CYFLARE
Where cyber becomes clear.

Cyflare End Customer Solution Terms

Effective: September 1, 2026

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

General Assumptions

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

- Cyflare provides multiple support resources to assist with your services. A Customer Success Manager ("CSM") may be assigned as a primary point of contact; however, customers and partners without a named CSM can still access support through Cyflare's standard engagement channels, including email at customersuccess@Cyflare.com and other published contact methods.
- You [Customer] will identify a **liaison** who will be Cyflare's focal point of contact (e.g., scheduling, documentation collection, status reporting, and issue resolution)
- You [Customer] will share existing, relevant documentation with Cyflare (preferably in electronic formats)
- You [Customer] will not share sensitive or regulated data (e.g., PHI, PII, CUI, or CHD) with Cyflare unless mutually agreed upon and to the extent 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 [Customer] 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 to be considered executed.

Cyflare Security Inc.
950A Union Road, Suite 103
West Seneca, NY 14224

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

General Service Deliverables

Cyflare shall provide the following:

- Supporting documentation outlining all required items related to services to be deployed or delivered
- If applicable, provide access to the source XDR, VSS, Email, and EDR management platforms
- Access to Cyflare ONE
- 24/7/365 monitoring of security alarms, leveraging default and curated detections and playbooks for in-scope services
- 24/7/365 support for all security incidents from a Cyflare security analyst based on an incident response plan (to the extent the purchased platforms can provide)
- Full security incident report in the event of a confirmed compromise within the environment (to the extent the purchased platforms can provide)
- Monitoring the in-scope technical appliance(s) to ensure platforms are functional.
- Monitor, investigate, and provide tickets to the Customer based on the Service Level Agreement ("SLA") level subscribed to by Customer. Cyflare SLAs can be found at https://www.Cyflare.com/legal
- For applicable service offerings, support up to 5 change requests per month per Customer. Change requests include:
    - ATH Rule creation/modifications
    - Rule filters
    - Reporting requests
    - Configuration changes
    - Playbook modifications
- Monthly or quarterly milestone call to review the service delivery outcomes with Cyflare's customer success team

Cyflare Onboarding Responsibilities

Cyflare shall provide the following:

- Provide a designated Deployment Engineer (DE) and Project Manager (PM) to support technical tasks and track logistical tasks, respectively, associated with customer onboarding
    - MSP Partners will be expected to perform technical onboarding and project management activities without Cyflare's assigned resources
    - Cyflare will provide MSP Partners with Cyflare Certified Deployment Engineer (CCDE) training, ensuring they possess the necessary onboarding skills and knowledge to successfully onboard their sub-customers
- Provide access to Cyflare's Project Plan to track onboarding tasks and status
- Schedule regular deployment sessions for project tasks to be completed
- Operationalize and train the Customer on Incident Response plan settings to determine contact procedures for related service escalations
- Deploy the in-scope technical solutions defined by the quote and/or SOW

- Provide applicable service-related endpoint agent(s) and token(s) to Customer for deployment and/or configuration tasks
- Provide customers with a completed project plan upon onboarding task completion

Customer Responsibilities

Customer shall provide the following:

- The Customer will participate in scheduled onboarding calls with the provided Project Manager and Deployment Engineer (DE)
- The Customer will work with the onboarding team to populate the customer knowledgebase document that adds context to the Customer environment and integrates with service delivery teams
- The Customer will provide IP/Subnet/Gateway/DNS information for each appliance purchased
- The Customer is responsible for the physical installation of the purchased appliances
- 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
- Customer responsible for all network configurations as required by the vendor for each technical solution being installed. Cyflare will provide details for each platform during the onboarding.
- When applicable, the Customer will manage the operating system software installation of the supplied Windows/Linux server agent(s)
- When applicable, the Customer will only install supplied Windows/Linux server agent(s) on identified servers (Not end workstations)
- When applicable, the Customer will only install the number of Windows/Linux server agents identified and mutually agreed upon in writing.
- When applicable, the Customer will configure Syslog senders in accordance with the number of senders identified and mutually agreed upon in writing.
- When applicable, the Customer will provide API authentication tokens as needed for various integrations.
- When applicable, the Customer will list existing vendor exclusions or whitelisted items used within the current endpoint security solution.
- When applicable, the Customer will provide identification of servers, workstations, and laptops within scope for Sentinel One deployment.
- When applicable, the Customer will identify sensitive endpoints involved in deployment that are mission-critical to business workflows to ensure proper EDR and/or endpoint installations.
- When applicable, the Customer will manage the software installation of supplied EDR and/or endpoint software agents and tokens.
- When applicable, the Customer will ensure that vulnerability scanning tool requirements identified and mutually agreed upon in writing are satisfied.
- When applicable, the Customer will ensure target systems within the scope of work have the necessary connectivity from the vulnerability scanning tool to perform scans.

