you
3) Provide you access to CyFlare ONE Platform
4) Provide vulnerability scanning strategy template and guidance
5) Assist in vulnerability scanning design and architecture creation
   a) Identify external scanning targets
   b) Identify in-scope network scan subnets
   c) Identify machines requiring deployed scanning agent
   d) Configure Customer-requested scan schedules
   e) Configure Customer-provided credentials where required to enable authenticated scans
6) Provide agent licensing
7) Configure automated reporting to email target
8) Alert Customer Incident Handler when dark web hits occur
9) Configure Azure AD integration using Customer-provided API credentials
10) Continuous monitoring of operational health checks that include:
    a) Scan job completion
    b) Expired credentials
11) Regularly update agents as they become generally available

Table 7

Feature / Benefit	**Cyber Risk Intelligence (CRI)**
Vulnerability Scanning Strategy Development	✓
Scanning Architecture Development	✓
Configure Scanning Jobs	✓
Continuous Health Checks	✓
Internal / External Vulnerability Scanning	✓
Web Application Scanning	✓
Dark Web Monitoring & Alerting	✓
Active Directory Insights	✓

Ongoing Configuration Management	✓
Root Cause Analysis in UI	✓
Operational Dashboard (Coverage)	✓

Service Deliverables

CyFlare shall provide the following:

1. Supporting documentation outlining all required items related to appropriate services to be deployed
2. If applicable, access to the XDR management platform
3. Access to CyFlare ticketing platform
4. If applicable, access to the endpoint cloud management portal
5. Deployment audit document after 60 days of initial client engagement
6. If applicable, Curated playbooks based on CyFlare SIEM security detections (see https://desk.cyflare.cloud/portal/en/kb/articles/breach-detection-ser)
7. If applicable, provide a vulnerability scanning report generated by the scanning platform via email
8. 24/7/365 monitoring of security alarms leveraging default and curated playbooks
9. 24/7/365 support for all security incidents from CyFlare security analyst based on an incident response plan (to the extent the purchased platforms can provide)
10. Full security incident report in the event of a confirmed compromise within the environment (to the extent the purchased platforms can provide)
11. Monthly review of client ticketing summary report

CyFlare Responsibilities

1. Provide a designated Customer Success Manager (CSM)
2. Provide a designated Deployment Engineer (DE)
3. Provide access to CyFlare's secure ticketing portal
4. Schedule regular deployment sessions as needed for the first 30 days
5. A deployment audit summary at the end of the first 60 days
6. Deliver and operationalize a Customer-specific Incident Response plan to determine contact procedures and related conditions
7. If applicable, deploy the XDR solution in support of the defined scope of work
8. Monitoring of deployed appliance(s) to ensure services are functional
9. Review initial events received and work with the Customer to tune the XDR solution using Customer supplied context builder
10. If applicable, review, evaluate, and accommodate five custom requests per month from the Customer for new content. New content includes new curated security detections, dashboards, reports, or changes outside the default out-of-box security solutions offerings & standard processes. **Note**: all requests are subject to CyFlare approval or denial based on the internal evaluation. Any new content request requiring over 5 hours of development & implementation time may be subject to a flat fee.
11. If applicable, provide endpoint agent and token to Customer

12. If applicable, the configuration of the vulnerability scanning tool in accordance with recommended best practices of the platform (provide installation agent to Customer if applicable)
13. Monitor, investigate, and provide tickets to Customer based on the Service Level Agreement ("SLA") level subscribed to by Customer (24/7/365 monitoring based on XDR default CyFlare aligned detections) . CyFlare SLAs: https://cyflare.com/wp-content/uploads/SOC-Support-and-SLA-Overview-REV04_1023_FINAL.pdf

14. For applicable service offerings, fulfill up to 5 change requests per month per Customer. Change requests include:
    a. ATH Rule creation/modifications
    b. Rule filters
    c. Reporting requests
    d. Configuration changes
    e. Playbook modifications
15. Monthly or quarterly security briefing call to review the SOC ticketing report

Customer Responsibilities

1. The Customer will participate in scheduled deployment calls with the provided Customer Success Manager (CSM) and Deployment Engineer (DE)
2. The Customer will work with the CSM to populate the SOC Survey document that adds context to the Customer environment and integrates the SOC.
3. The Customer will provide IP/Subnet/Gateway/DNS information for each XDR appliance purchased
4. The Customer is responsible for the physical installation of the purchased XDR appliance.
5. The Customer is responsible for all physical network cabling and providing power in accordance with appliance specifications. CyFlare is NOT responsible for any physical network cabling or additional environmental items at the Customer's location.
6. Customer responsible for all network configurations as required by the XDR Quick Start Guide (QSG) located here: https://desk.cyflare.cloud/portal/kb/articles/cyflare-soc-in-a-box-quick-start-guide
7. The Customer will manage the software installation of the supplied XDR Windows/Linux server agent(s)
8. The Customer will only install supplied Windows/Linux server agent(s) on identified servers (Not end workstations)
9. The Customer will only install the number of XDR Windows/Linux server agents identified and mutually agreed upon in writing.
10. The Customer will configure Syslog senders in accordance with the number of XDR senders identified and mutually agreed upon in writing.
11. The Customer will provide API authentication tokens as needed for various integrations.
12. The Customer will list existing vendor exclusions or whitelisted items used within the current endpoint security solution.
13. The Customer will provide identification of servers, workstations, and laptops within the scope for Sentinel One deployment.
14. The Customer will identify sensitive endpoints involved in deployment that are mission-critical to business workflows to ensure proper Sentinel One installations.
15. The Customer will manage the software installation of supplied Sentinel One software agents and tokens.

16. The Customer will ensure vulnerability scanning tool requirements identified and mutually agreed upon in writing are satisfied.
17. The Customer will ensure target systems within the scope of work have the necessary connectivity from the vulnerability scanning tool to perform scans.
18. The Customer will ensure that the agreed upon vulnerability scanning timeframe is communicated to the organization to limit potential issues to production workflow.
19. The Customer will provide current email system configurations related to transport rules and other system integrations that alter normal mail flow.
20. Configuration related to all DNS changes to Customer domains is the Customer's responsibility. If 3rd party vendors are involved with the required changes, the Customer must coordinate. CyFlare is not responsible for interactions with entities other than the Customer.
21. The Customer will participate and respond to CyFlare security tickets within ten days. After ten days, tickets within the CyFlare ticketing platform will auto-close without approval.