CyFlare Solution Terms

Effective October 2022

The following solution-specific scope and terms ("Solution Terms") apply to Services purchased by the Customer ("Customer" or "you") in a signed quote. These Solution Terms are issued pursuant to the Master Service Agreement ("MSA") between the Customer and CyFlare LLC ("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

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, LLC
21 Goodway Drive, Suite L4
Rochester, NY 14623

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

Scope of Services

CyFlare shall provide the following:

XDR as a Service (XDRaaS)

1. Ship any ordered appliances to Customer identified location(s)
2. Create tenant(s) within the XDR management platform
3. Create users within the XDR management platform for Customer access to Customer tenant environment
4. Provide XDR Windows/Linux server software agents to Customer
5. Provide an example of XDR software agent installation to Windows and/or Linux server
6. Walkthrough of single CyFlare XDR appliance installation
7. Provide documentation for XDR Syslog ingestion (vendor/port numbers)
8. Provide XDR API integration documentation for XDR API integrations
9. Provide API integration configuration within the XDR management platform
10. Ensure log data is seen within the management platform for installed XDR sensors
11. Deployment Bill of Materials shall be mutually agreed upon in writing by Customer and CyFlare before the start of implementation
12. In-scope XDR Integrations for an implementation shall be mutually agreed upon in writing by Customer and CyFlare before the start of implementation
13. CyFlare quote signed by the Customer outlines the maximum utilization of XDR. Any utilization overages for XDR shall be billed by CyFlare the following month

Managed Endpoint

1. Configure cloud management portal for Customer environment
2. Enable access to users designated by Customer to the management portal
3. Review endpoint configuration and organization setup methodology
4. Provide installation agent and token to Customer for agent deployment
5. CyFlare quote signed by the Customer outlines licensed endpoints purchased for this deployment. Any license overages shall be billed by CyFlare the following month at the agreed-upon rate specified within the quotation
6. Review and provide an example of the installation process for the endpoint agent
7. Provide best practice guidance for deployment according to Customer environment
8. Configure security policies within the cloud management portal
9. Configure and maintain whitelists and blacklists for customer site within the management portal

Vulnerability Scanning

1. Configure, Run, and report on periodic vulnerability scans
    a. Configure and run vulnerability scans monthly
    b. Gather scan configuration requirements from the Customer during the Onboarding phase of the service

CyFlare, LLC
21 Goodway Drive, Suite L4
Rochester, NY 14623

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

c. Validate definitions are downloaded correctly and any scheduled scans have been completed successfully
d. Adjust scanning schedules, define new sites and their associated ranges, and change IP Ranges of sites as per Customer request.

2. Provide vulnerability scanning of Customer environment per the vulnerability scanning parameters agreed upon in writing by the Customer and CyFlare
3. Provide an explanation of the vulnerability scanning process to the Customer
4. Explain vulnerability scanning findings
5. Provide recommendations on how to remediate or mitigate vulnerabilities identified on target systems within the vulnerability scanning scope
6. CyFlare is not responsible for patch management of Customer infrastructure

Proofpoint Essentials

1. Configure Customer company within the Proofpoint Essentials management portal
2. Configure and validate Customer domains that receive Customer emails within the Proofpoint Essentials platform
3. Create configuration within the Proofpoint Essentials platform to connect to the Customer email system
4. Ingest Customer users into the Proofpoint Essentials platform leveraging API integration
5. The Customer will decide on default user type ingestion (Silent User or End User)
6. Configure SPAM settings within the Proofpoint Essentials platform
7. Configure URL Defense functionality within the Proofpoint Essentials platform
8. Review other Proofpoint Essentials configuration options such as email encryption, inbound/outbound filter policies, digest frequency, and email disclaimers. Implement these features within the Proofpoint Essentials platform based on Customer feedback
9. CyFlare is not responsible for advising or modifying any related systems, including DNS, related mail systems, certificate services, or any 3rd party not explicitly identified within the quotation. Proofpoint support will be required to support all 3rd party integrations or dependencies

ZTEdge Platform

1. Configure cloud management portal for Customer environment
2. Enable access to users designated by Customer to the management portal
3. Review configuration and policy requirements
4. Provide installation agent and to Customer for agent deployment or direction for PAC file deployment method if required
5. CyFlare quote signed by the Customer outlines licensed users purchased for this deployment. Any license overages shall be billed by CyFlare the following month
6. Review and provide an example of the installation process for the endpoint agent
7. Provide best practice guidance for deployment according to Customer environment
8. Configure security policies within the cloud management portal according to client requirements, limited by the platform capabilities

9. Configure and maintain whitelist and blacklists for customer site within the management portal

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. If applicable, access to the Proofpoint Essentials cloud management portal
6. Deployment audit document after 60 days of initial client engagement
7. If applicable, Curated playbooks based on CyFlare SIEM security detections (see https://desk.cyflare.cloud/portal/en/kb/articles/breach-detection-ser)
8. If applicable, provide a vulnerability scanning report generated by the scanning platform via email
9. 24/7/365 monitoring of security alarms leveraging default and curated playbooks
10. 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)
11. Full security incident report in the event of a confirmed compromise within the environment (to the extent the purchased platforms can provide)
12. 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 a total of 5 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

CyFlare, LLC
21 Goodway Drive, Suite L4
Rochester, NY 14623

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

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. All configurations related to the Proofpoint Essentials admin console for the deployment of service
14. 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://www.cyflare.com/wp-content/uploads/2021/04/CyFlare-SOC_SLA_SLO-Datasheet-REV03-1021-1.pdf
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 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 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 provide a list of 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 provide identifications of 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 that are within the scope of work have the necessary connectivity from the vulnerability scanning tool to perform scans
18. The Customer will ensure agreed upon vulnerability scanning timeframe is communicated to the organization to limit potential issues to production workflow

CyFlare, LLC
21 Goodway Drive, Suite L4
Rochester, NY 14623

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

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 any interactions with other entities other than the Customer
21. Configuration of the current email platform to integrate with the Proofpoint Essentials email service. This may include but is not limited to API key generations, email rule creation, additional user creations, and mail flow connectors
22. Notification to end users prior to email cutover to Proofpoint Essentials service. This ensures understanding of a change in workflow with Customer email service
23. 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

CyFlare, LLC
21 Goodway Drive, Suite L4
Rochester, NY 14623

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