Effective July 14, 2023. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

SisCare Managed Services

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Server Monitoring and Management – Provider will perform server monitoring and management including, alert monitoring and management of servers, periodic reporting and performance tuning, and prioritization of alerts to identify high-priority incidents. Provider will also perform remote remediation services as needed, and backup software monitoring and management. The Service Fee does not include major hardware / software upgrades or replacements or new server installations.

Desktop Monitoring and Management – Provider will perform desktop monitoring and management including, alert monitoring & management of desktops, prioritization of alerts to identify high-priority incidents, remote remediation services as needed, quarterly configuration backups, quarterly firmware updates as required by manufacturer, and quarterly reporting and performance tuning. The Service Fee does not include hardware replacement or new hardware installations.

Help Desk Services – Provider will provide help desk support via client portal, e-mail, and phone. Provider has the ability to remotely control desktops to support employees. Unless otherwise included in an order, all help desk services will include unlimited remote support as required.

On-site Support - Upon request and subject to the limitations identified in the Order, for Services that are within the scope of this Service Attachment, Provider will also deliver support Services on-site at your location during normal business hours. For on-site support that is not included in the Order, Client, Client will pay Provider's then-prevailing hourly rate. Emergency and Scheduled After-Hours support maybe be covered as defined in the Order.

Core Security Services – Provider will include in its services monthly Microsoft patch management, antivirus software and management, and remote software installations. Core Security Services also includes new / terminated employee setup and configuration.

Problem Management Services - Provider will undertake problem management as soon as the Provider's monitoring staff becomes aware of an incident. All incidents, with status or resolution, will be documented by posting updates to the Problem (Incident) Ticket Tracking System assigned to Client ("Problem Tickets").

Included Security Services –

Firewall, Anti-malware, and Intrusion Detection – Provider will install and configure firewall traffic policies, apply updated firmware when applicable, and configure changes

when needed. The first installation and configuration is billed pursuant to the project fees. With respect to the firewall, Provider will include the following:

- Intrusion Prevention - provides real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.
- URL Filtering - blocks known malicious sites, and delivers granular content and URL filtering tools to block inappropriate content.
- Gateway Antivirus - continuously updated signatures, identify and block known spyware, viruses, trojans, worms, rogueware and blended threats – including new variants of known viruses.

Security Risk Assessment

- Malware and Vulnerability Review – Using one or more tools to determine the existence of malware or vulnerabilities.
- Personally Identifiable Information ("PII") – Review practices related to PII, including location, treatment, and risk mitigation.
- Report – Provider's findings will be included in a Risk Assessment Report.

Reputation-Based Threat Prevention - Cloud-based web reputation service that aggregates data from multiple feeds to provide real-time protection from malicious sites and botnets, while dramatically improving web processing overhead.

Network Discovery - generates a visual map of all nodes on your network, making it easy to see where you may be at risk.

Spam Prevention - Real-time, continuous, and highly reliable protection from spam and phishing attempts.

Intelligent Antivirus – leverages signature-less anti-malware solution that relies on artificial intelligence to automate malware discovery.

Anti-malware - Provider will provide and install anti-malware software of Provider's choosing for each Device covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client's network are safe from viruses, malware, bugs, hacking, phishing schemes or defective or malicious files, programs or links ("Harmful Content"), of any kind whether now known or hereinafter invented, Provider does not guarantee that Client computers or network cannot be infected by Harmful Content. Where this does happen, Provider will provide commercially reasonable Services to mitigate the Harmful Content. Additional Services will be available upon mutual agreement of the parties.

Remote Access - Provider will install remote access and remote monitoring and management software on Client's Devices possibly other equipment at Client's office. Client grants permission to Provider to install any remote access or remote monitoring and management software deemed necessary by Provider.

Security Awareness Training Phishing Simulations - Provider will acquire and will assign an appropriate number of licenses to support the client environment. The Service will schedule phishing campaigns to send at random times during a specified period. The

campaigns are trackable and fully customizable designed to keep track of every user's participation, making all cybersecurity education accountable and measurable.

Multi-Factor Authentication Services / Password Credential Management Services – Provider will configure two-factor authentication for compatible software applications, institute single sign-on services for compatible software applications and customized security policies and procedures. After performing a security assessment and assessing the state of Client's existing policies and procedures pertaining to network security (if any), Provider will work with Client to prepare a new or revised set of policies and procedures that incorporate cutting edge best practices and that take advantage of the other Services delivered by Provider. Setup and al other fees are defined in the Order.

SisCare Secure – Managed Security Services

In addition to all services listed in SisCare Manage Services, the following Services are included.

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

Customized Phishing Simulations - Provider will create custom Phishing simulation test with you specific company information periodically to further challenge your staff's cyber knowledge.

