SecureWatch Managed Service Agreement

This SecureWatch Managed Service Agreement ("Agreement") is made effective as of the Effective Date (defined below) by and between the Corero entity as defined below ("Corero") 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.

"Corero" shall mean the Corero corporate entity identified in the Sales Quotation or Order Acceptance (each as defined below), either Corero Network Security, Inc., a Delaware corporation with its head office located at 293 Boston Post Road West, Suite 310, Marlborough, MA 01752, United States or Corero Network Security (UK) Ltd, a company incorporated in England and Wales with registration number 04047090 with its registered office at Regus House, Highbridge, Oxford Road, Uxbridge, UB8 1HR, UK.

CUSTOMERS WHO PURCHASE SECUREWATCH MANAGED SERVICES FROM CORERO SHALL RECEIVE THE SERVICES DEFINED IN THIS 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 AGREEMENT.

Purchase of Services

Customer shall offer to purchase the Services by submitting a Purchase Order to Corero, either directly or via an Authorized Partner.

Corero shall indicate its acceptance of Customer or Authorized Partner's Purchase Order either by accepting such Purchase Order in writing ("Order Acceptance") or by commencing, or continuing, to provide the Services. Any term and condition stated on such Purchase Order or any Sales Quotation or other similar document that conflicts with the provisions of this Agreement shall be null and void.

The purchase price for Services shall be as set forth in the applicable Sales Quotation issued by Corero to Customer or Authorized Partner. Prices set forth in a Sales Quotation shall be valid and binding on Corero for sixty (60) days after the issuance of such Sales Quotation, or until the expiration date set forth on such Sales Quotation, whichever occurs earlier. Absent a binding Sales Quotation the prices shall be those set forth in an accepted Purchase Order.

Each Purchase Order shall be subject to Corero's or the Authorized Partner's written confirmation and acceptance and shall not be binding upon Corero until it has been accepted. Purchase Orders must be accepted or rejected in their totality.

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 Corero products and purchased an active Software, Maintenance, Updates and Maintain ("SMUM") Services agreement for each of the Corero products listed in Exhibit B.

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 failure in Corero supplied hardware.

D. Deliver reports of the standard weekly configuration, performance, fault and security such as:

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

G. If/once Customer 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; and
- 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 the SmartWall Solution 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; and
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 Corero Support Portal.
https://corero.force.com/support

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 SmartWall Solution as deemed appropriate by Customer in its sole discretion. If the means for Corero to access the SmartWall Solution 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 and Corero shall have no liability to Customer for such adverse impacts.

C. Provide the SOC with Customer's standard operating procedures, if any, for Change Management relating to the SmartWall Solution.

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 reasonably 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 SmartWall Solution installation location 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. Informing the SOC of changes to Customer environment; and
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.

General Terms

Term and Termination

1.1 The term of this Agreement shall begin on the Effective Date and unless terminated earlier in accordance with this Agreement shall continue for the specific period indicated on Customer's Purchase Order ("Initial Term"). Customer or Authorized Partner may extend the term of this Agreement by submitting a Purchase Order for the renewal of services prior to the expiration of the Initial Term. Each extension of the term as indicated on the Purchase Order shall be defined as a "Renewal Term." The Initial Term and all subsequent Renewal Terms shall collectively be referred to as the "Term."

1.2 If either party fails to perform any material obligation under this Agreement or otherwise materially breaches this Agreement, the non-breaching party may terminate this Agreement upon thirty (30) days written notice to the breaching party specifying the default (the "Default Notice") unless (a) the default specified in the Default Notice has been cured within the thirty (30) day period, or (b) the default reasonably requires more than thirty (30) days to correct (excluding any failure to pay money) and the defaulting party has begun substantial corrective action to correct the default within such thirty (30) day period, in which case the termination shall not be effective unless the default has not been remedied and ninety (90) days have expired from the date of the Default Notice.

1.3 Except for willful wrongful conduct by or on behalf of Corero, termination of this Agreement shall be Customer's sole and exclusive remedy for any breach of this Agreement by Corero.

1.4 If the Equipment which is the subject of the Services is moved to another location without prior written notification to Corero in accordance with Customer's Responsibility described in this Agreement and the Exhibits, and such failure to notify Corero prevents the delivery of Services by Corero, such failure by Corero shall not constitute a breach of this Agreement.

2. **Charges, Payment and Tax**

2.1 Customer shall pay Corero either directly or via an Authorized Partner the fees and charges set forth in the accepted Purchase Order; provided that unless specified otherwise in a Purchase Order, Services priced in one year increments may be adjusted annually as mutually agreed by the parties, provided, however, that in the absence of such agreement, Corero may increase the amount of such charges provided, however, the amount of such annual increase shall not exceed five (5) per cent. Amounts due annually shall be invoiced at the commencement of each such annual service period.

