SecureWatch Managed Service Agreement

This SecureWatch Managed Service Description and Agreement ("Agreement") is made effective as of the Effective Date (defined below) by and between Corero Network Security, Inc. ("Corero") a Delaware corporation with its head office located at 225 Cedar Hill Street, Suite 337, Marlborough, Massachusetts, 01752, United States and the customer ("Customer") who purchases the Services (defined below). Customer shall evidence its intent to order the Services and its acceptance of this Agreement by submitting a Purchase Order to Corero, either directly or via an authorized Corero Distributor or Reseller (the "Purchase Order"). Such Purchase Order shall also provide Customer's corporate identity information. Corero shall indicate its acceptance of Customer's Purchase Order either via an Order Acceptance or by commencing, or continuing, to provide the Services.

As used herein "Effective Date" means the date as identified in the applicable Purchase Order as the effective start date for the period over which Services shall be rendered or if no date is specified then either (1) first date that Corero provides Customer with any Services or (2) the expiration date of any previous service term between Corero and Customer for similar services. In consideration of the mutual promises below and other good and valuable consideration the sufficiency of which are hereby acknowledged, the parties agree to the terms of this Agreement.

CUSTOMERS WHO PURCHASE SECUREWATCH MANAGED SERVICES FROM CORERO SHALL RECEIVE THE SERVICES DEFINED IN THIS DESCRIPTION AND AGREEMENT, SUBJECT TO THE TERMS AND CONDITIONS STATED HEREIN. CORERO MAY MAKE CHANGES TO THE SERVICES, OR THE MANNER IN WHICH IT PROVIDES SERVICES, UPON NOTICE TO CUSTOMER WHICH SHALL BE DEEMED TO HAVE BEEN PROVIDED WHEN POSTED ON THE CORERO SUPPORT PORTAL; PROVIDED THAT ANY SUCH CHANGES SHALL NOT DIMINISH THE SUBSTANCE OF THE SERVICES. BY ORDERING SECUREWATCH MANAGED SERVICES AND ACCEPTING THE BENEFIT OF THE SERVICES, CUSTOMER CONCLUSIVELY INDICATES THAT IT ACCEPTS ALL OF THE TERMS OF THIS DESCRIPTION AND AGREEMENT.

Description of Services

The SecureWatch Managed Service is a suite of configuration optimization, monitoring and response services delivered by the Corero Security Operations Center ("SOC"). Customers receive expert DDoS services including monitoring and response in the event of a DDoS attack.

1.0 Pre-requisites

In order for Corero to deliver the Services, Customer must have installed the following Corero products and services for each of the Corero devices comprising the Equipment: Centralized Management System Software and SecureWatch Analytics Software and purchased an active Software, Maintenance, Updates, and Maintain ("SMUM") Services agreement for each of the Corero devices listed in the Equipment Summary.

2.0 Initiation Services

A. The SOC will audit Customer's IT environment and standard customer IP traffic patterns in order to establish a baseline.

B. The SOC will create and deploy a defensive configuration ("Defensive Configuration") based on results of the audit for the Equipment deployed at the specified Customer location based on Customer's security policy, business objectives and DDoS defense best practices.

C. The SOC and Customer shall collaboratively establish a coordinated DDoS threat response plan for timely and effective actions that ensure high availability of critical systems and applications in the event of an attack (the "Response Plan").

3.0 Ongoing Services

The SOC will deliver the following services on an ongoing basis during the Term:

A. Install all Software Updates for deployed Corero products in accordance with the Change Management Process.

B. Implement actions described in Threat Update Security Advisories in accordance with the Change Management Process.

C. Initiate the Advanced Hardware Replacement (AHR) process, if subscribed to by the Customer, in the event of a Hardware failure.

D. Deliver e-mail reports of the standard weekly configuration, performance, fault and security activity including:

- Device status
- Software Upgrade availability
- Uptime summary
- Analysis of base line DDoS rates
- Service request(s) status
- Malicious Activity Summary

- Top Sources of Attack
- Top Destinations of Attack
- Volumetric Security Events
- Top 25 Rules Blocked
- Detailed Threat View
- Security in the news

E. Ongoing collaboration and communication between the SOC and Customer to ensure up-to-date defenses in the face of evolving threats and a dynamic end-user environment.

F. Corero device system monitoring, on a 24x7 basis, to deliver real-time alerting to Customer.

G. If/once Customer's Equipment is under attack, Corero's SecureWatch Analysis Team ("SWAT") will initiate the DDoS Defense Response Services as defined below.

