Attachment A

13430 Northwest Freeway, Suite 1000
Houston, TX 77040
Phone 866.609.PATH

Number	Q-10579
Date	1/10/2025
Agreement Term	36 Months

Client

Ridgeview Schools CUSD #19
300 S Harrison
Colfax, IL 61728
United States

Phone 3097235111
Email **eyoung@ridgeview19.org**

Ship To

Ridgeview Schools CUSD #19
300 S Harrison
Colfax, IL 61728
United States

Phone 3097235111
FAX (309) 723-2019

DYOPATH Contact	Phone Number	Fax	Email
Connor Sweeney	(713) 485-7148		connor.sweeney@dyopath.com

The fees contained in this Attachment A are valid for 30 days from the Date referenced above and are subject to change thereafter.

Advanced Security Services (Monthly Recurring)

Description	Quantity	Unit-Price	Extended Price
DYOGUARD Protect Pro	1	$0.00	$0.00
360 Platform Access	119	$12.61	$1,500.00
Physical Log Ingestion aka: IDS Device or Network Traffic Analyzer (NTA)	1	$150.00	$150.00
DYOGUARD Agent	119	$0.76	$90.44
SOC Service	119	$3.76	$447.44
Cybereason License	119	$3.76	$447.44
DYOGUARD Integration Marketplace	1	$225.00	$225.00
Check Point Harmony Complete (Email Only)	200	$6.30	$1,260.00
Security Analyst 2	7	$200.00	$1,400.00
Symbol Tenant Management	1	$150.00	$150.00
Symbol Security PRO - Security Awareness Training	200	$3.48	$696.00
	Subtotal		**$6,366.32**

Managed Services (Monthly Recurring)

Description	Quantity	Unit-Price	Extended Price
Ticket Ingestion	4	$32.00	$128.00
	Subtotal		**$128.00**

Managed Services (Non-Recurring)

Description	Quantity	Unit-Price	Extended Price
Ticket Ingestion -Onboarding	16	$170.00	$2,720.00
	Subtotal		**$2,720.00**

Professional Service (Non-Recurring)

Description	Quantity	Unit-Price	Extended Price
Senior Engineer Business Hours	1	$188.00	$188.00
Security Analyst 1	7	$100.00	$700.00
Security Advisor	1	$280.00	$280.00
Project Management Hours - T&M Estimate	17	$170.00	$2,890.00
	Subtotal		**$4,058.00**

Service Definitions	
DYOGUARD Protect Pro	In an era where digital threats loom large and organizational resilience is paramount, DYOGUARD is a comprehensive suite of services designed to safeguard your digital assets while empowering executive decision-making. At the core of DYOGUARD ProtectPro is our "all in one" SOC Portal, a single pane of glass where all security operations reside, including dashboards to manage vulnerabilities, potential dark web threats, reporting, tickets, and incidents among many other functions. A fully transparent, co-managed security platform designed to bolster and inform your overall Cybersecurity Program, the SOC Portal aggregates and retains logs, enriches alerting with up-to-date threat intelligence, performs Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) functions. The DYOGUARD Managed Detection & Response (MDR) service offers proactive threat hunting, continuous monitoring to fortify your defenses against evolving cyber threats, and rapid incident response. Complementing our MDR platform is our Managed Email Security (MES) service, delivering robust protection against email-borne threats, ensuring the integrity of your primary communication channels. With DYOGAURD ProtectPro, you will receive regular vulnerability scanning and penetration testing. Your dedicated Security Analyst will advise on the criticality of any perceived security risks and provide thoughtful recommendations to remediate with a deep understanding of your systems and business requirements. DYOGUARD ProtectPro also offers Security Reputation Monitoring (SRP) and Darkweb Monitoring (DWM), both of which provide invaluable insights into your organization's external security posture. By continuously analyzing the same information leveraged by malicious actors to identify potential targets, together, SRP and DWM arm C-Level executives and board members with a nuanced understanding of your organization's total risk landscape. DYOGUARD Protect Pro is rooted in the belief that understanding your organization's security posture as perceived by the outside world is essential to make informed and concise business decisions. By providing executive leadership with comprehensive security performance grading, DYOGUARD Protect Pro empowers organizations to proactively address vulnerabilities, enhance resilience, and stay ahead of emerging threats.
Physical Log Ingestion aka: IDS Device or Network Traffic Analyzer (NTA)	DYOPATH will deploy a Network Traffic Analyzer (NTA) at all locations with local internet access to inspect inbound and outbound network traffic data packets and to identify any potential threats within your network. The NTA will continuously collect syslog from all supported network devices and forward the data via an encrypted tunnel to the SIEM for correlation by the SOC team.
DYOGUARD Agent	In addition to collecting logs from network devices and external platforms via API integrations, the DYOGUARD SIEM also pulls critical endpoint logs from all workstations and servers within your environment. On each device, we will install the collector agent to pull logs such as: Device Events Collection, Device Performance Metrics, Process Analysis, Configuration Management Database (per device), System Log Collection for in-scope Network Devices, Application Monitoring, and Device-based Network Monitoring.
SOC Service	Managed SIEM and XDR represent the core functionality of DYOGUARD ProtectPro, optimized to defend your IT infrastructure from existing and emerging cyber threats. The managed SIEM (Security Information and Event Management) platform collects and analyzes security logs from various devices and applications across your network. The SIEM analyzes the logs to identify any suspicious activity and generates automated security alerts as part of our continuous monitoring and threat detection system. By combining our MDR (Managed Detection and Response) with the SIEM service, your organization can rest assured that the SOC team is performing continuous threat detection and rapid investigation and response to all alerts 24x7x365. XDR (Extended Detection and Response) is an evolution of traditional EDR (Endpoint Detection and Response) in that XDR goes far beyond protecting just your workstations and servers. Rather, XDR ensures the collection of security data from a much wider range of sources, including network devices (firewalls, switches) as well as cloud applications and environments which empowers our SOC team with a more holistic view of your total security landscape. While all DYOGUARD solutions leverage advanced analytics and machine learning to identify sophisticated threats that might evade traditional detection methods, the SOC team along with your dedicated Security Analyst actively monitor your network for threats 24/7. They investigate all security alerts and incidents to determine their legitimacy and severity. If necessary, incidents may be escalated to the DYOPATH NOC and/or your internal IT staff to take appropriate action to contain threats and mitigate damage as quickly as possible.