2.2 Payment terms are net thirty (30) days from the invoice date. All charges shall be invoiced and paid in the currency identified in the Sales Quotation.

2.3 The charges and fees hereunder are exclusive of all taxes, duties and charges imposed or levied in any applicable governmental entity or any political subdivision thereof in connection with the provision of Services. Customer shall be liable for any such taxes, duties or charges, other than taxes based on Corero's gross or net income.

3. **Confidential Information**

3.1 "Confidential Information" means, without limitation, (a) Corero's product price lists, non-public technical information and documentation marked as "confidential."; (b) the terms and conditions of this Agreement and the Exhibits; (c) any information about Customer's business, or operations, including without limitation about the design, operation, architecture, software, devices or procedures of any Customer network; (d) any data stored on or transiting on, to or from Customer's network (including without limitation, computers, servers, routers, switches or any other interconnected device) and (e) any data about or identifying any individual, whether customer or employee (past, present or prospective) or his/her interactions with Customer, including without limitation usage information, payment and financial information (data defined by subsections (d) and (e), above shall be collectively "Network Data"). Confidential Information shall not include any information that (a) is or becomes a part of the public domain through no act or omission or breach of this Agreement by Customer, (b) was in Customer's lawful possession prior to disclosure as shown by its written records, (c) is lawfully disclosed to Customer by a third party without restriction on disclosure, or (d) is independently developed by the Customer without use of the Confidential Information.

3.2 Neither party shall disclose any of the other party's Confidential Information to any person, or permit any person to use, examine or reproduce Confidential Information, unless such Confidential Information has become public knowledge through means other than breach of this Agreement, without the prior written consent of the other party. Each party shall exercise at least the same degree of care to protect the confidentiality of the other party's Confidential Information which it exercises to protect the confidentiality of its own similar confidential information, but in no event less than reasonable care or less than those measures required by applicable law.

3.3. Injunctive Relief. Each party acknowledges that any violation of the provisions of this Agreement may result in irreparable harm to the other party and that such other

party may have no adequate remedy at law. The parties agree that in addition to a right to terminate this Agreement upon a breach of confidentiality each party shall have the right to seek equitable relief by the way of injunction to restrain such violation and to such further relief it may be entitled at law or in equity.

3.4 Survival. The provisions of this Section 6 shall survive termination or expiration of this Agreement.

4. **Warranties**

4.1 Corero warrants that the Services shall be provided in a professional and workmanlike manner, in accordance with the description provided herein.

4.2 TO THE MAXIMUM EXTENT PREMITTED BY APPLICABLE LAW, EXCEPT AS SET FORTH IN THIS AGREEMENT, CORERO DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

NEITHER THIS AGREEMENT NOR ANY DOCUMENTATION FURNISHED UNDER IT IS INTENDED TO GUARANTEE OR IMPLY THAT THE OPERATION OF THE SERVICES (i) WILL BE UNINTERRUPTED, TIMELY, OR ERROR-FREE OR THAT THE EQUIPMENT WILL PROTECT AGAINST ALL POSSIBLE THREATS OR ATTACKS, (ii) SECURITY THREATS, MALICIOUS CODE AND/OR VULNERABILITIES WILL BE IDENTIFIED AND BLOCKED, (iii) THE OPERATION OF THE SERVICES WILL RENDER CUSTOMER'S NETWORK AND SYSTEMS SAFE FROM MALICIOUS CODE, INTRUSIONS OR OTHER SECURITY BREACHES, (iv) THERE WILL BE NO FALSE POSITIVES.

THE LIMITED WARRANTY SET FORTH IN THIS WARRANTY AGREEMENT GIVES THE CUSTOMER SPECIFIC LEGAL RIGHTS. THE CUSTOMER MAY HAVE OTHER RIGHTS UNDER APPLICABLE LAW, WHICH MAY VARY DEPENDING ON THE CUSTOMER LOCATION. NO DEALER, DISTRIBUTOR, AGENT OR EMPLOYEE OF CORERO IS AUTHORIZED TO CHANGE OR ADD TO THE WARRANTY AND REMEDIES SET FORTH HEREIN.

All warranties and representations contained in this Section 4 shall survive termination or expiration of this Agreement.