H. Maintain at least monthly bi-lateral communications between the SOC and Customer to include:
- Customer awareness of latest general DDoS threat activity
- Maintenance of documentation describing Customer IT environment
- Maintenance of Defensive Configuration
- Review and validation of the ongoing applicability of the Response Plan

4.0 DDoS Defense Response Levels

The frequency of DDoS Defense Response incidents is defined by the SecureWatch Managed Service Level that Customer submits a Purchase Order for. The SecureWatch Managed Service Levels are:

A. SWM-Q: 4 incidents per annum
B. SWM-M: 12 incidents per annum
C. SWM-U: Unlimited incidents

"Incident(s)" means a Customer triggered investigation resulting in the requirement for network traffic analysis, which may lead to proposed security configuration tuning that goes beyond SecureWatch Managed Service best-practices configuration. This does not include any Customer triggered investigation relating to Hardware malfunction, software bugs, or the security configuration tuning within the initial on-boarding period. Each Incident investigation and tuning is limited to a 24-hour time period from time of Customer initiation.

Customer's that use their contracted number of SecureWatch Managed Service Incidents prior to the expiration of the annual service will be required to submit a new Purchase Order for a SecureWatch Managed Service offering in order to receive continued Incident support from the SOC. DDoS Defense Response incidents are defined in Section 5.

5.0 DDoS Defense Response Services

A. The SOC shall use all commercially reasonable efforts on a 24x7x365 basis to provide support and coordination, according to the Response Plan, to mitigate the DDoS attack, with the following objectives:

i. Minimal impact to Customer major business operations
ii. Only occasional or intermittent instabilities of Customer core business functions
iii. Limited Customer traffic impact, loss of connectivity or security exposure

All Mitigation efforts defined above and the results of such efforts are limited to and by:

1) Product capabilities as documented in the Corero Product specifications,
2) Deployment location or configuration limitations, and
3) Network bandwidth, in the case of DDoS attacks that are beyond the capacity of Customer subscribed network bandwidth.

B. The SOC shall deliver mitigation support according to the following specific commitments:

Initial Response to Attack	Maximum Reporting Interval	Corero Engagement
< 30 minutes	Every 2 hours	Ongoing commercially reasonable engagement until mitigation

C. The SOC will deliver a post-incident report containing an assessment of the DDoS attack, impact and recommended measures to improve preparation for and response to possible future attacks.

The Services description and method of delivery may be changed by Corero from time to time and shall be deemed amended when an updated description is posted on the Support Portal.

6.0 Customer Responsibilities

In order for Corero to deliver the Services, Customer shall provide and perform the following:

A. Complete and execute the SecureWatch Access Authorization Form and return it to Corero.

B. Provide the SOC with ongoing remote access to the Controller server and the Equipment as deemed appropriate by Customer in its sole

discretion. If the means for Corero to access any or all of the Equipment changes, Customer shall provide Corero with one-week prior written notice communicated to the SOC. If failure to provide remote access to Corero or deliver such notice directly and adversely impacts Corero's ability to deliver the Services, Customer shall not be entitled to terminate this Agreement.

C. Provide the SOC with Customer's standard operating procedures, if any, for Change Management of the Equipment.

D. Provide the SOC with a Customer contact list including names and contact information (phone and email) (1) for reporting purposes and (2) for escalation of issues necessary for the successful delivery of the Services.

E. Make necessary arrangements to work cooperatively with the SOC in the isolation and resolution of reported service requests. If such reasonable necessary arrangements are inadequate and directly and adversely impact Corero's ability to deliver the Services, Customer shall not be entitled to terminate this Agreement.

F. Provide all information on Customer environment including security policy, business objectives, server configurations and applications usage baseline. If all information reasonably required by Corero is not provided and this directly and adversely impacts Corero's ability to deliver the Services, Customer shall not be entitled to terminate this Agreement.

G. Provide Corero SOC at least thirty (30) days advance written notice of its intention to move the Equipment which notice must specify the new location; provided, however, that Customer shall provide Corero written notice of an emergency move within ten (10) days after such emergency move. Failure to provide any such notice, shall not constitute a breach of this Agreement. If failure to deliver such notice directly and adversely impacts Corero's ability to deliver the Services, Customer shall not be entitled to terminate this Agreement.

H. Work with the SOC to define a DDoS Response Plan.

I. Engage in bi-lateral communications with the SOC, at least monthly, to include:
   i. Provide the SOC with awareness of changes to Customer environment
   ii. Review and validation of the ongoing applicability of the DDoS Response Plan

J. Ensure 24x7 availability of a named Customer contact in the event of a DDoS attack, to deliver Customer specific aspects defined within the Response Plan, until mitigation of the DDoS attack. If Customer fails to make Customer contact available and this directly and adversely impacts Corero's ability to deliver the Services, Customer shall not be entitled to terminate this Agreement.

