Corero Network Security:
General Data Privacy Statement

If you reside in the European Economic Area (EEA) and are either personally a customer, prospect, supplier, service provider, agent or other business partner, or a representative of a corporate business partner, of Corero Network Security plc. or any of its group affiliates (collectively, "Corero Network Security" or "we"), this privacy notice is issued to you by Corero Network Security as Data Processor.

For a full list of Corero Network Security company details and contact information, please visit www.corero.com/contact/

Data Categories Collected And Purposes Of Processing

You may provide to us, or we may collect about you, contact information (name, business address, email address and work phone number), professional information, data related to purchasing and interactions, and data concerning related IT support and technology requests. We process this data to be able to do business with you and contact you about business opportunities. Any data that you do not provide to us directly is either collected from publicly available sources such as company websites or professional networking sites or provided by another business professional in your field.

Legal Bases For Processing

We process your personal data on several different legal bases, as follows:

Based on necessity to perform contracts with you (for instance, based on Art. 6(1)(b) of the European Union General Data Protection Regulation ("GDPR")): We need to process your personal data to fulfill sample requests and orders, answer questions and requests from you, and provide customer support.

Based on legitimate interests (for instance, based on Art. 6(1)(f) of the GDPR): We process personal data from you for security and safety; to detect and prevent fraud; to protect and defend the rights or property of others, or our own rights and interests; we consider your privacy interests in this regard and redact personal information to the largest extent practicable to avoid affecting your privacy rights.

Based on compliance with legal obligations (for instance, based on Art. 6(1)(c) of the GDPR): We may need to process your personal data to comply with relevant laws, regulatory requirements and to respond to lawful requests, court orders, and legal processes.

Where required by applicable law, based on your consent (for instance, based on Art. 6(1)(a) of the GDPR): If you consent to receiving marketing communications, we may send you marketing communications on the basis of such consent.

Your Rights And Choices

You can contact us at any time to request copies of your personal data. Subject to the applicable statutory prerequisites, you can also ask us to correct or archive/erase your personal data or request your personal data to be made available according to portability requirements. You can exercise these rights by contacting us at dataprivacy@corero.com. You also have the right to lodge a complaint with a supervisory authority. Having a business relationship with us is voluntary, but it may not be possible to work with you without processing some personal data about you such as your contact information.

Processing And Storage Of Personal Data

We and our group affiliates and service providers process and store your personal data on servers in the secure colocation facilities, in accordance with the provisions of regulations laid out by the European Commission. We provide adequate protection for your personal data by having entered into data processing agreements and data transfer agreements that include standard contractual clauses approved by the European Commission. Such data processing agreements and data transfer agreement are available upon request by contacting dataprivacy@corero.com.

Data Retention

We retain your personal data as long as you have a business relationship with us and for 5 years thereafter, subject to applicable laws.

Data Protection Officer

Where applicable to Corero Network Security, the the data protection officer can be contacted on dataprivacy@corero.com and the data protection representative is shown below.

Data Protection Representative

In accordance with Article 27 of the European Union General Data Protection Regulation ("GDPR"), Corero Network Security has designated the following as its initial representative related to the GDPR:

Corero Network Security (UK) Ltd
St Mary's Court,
The Broadway,
Amersham, Buckinghamshire, HP7 0UT, UK

Corero Network Security:
Data Privacy and Our Website

Corero Network Security plc. or any of its group affiliates (collectively, "Corero Network Security" or "we"), provide this Privacy Policy to inform you regarding the collection, use and disclosure of personal data that we receive from you when you visit and user this website located at www.corero.com and other web pages that directly link to this Privacy Policy (collectively "Site").

Please note that this Privacy Policy only applies to this Site. This Privacy Policy is subject to change and may be modified from time to time for any reason. We will notify you of any material changes to our Privacy Policy, for example, by posting the new Privacy Policy on our Site. You are advised to consult this Privacy Policy for any changes.

Information That You Provide

You may visit the Site without registering or actively submitting personal data to us. If you do not register, then we receive only information that your computer or other device sends to us in connection with access requests and via cookies and other technologies that we use to analyze and enhance your use of our Site.