Other Limitations

5.1 EXCEPT FOR EACH PARTY'S INDEMNIFICATION OBLIGATIONS CONTAINED IN SECTION 5, HEREIN, IN NO EVENT (i) SHALL EITHER PARTY'S LIABILITY FOR ANY DAMAGES EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER TO CORERO HEREUNDER, DURING THE IMMEDIATELY PRECEDING TWELVE MONTH PERIOD, FOR THE SPECIFIC SERVICES WHICH CAUSED SUCH DAMAGE, OR (ii) SHALL EITHER PARTY OR ITS SUBCONTRACTORS OR ANY ENTITIES UNDER COMMON OWNERSHIP OR CONTROL WITH SUCH PARTY BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, SPECIAL OR INDIRECT DAMAGES (INCLUDING BUT NOT LIMITED TO LOST BUSINESS PROFITS AND LOSS, DAMAGE OR DESTRUCTION OF DATA), WHETHER THE CLAIM IS BASED ON CONTRACT, NEGLIGENCE OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF THE SAME.

5.2 Customer acknowledges that the information, data and other analysis ("Data") provided by Corero as part of the Services is intended for use only with and as part of the Services. Such Data is not warranted for use for any other purpose or to be error free. If Customer uses the Data for any other purposes, Customer will indemnify, defend and hold Corero, its affiliates and their respective directors, officers, employees, agents and representatives, harmless from and against any and all third party claims, suits, actions, proceedings, damages, costs, liabilities, losses, and expenses (including, but not limited to, reasonable attorneys' fees) arising out of or relating to any such use, including but not limited to, reliance on any such Data for claims or actions against any third parties.

5.3 Customer acknowledges that Corero has set its prices and entered into this Agreement in reliance upon the limitations of liability and the disclaimers of warranties and damages set forth above, and that the same form an essential basis of the bargain between Customer and Corero. Customer and Corero agree that the limitations and exclusions of liability and disclaimers specified in this Agreement will survive and apply even if found to have failed of their essential purpose.

5.4 All limitations contained in this Section 5 shall survive termination or expiration of this Agreement.

Other General Terms

6.1 Except with regard to Customer payment obligations, neither party shall be deemed in breach hereunder for any cessation, interruption or delay in the performance of its obligations due to causes beyond its reasonable control, including, without limitation, earthquake, flood, or other catastrophic natural disaster, act of God, labor controversy, civil disturbance, terrorism, war or the inability to obtain sufficient supplies, transportation, or other essential service required in the conduct of its business, or any change in or the adoption of any law, regulation, judgment or decree (each a "Force Majeure Event"); provided that, (a) the non-performing party gives prompt written notice thereof to the other; and (b) the non-performing party takes all reasonable steps to mitigate the effects of the Force Majeure Event. If a Force Majeure Event that affects a party's ability to perform continues for more

than thirty (30) days, the other party may elect to terminate this Agreement.

6.2 Failure by either party to enforce any term of this Agreement shall not be deemed a waiver of future enforcement of that or any term. The provisions of these Terms and Conditions are severable. If any provision of these Terms and Conditions is held to be unenforceable or invalid, the remaining provisions shall be given full effect, and the parties agree to negotiate, in good faith, a substitute valid provision that most nearly approximates the parties' intent unless such provision goes to the essence of the agreement, in which case this Agreement may be terminated.

6.3 This Agreement makes up the complete and exclusive agreement for the supply of Services and supersedes and replaces all prior or contemporaneous representations, understandings or agreements, written or oral, regarding such subject matter, and prevails over any conflicting and/or additional terms or conditions contained on printed forms such as purchase orders, sales acknowledgments or quotations. Only a written instrument signed by authorized representatives of Customer and Corero may modify this Agreement.

6.4 Corero reserves the right to assign any service obligation to its Authorized Partner or subsidiaries and to subcontract any of its obligations under this Agreement, but Corero will remain primarily liable for such assigned or subcontracted performance and compliance with this Agreement. Notwithstanding the foregoing, no such consent is required if either party assigns this Agreement in connection with a merger, acquisition, or sale of all or substantially all of its assets to any third party who assumes the obligations of this Agreement. Notwithstanding the foregoing, consent shall be required if a party attempts to assign this Agreement, whether through merger, acquisition or sale of all of substantially all of its assets or otherwise, to a direct competitor of the non-assigning party.

6.5 It is acknowledged and agreed that Corero's relationship with Customer is at all times hereunder an independent contractor. Corero shall have no authority to act on behalf of, or legally bind the Customer, and Corero shall not hold itself out as having any such authority. This Agreement shall not be construed as creating a partnership or joint venture.

6.6 All notices under this Agreement shall be in writing and shall be sent to the parties at their respective addresses listed on the first page of this Agreement. Notices will be deemed given when: (i) delivered personally; (ii) sent by confirmed fax; (iii) five (5) days after having been sent by registered or certified mail, return receipt requested, postage prepaid; or (iv) one (1) day after deposit with a commercial overnight carrier, with written verification of receipt.