Cybereason License	Cybereason is DYOGUARD's entry level Endpoint Detection and Response (EDR) offering which focuses on MalOps, rapid response times, advanced detection, and global coverage. Few EDR solutions have been able to surpass Cybereason in the overall protection of ransomware specifically and other performance indicators in recent years. Cybereason provides the option of co-management of any environment with greater than 500 hosts.
DYOGUARD Integration Marketplace	As a DYOGUARD client, you will receive full access to all current and future API integrations present in the ArmorPoint Integration Marketplace. As development of new connections to the SOC Portal are developed, they will be systematically added to the SOC service.
Check Point Harmony Complete (Email Only)	Check Point Harmony Complete Protect (Email Only) is a cloud-based email security solution designed to protect organizations from a wide range of email-borne threats, including phishing, malware, ransomware, and spam. It leverages advanced AI and machine learning algorithms to analyze incoming, outgoing, and internal emails, providing comprehensive protection for your Microsoft 365 environment. It also includes Data Loss Prevention (DLP) and managed encryption emails.
Security Analyst 2	By leveraging the expertise and experience of a dedicated DYOPATH security analyst, you can significantly enhance your organization's cybersecurity posture, improve threat detection and response capabilities, and free up your internal IT staff to focus on other critical tasks.
Symbol Security PRO - Security Awareness Training	DYOGUARD Security Awareness Training improves our clients' cyber resilience by launching regularly scheduled phishing campaigns that leverage engaging content and practical simulations. This service focuses on educating employees on real-life cyber threats and the promotion of proactive defensive cybersecurity behaviors. The DYOGUARD Security Awareness Training program integrates interactive videos and real-life scenarios to meet compliance needs while reducing human-related cyber risk. This thorough training solution aims to empower employees with the knowledge and skills to exercise better security practices in their daily activities. The program recommends quarterly training content and phishing simulation, as well as provides reporting on a monthly or "as needed" basis.
Security Advisor	

DYOGUARD PROTECT PRO

- The quote assumes the client will deploy the required monitoring agents to endpoints.
- The quote assumes the client's production switching equipment is capable of performing port mirroring/SPAN. If the switching is unable to perform port mirroring/SPAN, re-configuration and pricing changes will incur.
- The quote does not include any vulnerability scanning remediation services. However, DYOPATH can help with any remediation requests, if any remediation is required will be billed on a T&M basis at the client's request.
- Quoted device and network log ingestion point quantities are estimates - the purchase of additional device support may be required.
- The client is responsible for shipping physical network log ingestion hardware to international sites. Additional monthly charges will apply if shipped by DYOPATH.
- If the client does not have the comfort level or resources to install an NTA, onsite T&M dispatch will be required to deploy the necessary equipment for DYOPATH to provide services.
- Armorpoint/N-Central installation requires either an MDM, RMM, or Windows Domain environment with the ability to deploy a GPO (requires all workstations to be in the office or have VPN capability for WFH individuals). If none of these are in place, a separate project to deploy an MDM/RMM solution prior to onboarding will be required.
- The quote includes seven hours of Security Analyst Management and Support. Any support beyond seven hours will be invoiced on a T&M basis.
- The quote assumes onboarding will be performed during normal business hours, Monday to Friday, 9:00 AM – 5:00 PM.