There are certain services we offer, however, which require the submission of personally identifiable information, such as your first name, last name, email address, phone number, country, company name, and industry. If you contact us by email through the Site, we may keep a record of your contact information and correspondence, and may use your email address, and any information that you provide to us in your message, to respond to you. We also may use your personally identifiable information to send you other publications or information about our products that may be of interest to you. In addition, we may send you important administrative information regarding the Site and/or services we offer via the Site. If you decide at any time that you no longer wish to receive communications from us, please send an email to dataprivacy@corero.com to unsubscribe or opt-out. Every correspondence we send externally provides the ability for the recipient to opt-out of any further communications, which in turns updates our system and removes you from future correspondence, until you opt back in.
If you purchase services or register for an event, we may also require you to provide with financial qualification and billing information, such as billing name and address and the number of employees within the organization that will be using the services.

If you apply for a job, we may also require you to submit additional personal information as well as a resume or curriculum vitae.

Tracking Technologies

When you visit the Site, our servers automatically record information that your browser sends whenever you visit a website. Log data may include information such as your IP address, browser type or the domain from which you are visiting as Internet domain and host names; operating system types; clickstream patterns; and dates and times that our site is accessed. For most users accessing the Internet from an Internet service provider, the IP address will be different every time you log on. We use it to monitor use of the Site and the services we offer via the Site and for the Site's technical administration.

Like the vast majority of websites, we also use "cookie" technology to collect additional website usage data and to improve the Site and the services we offer via the Site. A cookie is a small data file that we transfer to your computer's hard disk. We do not use cookies to collect names or contact information. However, IP addresses are collected by the use of cookies. We mainly use "session cookies", which enable certain features of the Site and services we offer via the Site, to better understand how you interact with the Site and services we offer via the Site, to monitor aggregate usage by our users and web traffic routing on the Site, and to improve the Site and services we offer via the Site. This session cookie is deleted from your computer when you disconnect from or leave the Site. Most Internet browsers automatically accept cookies. You can instruct your browser, by editing its options, to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit.

We do not recognize or take action in response to Do-Not-Track (DNT) signals from Web browsers. At this time there is not any universally accepted standard for a company's adoption for how to respond when a DNT signal is detected. In the event a final standard is established, we will determine how to appropriately respond to these signals.

Use of Personal Data

We use your information to operate, evaluate and improve our Site and business (including developing new products and services; enhancing and improving our services; managing our communications; and analyzing our products) and to communicate

with you and respond to your requests. We also use personal data about Corero Network Security event attendees to plan and host corporate events, host online forums and social networks in which event attendees may participate.

Sharing of Personal Data

We disclose your personal information only as follows:

- With your consent.
- We use affiliated and unaffiliated service providers all over the world that help us deliver our service and run our business subject to confidentiality agreements.
- We share aggregated usage statistics that cannot be used to identify you individually.
- We will disclose data as required by law or to protect you, other users, us or third parties from harm, including fraud, data security breaches or where someone's physical safety seems at risk.
- In a reorganization or sale of our company or assets, your data may be transferred, subject to the acquirer accepting the commitments made in this Privacy Policy and compliance with applicable law.

Data Security

Corero Network Security employs robust administrative, physical and electronic measures designed to protect your information from unauthorized access.

Information Storage and International Transfers

We and our service providers process and store your personal information on servers around the world, including in our secure colocation facilities.

Links to Other Sites

Our Site may contain links to other websites including those of our clients. If you choose to visit an advertiser by "clicking on" a link or other type of advertisement, you will be directed to that third party's website. The fact that we link to a website is not an endorsement, authorization or representation of our affiliation with that third party. We do not exercise control over third party websites. These other websites may place their own cookies or other files on your computer, collect data or solicit personal information from you. This Privacy Policy addresses the use and disclosure of information that we collect from you through this Site. Other sites follow different rules regarding the use or disclosure of the personal information you submit to them. We encourage you to read the privacy policies or statements of the other websites you visit.

Corero Network Security:
Specific Data Privacy with regard to our Solutions:
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 Network Security solutions in protecting customer infrastructure and data.

Within the context and scope of the SecureWatch service delivery, Corero Network Security 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 Network Security 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 Network Security 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 Network Security 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, who collect only relevant data to secure qualify a valid license for operating our elements. 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 Network Security 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 Corero Network Security 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 Network Security'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 Network Security 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 Network Security 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.

Corero Network Security:
Specific Data Privacy with regard to Job Applicants

This Privacy Notice applies to all applicants based in the EU applying to Corero Network Security plc or any of its group affliates ("Corero Network Security") for work as employees, self-employed contractors or interns ("Job Applicants").

Corero Network Security takes its data protection obligations seriously and this notice explains how we will use your personal data and the measures we take to protect it.

The personal data we collect and where it comes from

If you make your application directly through our website then your application information will be processed using ApplicantPro, a tool provided by a third party based in the United States.