K. Customer contact availability is defined according to the following Customer commitment:

Initial Availability Subsequent to an Attack	Maximum Response time for Customer actions within DDoS Response Plan execution	Customer Engagement
< 30 minutes	< 30 minutes	Ongoing commercially reasonable engagement until mitigation

Failure by Customer to meet these targets shall not constitute a breach of this Agreement. If Customer fails to engage in commercially reasonable engagement and that directly and adversely impacts Corero's ability to deliver the Services and its targets, Customer shall not be entitled to terminate this Agreement.

SecureWatch Data Collection, Storage and Access Guide

Introduction
SecureWatch is a suite of subscription based security services provided by Corero to customers and designed to maximize the effectiveness of Corero security solutions in protecting customer infrastructure and data.

Within the context and scope of SecureWatch service delivery, Corero requires access to the installed Corero Equipment (Equipment purchased by customer from Corero) for the purposes of fault, configuration, performance and security management. In addition, the Service requires the capture and analysis of device management and security events generated by the Corero products for the purposes of optimizing customer security protections, maintaining system performance and incident handling.

Corero provides and maintains a secure Server ("Corero Server") to enable this service which contains the central management and analytics tools both accessible by the customer locally.

Corero assigns critical importance to the control, security and confidentiality of Customer's information and places major significance on providing clear definitions of the scope of the information collected and the nature of any analysis undertaken.

The Corero Network Security data usage policy is described below.

Overview
The Corero SecureWatch Service leverages industry standard, enterprise grade monitoring tools that have been customized to gather detailed operational information from Corero Equipment and management applications providing automated administration and response where required. The service is restricted to monitoring Corero-supplied devices only (collectively "Corero Hardware").

For licensing purposes, the monitoring and reporting components are tied to a central license server within the Corero facilities. A failure to communicate with the license server will shut down the service.

Data Usage and Storage
The SecureWatch systems capture information using custom software designed specifically to interact with the Corero Hardware over encrypted data channels together with core system events from the central management and security solutions. This information is used in the analysis of system faults and security events for policy design and incident handling.

Access to these systems is restricted, monitored and recorded for audit purposes. Corero will make access records to customer's system available upon Customer's request.

What Information is collected?
The following is a summary listing of the categories and types of data collected under each category:

- **Network Traffic, Security Event, Corero SmartWall Device Health Information:** Summarized Network Traffic Meta Data and Security Events generated by the Corero Hardware are collected to provide customer Dashboards, Alerting and Reporting. This information includes Security Messages, Network Messages, Top Type Meta Data messages, System Messages and sampled Sflow sample messages.

- **System Configurations and Logs Information:** Periodically system configuration and device log information are collected from the Corero Server. This information includes Central Management System backup files and audit and diagnostic log files.

- **Server System Health information:** The Corero Server VM and physical Health information is collected to provide forensic backup information during the analysis of customer incidents. This information includes VM CPU and memory usage as well as the Corero Server management port statistics.

This full set of collected information is available at any time on request by Customer to the SOC.

Where Information is stored?

- **Network Traffic, Security Event, Corero SmartWall Device Health Information:** The customer sensitive data is all stored locally at the customer location on the provided server. All incident analysis is conducted using the locally stored data.

- **System Configurations and Logs Information:** The system configuration and logs data is stored at Corero's secure colocation facilities. This information does not contain any specific customer data.

- **Server System Health information:** The server system health information is stored at Corero's secure colocation facilities. This information does not contain any customer sensitive data.

Connecting the Corero Equipment to the Corero SOC
The SecureWatch service requires a secure connection between the Corero Server and the monitoring systems in Corero's primary and backup secure colocation facilities. The Corero Server initiates and maintains a secure OpenVPN or SSH tunnel with the various secure co-locations. Access to these co-locations is restricted to Corero SOC personal and protected by multi-vendor solutions.

Access Requirements
Once connectivity is established the Corero SOC team will have direct access to the Corero Server, central management and reporting solutions as well as the Corero devices.

Change Control
Changes to customer policies is carried out in accordance with customer defined change control procedures. These typically include emergency change control procedures that provide Corero SOC personnel the ability to apply changes to the policy to ensure continuity of service during sustained high volume events.

All changes are documented and reviewed with the Customer.

Equipment Summary

Customer Technical Contact Information:

Company Name: _____
Name: _____
Title: _____
Phone: _____
Email: _____

The SecureWatch Managed Service purchased by the Customer ("the Service") is associated with a set of unique Corero devices and Customer location ("Location"). The following form, defines the Equipment and Location covered by the Service purchased ("Equipment Summary").

Corero Product Model	Serial Number	Location
1)		
2)		
3)		
4)		
5)		
6)		
7)		
8)		
9)		
10)		
11)		
12)		
13)		
14)		
15)		
16)		
17)		
18)		
19)		
20)		