- When applicable, the Customer will ensure that the agreed-upon vulnerability scanning timeframe is communicated to the organization to minimize potential issues affecting the production workflow.
- When applicable, the Customer will provide current email system configurations, including transport rules and other system integrations that alter normal mail flow.
- Configuration related to all DNS changes to Customer domains is the Customer's responsibility. If third-party vendors are involved in the required changes, the Customer must coordinate. Cyflare is not responsible for interactions with entities other than the Customer.
- The Customer will participate and respond to Cyflare security tickets within fourteen days. After fourteen days, tickets within the Cyflare ticketing platform will auto-close without approval. Cyflare will administer the final disposition status based on the case details on a best-effort basis.
- Incident Response Call Tree Responsibility:
    - Customer is solely responsible for configuring, maintaining, and keeping current the Incident Response call tree and escalation contacts within the Cyflare ONE platform.
    - Cyflare is not responsible for failed, delayed, or missed incident notifications resulting from incomplete, inaccurate, or outdated call tree information.
    - Failure to maintain the Incident Response call tree may result in Cyflare being unable to initiate escalation communications.
- Customer Configuration Changes:
    - If Customer personnel are provisioned with any role or permission that allows modification of detection logic, security policies, scan schedules, response automation, logging sources, or other platform configurations across any Cyflare-managed solution, Customer shall submit a ticket to Cyflare **before** applying such changes.
    - Cyflare will not be responsible for missed detections, scan or policy failures, service interruptions, or degraded security posture resulting from Customer-driven changes, whether disclosed to Cyflare or not.

Customer Administrative Access and Platform Changes

Cyflare may provide Customer with administrative or privileged access to certain platforms, security tools, or software environments that are hosted, licensed, or managed by Cyflare as part of the Services.

Customer acknowledges that administrative access may allow Customer personnel to enable features, modules, integrations, logging sources, security controls, or other platform capabilities that may increase vendor licensing tiers, platform consumption, storage requirements, or Cyflare service scope.

Any configuration changes, feature enablement, or platform modifications initiated by Customer personnel that result in additional vendor licensing costs, increased platform consumption, activation of paid modules, or expanded service scope will be billable to Customer, regardless of whether such changes were made intentionally or inadvertently.

Cyflare is not responsible for monitoring or preventing Customer-initiated configuration changes that impact licensing or consumption levels. Customer remains responsible for all costs resulting from administrative actions taken within the platforms to which Customer has been granted access.

Where reasonably practicable, Cyflare will notify Customer of material changes to platform licensing or service scope resulting from Customer configuration changes. However, the absence of such notification does not waive Customer's responsibility for associated costs.

Scope of Individual Services

Cyflare shall provide the following for each respective in-scope services:

Cyflare mXDR Initiate, Complete (Including O365 which is no longer a valid SKU)