APT Blocker - detects and stops the most sophisticated attacks including ransomware, zero-day threats, and other advanced malware designed to evade traditional network security defenses.

Threat Detection & Response - Security data collected from the firewall is correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attack.

DNS Filtering - detects and blocks malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices. This Service is offered with SisCare Secure.

Client-Side DNS Filtering - Provider will acquire and will assign an appropriate number of licenses to support the deployment of client-side DNS Filtering on all laptop systems. The DNS filtering is designed to detect and block malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices and to protect laptops while away from the corporate network. This Service is offered with Field Effect/SisCare Secure.

Security Operations Center – The Service below are offered with Field Effect/SisCare Secure:

- Advanced Malware Protection supported by Security Operations Center (SOC).
- Deployment of advanced malware protection applications to all Windows based devices on customer network.
- 24x7 SOC service analyzes quarantined applications and files, reducing false positives.
- Immediate risk identification – Provides rapid recognition of thousands of viruses and malware attack variants, including cryptomining attacks, as well as the root causes of these malicious behaviors, by quickly identifying and diagnosing corrupt source processes and system settings.
- Ransomware rollback - quickly rollback files to previous safe versions through tracking changes in your devices and restoring them to an acceptable risk state.

Security Log Management – Provider will configure log sources to capture and retain information without creating excessive logging, limit user access to log files, avoid logging sensitive or protected information, secure the processes that generate logs, identify and resolve logging errors, and analyze log entries, prioritize entries, and respond to those requiring action.

Security Incident Event Management (SIEM) Services supported by SOC – Provider will deploy SIEM monitoring probes to monitor all critical network devices including; domain controller, firewalls, network switches and routers. When meeting compliance requirement deployment will include all Windows devices as well.

Incident Response - Provider will assist Client in the hours immediately following a data breach to identify the likely source of the breach and to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts past the first twenty-four (24) hours following a breach – including but not limited to breach-notification planning, in-depth forensic examinations of the source of a breach, and significant, post-breach systems reconfiguration – are not within the scope of this Service Attachment. If Client requests Provider's assistance with such activities, Provider will prepare a separate Service Attachment for Project Services that will specify what the charges will be for such assistance.

MANAGED DETECTION & RESPONSE (MDR)

- Built from the ground-up to detect and respond to abnormal behavior on endpoints, cloud services, and networks, Covalence is a holistic cyber security solution that delivers visibility into the threats and risks facing your business—giving you the advantages of automated cyber security, backed by human intelligence.
- Secure your network by analyzing all network traffic, including known and unknown devices, Internet of Things (IoT) devices, and mobile devices. Identify and respond to threats and potential vulnerabilities to your network.
- Protect all your endpoints—including servers, desktops, and laptops—and identify anomalous behavior to actively block known and emerging malware and attack techniques.
- Use our cloud-native monitoring sensor to protect your company domain and cloud-based programs and applications, including Microsoft 365, Google Workspace, Amazon Web Services, Azure, Dropbox, Box, Okta, Salesforce, and more.
- MDR researched and built with an attacker mindset, applying the techniques and tactics used to infiltrate an environment. This has resulted in a security solution capable and proven to identify techniques at the earliest phase possible of an attack and thwart the attack in real-time.

24X7 ACTIVE RESPONSE

- Active Response is a feature that, when enabled, gives our analysts immediate access to intervene when a threat is detected in your environment. Depending on your response policy, our analysts will intervene with response actions that can stop the threat or resolve the vulnerability. The more aggressive the response policy, the more aggressive the response action will be.
- A response action could involve human intervention, but if the threat is severe and clearly identified as a threat, Covalence may initiate an automated response action.
- Automatic response actions include blocking malware, isolating devices, or an analyst taking further action to protect your business. We take the appropriate action on your behalf based on your risk tolerance.

THREAT ISOLATION & CONTAINMENT

- Obtain better insight and security recommendations thanks to our expert threat hunters who dive deep into network and Covalence data to identify new, emerging, or otherwise undetected weaknesses and threats.
- Benefit from machine learning and analytic capabilities that provide continuous analysis of user and service data to identify and address threats. The result is real-time visibility to detect, monitor, measure, manage, and reduce attackable points from end to end.

VULNERABILITY MANAGEMENT

- Proactive identification of all known vulnerabilities, and a multitude of operational vulnerabilities likely to affect your organization's operation.
- Identify important changes and activity across your IT environment that indicate risks—including misconfigured cloud services or firewall ports, unpatched or vulnerable software, legacy or vulnerable encryption technology or protocols in use, systems out of patch, incorrect service configs & more —and receive detailed steps to resolve issues to harden your attack surface.