6.7 During the Term and for twelve months thereafter, neither party shall solicit, induce, recruit or encourage any person employed by the other or engaged by the other to assist with performance hereunder to terminate his or her employment or engagement with such party and shall not hire such individual as an employee or independent contractor. The foregoing restriction shall not apply to any employee who applies for a post with the other party which is advertised online or in any other manner provided that the employee in question has not been approached by the other party prior to that employee making such application.

6.8 If the Corero entity that is a party to this Agreement in Corero Network Security Inc., then this Agreement shall be governed by and construed in accordance with the substantive laws of the Commonwealth of Massachusetts excluding choice-of-law provisions thereof that would mandate application of the laws of any other State. If the Corero entity is Corero Network Security (UK) Ltd, then this Agreement shall be governed by and construed in accordance with the laws of England and Wales.

6.9 Arbitration. Any dispute, controversy, or claim arising out of, relating to, involving, or having any connection with this Agreement, including any question regarding the validity, interpretation, scope, performance, or enforceability of this dispute resolution provision, shall be exclusively and finally settled by binding and confidential arbitration in accordance with the International Arbitration Rules of the International Centre for Dispute Resolution (the "ICDR Rules"). The arbitration will be conducted in the English language and the place of the arbitration shall be either Boston, Massachusetts (for contracts under Massachusetts law) or London, England (for contracts under English law). The arbitration will be conducted by three arbitrators. Each Party will appoint an arbitrator, obtain its appointee's acceptance of such appointment, and deliver written notification of such appointment and acceptance to the other Party within 15 days after the due date of the respondent's answering statement. The two Party-appointed arbitrators will, within 30 days of their own appointment, jointly agree upon and appoint a third arbitrator who will serve as the chairperson of the arbitral panel. Absent agreement by the two party-appointed arbitrators on a third arbitrator within that 30-day time period, the chairperson shall be selected by the ICDR in accordance with the ICDR Rules. All decisions, rulings, and awards of the arbitral panel will be made pursuant to majority vote of the three arbitrators. The award will be in accordance with the applicable law, will be in writing, and will state the reasons upon which it is based. The arbitrators will have no power to modify or abridge the terms of this Agreement. The award of the arbitrators will be final, and judgment on the award may be entered and enforced in any court having jurisdiction to do so.

6.10 Legal Actions. Nothing in this Section will prevent either party from seeking interim injunctive relief against the other party in the courts having jurisdiction over the other party. Each party hereby unconditionally submit to the exclusive jurisdiction of the United States federal courts in Boston, Massachusetts or London, England, respectively, for all matters related to the enforcement of any arbitral

award and legal actions seeking injunctive relief. The application of the United Nations Convention of Contracts for the Sale of Goods is expressly excluded.

Exhibit A
SecureWatch Data Collection, Storage and Access Guide

Introduction
SecureWatch is a suite of subscription-based security services to provide additional support to maximize the effectiveness of Corero security solutions in protecting customer infrastructure and data.

Within the context and scope of the SecureWatch service delivery, Corero requires access to the installed SmartWall Solution 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 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 the SmartWall Solution providing automated administration and response where required. The service is restricted to monitoring Corero products only including software and where applicable hardware components (collectively the "SmartWall Solution").

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 SmartWall Solution 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 System Health Information:** Summarized Network Traffic Metadata and Security Events generated by the SmartWall Solution are collected to provide customer Dashboards, Alerting and Reporting. This information includes Security Messages, Network Messages, Top-Type Metadata messages, System Messages and sampled sFlow sample messages.

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

- **System Health information:** The SmartWall Solution Health information is collected to provide forensic backup information during the analysis of customer incidents. This information includes VM CPU and memory usage.

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 System Health Information:** The customer sensitive data is all stored locally at the customer location. 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.

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

Connecting the SmartWall Solution to the Corero SOC

The SecureWatch Service requires a secure connection between the SmartWall Solution and the monitoring systems in Corero's primary and backup secure colocation facilities. The SmartWall Solution 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 Customer's SmartWall Solution.

Change Control

Changes to customer policies are 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.

Exhibit B
Corero Product 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 products including software and where applicable hardware components ("Products"), and the Customer locations ("Location"). The following form, defines the Products and Locations covered by the Service purchased.

Note: The SecureWatch Managed Service is not available for and does not cover the Corero SmartWall Service Portal software.

Corero Product Model	Serial Number for hardware CMS UUID for virtual software instances	Location
1)		
2)		
3)		
4)		
5)		
6)		
7)		
8)		
9)		
10)		
11)		
12)		
13)		
14)		
15)		
16)		
17)		
18)		
19)		
20)		