Managed Security Onboarding Overview

DYOPATH's onboarding process is delivered in three phases and requires intense collaboration between the Onboarding Team and the client to achieve project success. Delivery of client-owned deliverables and non-standard DYOPATH deployments will extend the onboarding duration.

DYOPATH will provide a fully managed SIEM which includes:

- Platform Health, Security, and Maintenance
- Platform Support, including:
    - User Training
    - Dashboard and Report Customization
    - Alert Rule Generation
    - Event-Handling
    - Log Parsing
- Continuous Device Monitoring, including:
    - Agent Log Collection
    - Syslog Log Collection
    - File Tailing
    - EDR Data Collection
    - Performance Monitoring
    - 3rd Party / External Integration

Managed Security Onboarding Timeline

- Indicates Client-owned Deliverables. Adherence to the Onboarding Timeline is dependent upon completion and delivery of Client-owned Deliverables.

Contract Processing Phase:

- Contract Signature – DYOPATH Order Form
- Client Submits Billing and Payment Information
- DYOPATH Confirms all necessary paperwork is completed
- Payment Received or Financing Documents Completed
- Onboarding team receives new onboarding request; schedules kickoff call and delivers DYOPATH Onboarding Discovery Checklist

Phase 1:

- Onboarding Kickoff Meeting with Client
- Client's Full Onboarding Discovery Checklist Received by DYOPATH Onboarding Team*
- Integrations Provided to Client
- DYOPATH Configures Network Sensor Device for Client
- Network Sensor Shipped to Client
- EDR Agent Delivered to Client

Phase 2:

- Deployment of EDR Agents
- Configuration of self-service integrations
- Enable Detection Policy on EDR Agents
- DYOPATH validates successful deployment of Agents + Integrations + Policies
- Installation deployment of Network Sensor
- DYOPATH validates successful deployment of Network Sensor

Phase 3:

- Dashboard Orientation and Incident Response Planning with Client
- Service Activation
- Closing Call

Managed Security Exclusions & Assumptions

The following assumptions apply to the scope of the work stated above and have been incorporated into the pricing stated below:

- Quoted Project Management (PM) hours are the minimum number of PM hours for which the client will be invoiced.
- The client will be invoiced for all PM hours performed, and the actual number may exceed quoted hours depending on the duration of the project, the availability of hardware (if applicable), the services contracted, and the client's requirements for meeting cadence and communications.

Additional charges may apply for any of the following:

- Any work or services required, but not expressly provided herein.
- Any application development or integration efforts not expressly provided herein.
- Any hardware purchases for on-premises needs.
- Any migration or upgrade of infrastructure (servers, network, etc.).
- Any implementation of the recommendations made by DYOPATH unless specified in this document.
- Any efforts tied to re-installing OS due to virus or malware or any system instability after the removal of a virus.
- Any work related to being crypto-locked. DYOPATH will work to mitigate the spread by blocking at the edge and/or taking machines offline.
- Any data recovery and forensics work due to purposeful or malicious client or application errors.
- Any software license or physical hardware expenses.
- Any software license that's not explicitly mentioned and not covered by DYOPATH.
- All travel and lodging costs.
- Any fees related to shipping, handling, customs, duties, and/or taxes.
- Any additional work requested beyond the scope of this Agreement will be expressly set forth by subsequent agreement, including, but not limited to, a Contract Change Request ('CCR').

End of Life Device and Operating System Risk Acceptance Agreement

The Parties agree to the following relating to End of Life Devices and Operating Systems:

- DYOPATH does not provide SIEM agent installers for end-of-life devices and/or operating systems.
- DYOPATH recommends all clients upgrade to supported versions as soon as possible.

End-of-life devices and/or operating systems are unable to continue to be patched from a security perspective and are high-risk security profiles for both the client and DYOPATH to support.