- Execute an end customer-specific Incident Response plan as created in the ONE platform for escalations
- Monitoring of Customer-deployed tenants, sensors, connectors, and log senders
- MXDR O365 Only: Microsoft 365 and Azure AD / EntraID monitoring only included
- Review initial events received and work with the Customer to tune the solution using Customer-supplied context
- Customers are expected to share tuning requests with Cyflare when an unwanted escalation is received by opening a new case
- Cyflare will share the global curated detections with customers within the Cyflare ONE platform.
- The list is updated periodically by Cyflare and can be found in the 'resources' button in ONE platform.
- Monitor, investigate, and provide cases to Customers per the subscribed Service Level Agreement (24/7/365 monitoring based on XDR default Cyflare aligned detections).
- 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
- mXDR per-user licensing assumes an ingest ceiling of 60 megabytes/day, multiplied by the licensed user count.
    - For example, if 10 XDR users are licensed, a maximum ingestion of 600 mb/day will be expected. Cyflare reserves the right, with the Customer's express consent, to adjust service or license counts if the maximum threshold is exceeded.
- Join end-customer calls as requested in support of XDR platform tenants
- Optional: Enable SOC Automated Response Use-Case (See Table 7)
  Create filtering/exclusion rules required within the XDR platform
- Implement correlation rules as needed and subject to limits stated within the Cyflare Service Level Agreement located at: https://www.Cyflare.com/legal/.
- For mXDR Complete Only: Enable Network Traffic Analysis functionality with related security detections (when the network sensor is deployed)
- Review initial events received and work with the Customer to tune the XDR solution using the Customer-supplied context builder

- If applicable, review, evaluate, and support up to 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-the-box security solutions offerings & standard processes.
    - **Note**: all requests are subject to Cyflare approval or denial based on Cyflare's internal evaluation. Any new content request requiring over 5 hours of development & implementation time may be subject to a flat fee.

Cyflare mXDR Connect

- Support the SIEMs defined in Table 1 for monitoring and response actions via API Integration.
- Schedule regular integration sessions as needed during the onboarding process.
- Execute on the end customer-specific Incident Response plan as created in the ONE platform by the Customer
- Regular Monitoring of API Connector status
- Review initial events received and work with the Customer to tune the solution using a Customer-supplied context
    - Customers are expected to share tuning requests with Cyflare when an unwanted escalation is received by opening a new case
- Monitor, investigate, and provide cases to customers per the subscribed Service Level Agreement (24/7/365 monitoring).
    - **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.
    - **Note**: Endpoint and/or EDR-specific detections will require XDR correlation detections to be monitored and responded to. Cyflare requires the Customer to purchase mEDR-Connect to process EDR-based detections on a 1:1 basis.
- Join end-customer calls as requested.
- Consult only on creating filtering/exclusion rules required within the SIEM platform
- Consult only on implementing correlation rules as needed
- If leveraging a Customer-provided SIEM solution, Cyflare will process all detections that are tagged with a MITRE ID.
- Optional: Enable SOC Automated Response Use-Case (See Table 7)

CYFLARE
Where cyber becomes clear.

Table 1

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 2

Feature / Benefit	mXDR Connect	mXDR O365 (No Longer Available)	mXDR Initiate	mXDR Complete
Onboarding / Deployment Assistance	✓	✓	✓	✓
Unlimited IR Support by SOC	✓	✓	✓	✓
24x7 SOC Monitoring	✓	✓	✓	✓
XDR / SIEM Platform	BYO	✓	✓	✓
Advanced SLA	✓	✓	✓	✓
Cyflare ONE Platform	✓	✓	✓	✓
<1% False Positive Rate Target	✓	✓	✓	✓
UEBA, Machine Learning Detection Engines	BYO	✓	✓	✓

Cyflare Security Inc.
950A Union Road, Suite 103
West Seneca, NY 14224

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

Threat Containment & Response Automation	✓	-	-	✓
Log Storage Retention	-	30 Day Hot Searchable Optional: 12 Month Cold Extended Log Retention	30 Day Hot Searchable Optional: 12 Month Cold Extended Log Retention	30 Day Hot Searchable Optional: 12 Month Cold Extended Log Retention
Network Traffic Analysis / Network Detection & Response	-	-	-	✓

Note: Optional 12-Month Extended Log Retention refers to cold data retention, which archives security telemetry and log data for historical analysis and compliance purposes. Retrieval of archived data requires additional processing time and system rehydration. Cyflare must submit rehydration requests to the applicable XDR vendor, and all requests are subject to the vendor's processing times, technical capabilities, retrieval limits, and approval.

Rehydration timeframes may vary based on the volume and age of the data requested. The vendor may deny or limit requests that exceed its standard retrieval thresholds. Where the vendor permits Cyflare to exceed standard retrieval limits for an additional fee, Cyflare will notify the Customer in advance, and any such vendor charges will be passed through to the Customer upon the Customer's approval.