ApplicantPro will not pass information you provide specifically for a job with Corero Network Security on to anyone apart from us. ApplicantPro's privacy notice can be accessed through a link on the application form on our website.

If you make an application to Corero Network Security via a recruitment agency then in making the introduction that agency is acting as the data controller, determining what information we receive and how we may use it. You should make sure that you have read and understood the privacy notice and any terms of business that any recruitment agency you use applies.

During the application process we may collect additional information direct from you e.g. during interviews and from third party sources, such as referees and background checkers and from social media sites, for example, LinkedIn.

How we use your personal information

All the information that we collect will be used for the purposes of your application to work with Corero Network Security.

Who we share your personal information with

Internal sharing:

Corero Network Security shares all personal information that it collects with Corero Network Security, Inc ("Corero US"). Your information may be shared with other group companies, particularly Corero Group Services Limited, a company which is based in the UK. All group companies that we share personal information with are required to hold and use that data in accordance with the principles set out in this policy.

Any personal information that Corero Network Security collects about you may be shared with a limited number of employees and contractors who work for us on a confidential and "need to know" basis to take the recruitment process forward. Corero Network Security does not rely on automated decision making in its recruitment process.

External sharing:

Corero Network Security will not share any of your personal information outside of its corporate group without your express consent. If you progress through the recruitment process you may be asked to provide additional information to third party providers who provide services to Corero Network Security such as employee background checking. We will also collect and use such additional information about you as these third parties may provide to assist it with the recruitment decision making process. This may include information such as credit checks, right to work checks, confirmation of academic qualifications, references and criminal record checks. All of Corero Network Security's suppliers are under contractual obligations to use your personal data only for the purpose for which you have supplied it and to hold it in accordance with all applicable data protection laws.

Please note that if you sign up for job alerts using the form that also appears on the application page on our website then you will be supplying your data to a third party, ApplicantPro, whose privacy notice is available through a link on our website. You are not required to sign up for job alerts when making an application to Corero Network Security and Corero Network Security accepts no liability in respect of the processing of any data that you supply to ApplicantPro or any other third party.

Transferring your personal information outside the EEA

When personal information is being transferred outside the European Economic Area (EEA) we are under an obligation to ensure that such transfer is performed in a manner that ensures that your personal information is adequately protected.

Transfers to Corero Network Security US: Your personal information will be transferred to Corero Network Security US. We have entered a binding agreement with Corero Network Security US to ensure that it stores and uses your personal data in accordance with your rights under this policy.

Any data that you upload via our web-based recruitment tool will be held on secure servers in the United States managed by our third-party supplier ApplicantPro. Under the terms of our agreement with this supplier your data can only be used for the purposes that we specify, which will be in accordance with the terms of this notice.

Security

We are committed to ensuring that your personal information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the personal information we collect. However, please note that no transfer of personal information over the internet is ever completely secure. Consequently, we cannot guarantee the security of any personal information which you transfer to us, or which we transfer to you, over the internet.

How long we retain your personal information for

If your application is successful and you are engaged to work for Corero Network Security in the UK or EU then the personal data gathered during the recruitment process will continue to be held by Corero Network Security in accordance with its GDPR Policy for UK and EU Employees, Contractors and Interns, which will be supplied to you on joining. If your application is not successful then unless Corero Network Security has a legitimate reason to continue to hold your personal data your details will be held for six (6) months after the closure of the recruitment process for the job you applied for and then will be permanently deleted or destroyed.

Legal information

For the purposes of data protection law, the entity responsible for deciding how personal information within the scope of this policy is collected, stored and used ("data controller") is: Corero Network Security (UK) Limited ('Corero Network Security UK'), a company registered in England and Wales with company number 04047090, whose registered address is St Mary's Court, The Broadway, Amersham, Buckinghamshire, HP7 0UT, UK.

The person within Corero Network Security UK who is responsible for data privacy issues is the data controller. Any questions regarding this policy can be sent to him at dataprivacy@corero.com.

The lawful basis that Corero Network Security relies on for processing your data is to explore the possibility of employing you ("contract"); its own legitimate interest in hiring the best people for its business and defend itself from claims ("legitimate interests") and to fulfill its legal obligations ("legal obligation").

You have the right to request access to any personal data that we hold about you and to request its transfer to a third party. In certain circumstances you may also have the right to have your personal data rectified, erased or have its processing by us restricted, or to object to our processing your personal data at all. Where our processing is based on your consent you also have the right to withdraw your consent and unless we can rely on another legitimate basis processing will cease.