With this understanding, the client accepts this risk and acknowledges the following:

- Any support before onboarding is completed is out of scope.
- DYOPATH does not provide installers or collectors for device logs to be collected by the SIEM.
- DYOPATH will provide an EDR agent to devices where an EDR package has an approved installer on specific end-of-life devices.
- If the EDR agent does not install properly on an end-of-life device, troubleshooting becomes the responsibility of the client.
- DYOPATH will provide an EDR agent and installer, but there is no guarantee on performance or protection of those devices.
- Any such non-supported devices are not included in the bucket of support hours provided by DYOPATH.
- Any remediation work specifically tied to end-of-life devices and/or operating systems will be billed on a T&M basis.

Harmony Overview:

Harmony Advanced Protection is a top-tier email security solution that seamlessly integrates with major platforms like Office 365 and G Suite. Utilizing AI and machine learning, it offers advanced threat detection against phishing, malware, and ransomware. With multi-layered security measures such as sandboxing and URL protection, Harmony ensures robust protection. Its cloud-based architecture allows for scalability and rapid updates, while user behavior analysis provides proactive threat management. This solution not only enhances security but also boosts operational efficiency and cost-effectiveness, offering an intuitive and user-friendly experience for both IT administrators and end-users.

Harmony Onboarding:
DYOPATH will collaborate with the customer to ensure delivery and implementation of Harmony.

Symbol Security:

Implementation for the services quoted is included and addressed directly by Symbol.

Quantities have been provided by the client and may be trued up, with actual quantities billed if needed subscriptions exceed what is quoted.

Pricing Summary

Type	Monthly Recurring	Non-Recurring
Advanced Security Services	$6,366.32	$0.00
Managed Services	$128.00	$2,720.00
Professional Service	$0.00	$4,058.00
Totals	**$6,494.32**	**$6,778.00**

CLIENT SIGNATURE		DYOPATH SIGNATURE	
Client Signature		**Signature**	
Title	Superintendent	**Title**	COO
Client Name	Erik Young	**Name**	Steve Roth
Date Signed		**Date Signed**	

* This Attachment A is governed by the DYOPATH Managed Services Agreement (“MSA”), effective on the date this Attachment A is signed . The provisions set forth under the MSA are incorporated into and made part of this Attachment A as if the terms and conditions were fully set forth herein. Client unequivocally accepts the MSA and all related Attachments, Amendments, and/or Addendums (the ''Agreement'') and their respective terms. Any additions or changes to this Agreement must be set forth in a modification and agreed to by DYOPATH and Client.
* The DYOPATH MSA is available at https://dyopath.com/resources/legal/MSA and will be sent to Client upon request.
* If Professional Services are incorporated in this Attachment A, one or more of the following payment terms apply:
    1. **Dropship/Hardware/Software only purchases:** Immediately following contract execution, DYOPATH will invoice Client for 100% of the total price. Payments are due upon receipt of invoice.
    2. **Dropship/Hardware/Software purchases with Professional Services:** Immediately following contract execution, DYOPATH will invoice Client for 100% of all hardware/software/license and 50% of the Professional Services quoted. Balance will be due upon completion of the Services. Payments are due upon receipt of invoice.
    3. **Professional Services - Firm Fixed Price (FFP):** Immediately following contract execution, DYOPATH will invoice the Client for 50% of the total price. Balance will be due upon completion of the Services. Payments are due upon receipt of invoice.
    4. **Professional Services – Time & Materials (T&M):** T&M Professional Services with a duration of one month or less will be invoiced in full at completion of the Services. T&M Professional Services with a duration greater than one month will be invoiced monthly based on hours expended during each month. Payments are due upon receipt of invoice.
    5. **Security Remediation (non-existing clients):** Prior to commencing any related security remediation work, DYOPATH will provide payment instructions to Client (Wire Transfer or ACH). 100% of payment is due upon receipt of the instructions.

* Pricing does not include taxes, shipping, or handling.
* Pricing does not include carrier services, equipment, or installation (unless otherwise specified) including but not limited to: Wiring, circuit and/or station identification ("toning and tagging"), patch cables, cross connects, patch panels, racks, shelves, rack mounting kits, wire management, cable labels/tags, demarcation extension, environmental, UPS, orelectrical.
* Any 3rd party software or cloud licenses sold and billed on a regular basis by DYOPATH do not include services for ongoing monitoring and management of these solutions. These services will be billed on a time and material basis if requested.
* *Client is responsible for ensuring environmental requirements are met including but not limited to physical space, physical clearance, weight, electrical power, electrical static discharge, altitude, temperature, and humidity. DYOPATH to provide equipment data sheet upon request.*

* *Discounted pricing is contingent upon 3rd party vendor approval, if applicable.*
* *Any client provided hardware that requires remediation is not included in the scope of this project. DYOPATH will bill and invoice separately for this work on a time and material basis given Client approval.*