THREAT INTELLIGENCE

- Covalence includes manicured and continuously updated threat intelligence from government, public, private, and Field Effect-proprietary sources. These indicators include IP addresses, domains, and network signatures.
- Signatures and threat intelligence are updated as prevailing threats (such as a new botnet, highly publicized vulnerability, or crypto mining) shift and evolve.
- Blacklist hits/threat intelligence hits are fully managed and reviewed by Field Effect as part of the Covalence service.

DATA BACKUP AND DISASTER RECOVERY SERVICE

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a separate Order including those Services.

Local Backups - Using customer provider hardware and software (backup software), backups will be performed on the basis specified in the Order. Client owns the hardware and software agents (backup software) used to perform the backups. If Client subscribes to periodic Server Maintenance, Provider will review the backups during Maintenance and notify Client of backup failures. Client will notify the Provider of any failures, and upon request, perform simple on-site tasks (e.g., powering down and rebooting hardware).

Remote Backups - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data files are backed up via a third-party client-side desktop/server software application (the "Application"), encrypted, and then sent to a storage server at third-party vendor's data center facility. There is no local copy of the backed-up data. Data files can be restored from the cloud but the server itself cannot be recovered or "booted" in the cloud. Therefore, this service is not considered a disaster recovery solution. All data is backed up via a third-party client-side desktop/server software application (the "Application"). Provider will monitor the backups daily, notify Client of any failures, and work with third-party to resolve backup failures.

Cloud Backup - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data is backed up via a third-party client-side desktop/server application, encrypted, stored locally on a Datto Altos Provider-owned storage device ("Provider Owned Storage"), and then sent to a third-party owned storage server at the Third-Party Services Provider's data center facility. Provider will monitor the status of all scheduled backup jobs, notify Client of Provider-owned storage failures and corrective actions. Provider will also provide remote administrative services of Data Backup Service as requested by Client. Offsite Backup copies will have one-year retention unless specified in Order. Upon termination of these Services, Provider will request return of the backup hardware and remove the Application from Client systems.

Disaster Recovery

Provider will work with Client to develop a comprehensive disaster-recovery plan that incorporates the Services to be delivered under this Service Attachment.

If Client experiences an event precipitating a major, multi-user loss of data, Client may notify Provider that a data loss event has occurred.

FILE BACKUP AND RECOVERY

Provider will create, monitor, and modify up to the number of file backup jobs listed in the Order. Provider will also notify Client by email of backup drive failures and corrective actions.

Upon request, Provider will remotely restore files, subject to the number of operations listed in the Order

CLOUD AND HOSTING SERVICES

Public Cloud - Provider will move all Client's data to a cloud computing platform, allow Client to have access to data via virtual desktop from Client's own devices or device provided by Provider, and manage the cloud environment for Client.

Hybrid Cloud - Provider will move some of Client's data to a cloud computing platform, and upon Client's request, place a server on premises at Client's location. Any Client data being moved shall be agreed to by the parties in writing prior to moving with specific instructions as to identify which data will be moved, managed or unmanaged by Provider. Any Client data being moved or managed shall be specifically identified as to the location of the data on a particular server. Any Client data not being moved, or that is not specifically identified by Client will be considered not managed. Provider shall not be responsible for the identification, classification, or location of the data. Client is solely responsible for its data up to the outermost point of Provider's firewall with the public internet (the "Demarcation Point"). Once data has been identified, classified, its final location determined, and moved past the Demarcation Point, Provider shall then become responsible for Client data. Provider will also manage the cloud environment for client and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Private Cloud or Software Subscriptions - Provider will maintain all Client's data on premise at Client's location, manage the cloud environment and software subscriptions for Client, provide unmanaged cloud environment and software subscriptions for Client, and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Third-Party Cloud & SaaS Vendors - Provider will provide, install, and support the Third-Party Cloud or software-as-a-service vendors listed on the Order, including but not limited to Microsoft. Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this software is subject to the applicable third-party cloud or software-as-a-service vendor's agreement regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client agrees to be bound by any applicable third-party cloud or software-as-a-service vendor's agreements regarding terms or use or end user licensing, and Client understands that any applicable agreement regarding terms of user or end user licensing is subject to change by any Third-Party vendor or software-as-a-service provider without notice.

CYBER TRAINING SERVICES

Provider will implement and managed a managed cybersecurity awareness training platform ordered through a third party on Client's behalf. The program features:

- Enrolling all technology-facing workforce members in the program
- Access to a curriculum of industry-leading cybersecurity awareness education which can be customized to meet the unique needs and regulatory requirements of Client
- Management reporting and visibility into workforce participation and progress in the training
- Regular campaigns to test each workforce member's ability to recognize and effectively respond to cyberattacks which typically target individuals

- Automated enrollment in remedial training for individual workforce members, when appropriate
- Management reporting and visibility into workforce performance on testing campaigns
- Management reporting and visibility into the improvement in workforce awareness and performance over time
- Lowered risk to (Client) from cyberattacks which target unaware and untrained individuals

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.