Cyflare Microsoft ITDR (MS-ITDR)

- Execute the end customer-specific Incident Response plan as created in the ONE platform by the Customer
- Review initial events received and work with the Customer to tune the solution using customer supplied context
- Customers are expected to share tuning requests with Cyflare when an unwanted escalation is received by opening a new case
- Monitor, investigate, and provide cases to Customer per the subscribed Service Level Agreement (24/7/365 monitoring)
- Cyflare MS-ITDR provides 24x7 monitoring, investigation, and response support for supported identity and Microsoft 365 security events generated from Customer-authorized Microsoft Entra ID and Microsoft 365 telemetry.
- Assist with Incident Response investigations that may require log searching and review to identify related events
- Cyflare will share globally curated detections with customers within the Cyflare ONE platform.

- The Cyflare ITDR Service monitors supported detections made available and enabled by Cyflare. Detection coverage may be added, modified, tuned, replaced, or removed as Microsoft services, available telemetry, threat techniques, Cyflare detection logic, and underlying technologies evolve.
- Access to the underlying detection platform will not be accessible to customers or partners.
- The list is updated periodically by Cyflare and can be found in the 'resources' button on the ONE platform.
- Cyflare ITDR per-user licensing assumes the following formula for 'Core Users'.
    - Core Users = Total Users – Disabled Accounts – Guest Accounts.

Note: The Microsoft ITDR Service does not guarantee that every unauthorized action, compromised identity, malicious application, security event, or cyberattack will be prevented or detected. Service performance depends upon the availability, completeness, accuracy, configuration, licensing, and timely transmission of Customer-authorized Microsoft Entra ID and Microsoft 365 telemetry.

Table 3

Feature / Benefit	**Cyflare MS ITDR**
Onboarding / Deployment Assistance	✓
Unlimited IR Support by SOC	✓
24x7 SOC Monitoring	✓
Cyflare ITDR Detection Platform	✓
Advanced SLA	✓
Threat Containment & Response Automation (As Requested)	✓
Log Storage Retention	Default: 365 Day Cold Storage Optional: Additional Annual increments of Cold Data Retention for additional fees

Cyflare mEDR Connect & Complete

- Execute the end customer-specific Incident Response plan as created in the ONE platform by the Customer
- Review initial events received and work with the Customer to tune the solution using a Customer-supplied context
- Customers are expected to share tuning requests with Cyflare when an unwanted escalation is received by opening a new case
- Monitor, investigate, and provide cases to Customer per the subscribed Service Level Agreement (24/7/365 monitoring)
- Join Customer calls as requested in support of end customers
- Assist with Incident Response investigations that may require log searching and review to identify related events
- mEDR Complete Only: Provide licensing for CrowdStrike or SentinelOne agents
- mEDR Complete Only: Regularly manage/update agent versions as they become available
- Optional: Enable SOC Automated Response Use-Case (See Table 7)

Table 4

Feature / Benefit	mEDR Connect	mEDR Complete
Onboarding and Deployment Assistance	✓	✓
Advanced SLA	✓	✓
Unlimited Incident Response	✓	✓
EDR Platform	BYO	✓
24x7 SOC Monitoring	✓	✓
Automatic Threat Response & Containment	✓	✓
Cyflare ONE Platform	✓	✓
<1% False Positive Rate Target	✓	✓
Managed Agent Updates	-	✓
Policy Creation & Management	-	✓
EDR Platform Data Retention (SentinelOne)	-	90 Days (Hot Data)

Table 5

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
Armis	Yes	Yes
Azure Security Center	Yes	Yes

Cyflare Security Inc.
950A Union Road, Suite 103
West Seneca, NY 14224

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

OpSWAT	Yes	No
ProofPoint TAP	Yes	No
Tanium	Yes	No

Cyflare Vulnerability Scanning Services (VSS) Lite & Enhanced

Previously Cyber Risk Intelligence (CRI)

- Provide vulnerability scanning solution including recommended scan templates and guidance
- Assist in vulnerability scanning design and architecture creation
    - Identify external scanning targets
    - Identify in-scope network scan subnets
    - Identify machines requiring deployed scanning agent
    - Configure Customer-requested scan schedules
    - Configure Customer-provided credentials where required to enable authenticated scans
- Provide agent licensing
- Configure automated reporting to email target
- VSS Lite Only: Alert Customer Incident Handler when dark web hits occur
- Configure Azure AD integration using Customer-provided API credentials
- Continuous monitoring of operational health checks that include:
    - Scan job completion
    - Expired credentials
- Regularly update agents as they become generally available
- If applicable, provide a vulnerability scanning report generated by the scanning platform via email
- 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)
- VSS Enhanced Only:
    - Provide SOC monitoring and analysis for non-remediated critical and high-severity vulnerabilities identified by the vulnerability scanning solution
    - Optional: Enable SOC Automated Response Use-Case (See Table 7)

Table 6

Feature / Benefit	VSS Lite	VSS Enhanced
Vulnerability Scanning Strategy Development	✓	✓
Scanning Architecture Development	✓	✓
Configure Scanning Jobs	✓	✓
Continuous Health Checks	✓	✓
Internal/External Vulnerability Scanning	✓	✓
Dark Web Monitoring & Alerting	✓	-
Active Directory Insights	✓	-
Ongoing Configuration Management	✓	✓
Operational Dashboard (Coverage)	✓	✓
Patching w/ Virtual Patch Technology	-	✓
Cyflare mXDR Integration (Insights)	-	✓

Cyflare Managed Email Security (mES)

- Provide email security solution and licensing
- Integrate email security tenant with customer environment leveraging API
- Provide customer access to email security platform
- Configure email security settings and controls within platform using vendor best practices
- Monitor, investigate, and provide cases to Customer per the subscribed Service Level Agreement (24/7/365 monitoring)
    - Join Customer calls as requested in support of Cyflare provided email platform
    - Assist with Incident Response investigations that may require email platform query and review of related events
    - Configure email security reporting analytics as requested by Customer
    - Optional: Enable SOC Automated Response Use-Case (See Table 7)

Table 7

Feature / Benefit	mES Basic	mES Advanced	mES Complete
Secure All Email (Inbound, Outbound, Internal)	✓	✓	✓
Advanced AI-Based Anti-Phishing	✓	✓	✓
Anti-Spam Filtering	✓	✓	✓
Known Malware Prevention	✓	✓	✓
Protection from Zero-Day Malware (File Sandboxing)	-	✓	✓
File Sanitization (CDR)	-	✓	✓
Malicious URL Protection	✓	✓	✓
URL Click-time Protection	✓	✓	✓
Zero-Day Malicious URL Protection	-	✓	✓
Account Takeover Protection	✓	✓	✓
Unauthorized App Detection	✓	✓	✓
Data Loss Prevention	-	-	✓
Encryption	-	-	✓

Cyflare Security Inc.
950A Union Road, Suite 103
West Seneca, NY 14224

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

CYFLARE
Where cyber becomes clear.

Cyflare Automated Response Use-Cases

The following use cases (Table 7) are available for the applicable SOC-related services listed above. Customers may enable any of the following automatic actions as they see fit. Customers must provide written authorization/approval for Cyflare to perform actions. Customers can work with Cyflare to customize actions for specific events. Cyflare will require a case to be opened to enable automatic use case functions.

Table 8

Use Case	Use Case Description	Common CyFlare Response Actions	Typical Integrations
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 already been added) • Update geo-blocking from CKB (potential)	cisco, Juniper Networks, Fortinet, Check Point, paloalto
2	**Automated System Notification** Sends critical security alerts directly to communication channels, enabling faster response times and direct access to our ticketing system for streamlined incident resolution.	• Critical Escalations to Slack/Teams/SMS/Etc. • Curate Custom Notifications on Detections (Volume, Severity, Timeframe, Etc..) • Be Informed Instantly when Automation Response Occurs	slack, xmatters, Microsoft Teams
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)	CYBERARK, Active Directory, okta, G Suite
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, Harmony, Office 365, proofpoint, Symantec
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, SOPHOS, CROWDSTRIKE, SentinelOne
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., Symantec, SOPHOS, CROWDSTRIKE, SentinelOne

Cyflare Security Inc.
950A Union Road, Suite 103
West Seneca, NY 14224

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