

Privacy Notice for Customers

Last Updated: February 01, 2022

Purpose

Arctic Wolf Networks, Inc. (“AWN,” “Arctic Wolf”) is a corporation located at 8939 Columbine Road, Suite 150, Eden Prairie, MN 55347. Arctic Wolf and its affiliates (“we,” “us,” “our,” or the “Company”) describe in this Privacy Notice (the “notice”, “Privacy Notice”) our processing practices with respect to your data (“Customer Information” as defined below) provided by you and your authorized resources (“Users”, “you”, “your”) to use and while using the Arctic Wolf solutions (collectively, “Solutions”). For purposes of clarity, MSP Partners (“MSP,” “MSPs”) using the Solutions on behalf of its end-users are considered Users for the purposes of this Privacy Notice.

This Privacy Notice describes the Customer Information (as defined below) we collect in the delivery of the Solutions and the manner in which the Customer Information is used to deliver and support your use of the Solutions.

Terms of Use

If you have any dispute over the privacy of your information, the dispute is subject to this Privacy Notice and, as applicable, the Solutions Agreement or Partner Agreement made between us, including any provisions related to the limitation of liability and application of choice of law.

Scope

This Privacy Notice covers the Customer Information collected by us from Users of the Portals and Solutions and the access to and submission of Customer Information for the purpose of:

- Opening tickets
- Adding comments to existing tickets
- Adding attachment(s) to tickets
- Being authenticated to use the Solutions
- Uploading credentials for application event monitoring
- Obtaining configuration information, reports, and metrics related to the operation of the Solutions within your environment
- Supporting our business operations

Customer Information

Each User is responsible for the quality, integrity, reliability, and appropriateness of Customer Information submitted to us and in the Solutions and must comply with terms contained in the applicable Solutions Agreement or, in the case of certain MSPs, by the terms of the applicable Partner Agreement. The information we may collect from you while using the Solutions includes:

1) Point of Contact Information

Points of Contact may be contacted by Arctic Wolf to deliver the Solutions. Points of Contact data will be collected by Arctic Wolf during various phases of Solutions delivery and throughout the life of the subscription. Points of Contact data may include the following data: first name, last name, corporate email address, phone number, job title, address, and organization hierarchy.

2) Solutions Data

The Solutions, depending on their set up and deployment in your environment, may collect log data from various sources, including your:

- data center,
- applications,
- infrastructure in the cloud,
- on-premises infrastructure, and
- remote endpoints.

In addition, the Solutions may perform inspection of network traffic, scan internal and external-facing devices, and collect configuration data, vulnerability data, system-level inventory, and event data. Solutions Data received from these sources may include operational system log data and any other information provided by you in furtherance of your use of the Solutions and which you may elect to submit to Company through the Solutions, including, but not limited to operational values, event logs, and network data such as flow, HTTPS, TLS, DNS metadata, cursory inventory data, operating systems and versions, users and groups from Active Directory, system level inventory, event data, and network vulnerability data. Personal data included in the Solutions Data may include: first name, last name, IP (Internet Protocol) Addresses, geolocation, usernames, passwords, and email addresses. Arctic Wolf does not require any special categories of data to deliver the Solutions.

Point of Contact Information and Solutions Data are collectively referred to herein as “Customer Information”.

How We Use the Customer Information

We use Customer Information for the following purposes:

1) Support Ticket Management and Resolution

Support tickets are the primary medium that Users and the Security Services organization, including your Concierge Security™ team (CSTs) use to provide support to you. Point of Contact Information is used to communicate issues or requests over the use and improvement of the Solutions. Both parties can comment and provide more information in a support ticket until the issue/request is resolved. The CSTs use a ticketing system to communicate security alerts to Users allowing the Users to respond and see the status of the alert until it is closed.

2) Provision of the Solutions

Customer Information is integral to the functionality of our Solutions and is used to provision the Solutions. Solutions Data allows us to monitor and detect security and threat incidents within your network of connected applications and systems. Point of Contact Information can be viewed and managed by Users, including your MSP, if applicable, and may be accessed and viewed by Company employees for support ticket issue resolution. Based on your environment and configuration, the Customer Information allows for the following:

- configuration of the Solutions, and monitoring of cloud infrastructure resources to detect access and misuse of a User's networks, resources, and application instances;
- monitoring of SaaS applications to detect malicious activities and potential data exposures in cloud-based applications;
- monitoring of security events related to user single sign-on and malicious endpoint activity for security providers;
- accessing learning content and other resources available to you through the Solutions; and
- conducting trainings and preparing metrics related to your Users' activities within the Solutions.

3) Communication With You

Company may use your Point of Contact Information to manage its ongoing business activities such as billing, account management, and value-add communications such as generic threat intelligence briefings and additional Arctic Wolf product and marketing communications, updating you about changes to our terms and conditions, sending you general information about Company and its business, or other similar types of business purposes.

4) Improve the Solutions

Company may aggregate and anonymize your Solutions Data to create our own intellectual property. Such aggregated/anonymized data is owned by us and may be used to improve the Solutions, as well as for any other business purpose.

How We May Share the Customer Information

We may share Customer Information as expressly permitted in writing by the User or as required or permitted by law.

We may share Customer Information only in the manner described below. We do not control, however, how you or your third party service providers, collect, use, share or disclose Customer Information.

We may share or disclose Customer Information in the following ways:

- **When changing our business structure**

In the event of a proposed or completed merger, acquisition, bankruptcy, dissolution, reorganization, sale of some or all of our assets, similar transactions or proceedings, or steps in contemplation of such activities, Customer Information held by us may be among the assets transferred to the buyer or acquirer;

- **When conducting our business operations**

We may use third party service providers and tools to provide services on our behalf, including billing, customer ticketing and collaboration, internal support ticketing, access and identity management, cloud hosting, customer relations management, Solution improvement projects, etc. Our service providers are only provided with information they need to perform their designated functions and are not authorized to use or disclose information for their own marketing or other purposes. Our service providers may be located in the U.S., Canada or other foreign jurisdictions;

- **To conduct our joint sales or product promotion activities**

We may engage in joint sales or product promotions with select business partners and share your Point of Contact Information with those partners for purposes of participating in sales activities, marketing our products and services, and attending, hosting or sponsoring sales events;

- **To comply with laws**

We and our affiliates or service providers in the U.S. or other jurisdictions may disclose Customer Information to comply with applicable legal or regulatory requirements (which may include lawful access by U.S. or foreign courts, law enforcement or other government authorities) and to respond to lawful requests by public authorities, including to meet national security, law enforcement requirements, court orders and legal processes;

- **To protect rights and safety**

To protect and defend the brand, rights, property and safety of Company, our customers, including enforcing contracts or policies, or in connection with investigating and preventing fraud.

If Users have any questions about its Customer Information or rights with respect to the foregoing, please submit a request at [Data Protection](#) or open a ticket via the Solution.

Security

Company maintains administrative, physical, and technical safeguards to help protect the confidentiality and integrity of Customer Information that is submitted to us during transmission and once it is received. You should note that by submitting data through our Solutions, your Customer Information will be transferred through third-party infrastructures which are not under our control. We will strive to use tools and procedures to protect your Customer Information, however we cannot guarantee its absolute security. Customer is responsible for protecting themselves against unauthorized access to passwords, private keys and computers, and unauthorized disclosure, alteration, and destruction of Customer Information and timely provisioning and deprovisioning of Users.

Location of Customer Information

Arctic Wolf is headquartered in the United States. Arctic Wolf has affiliates, operations and service providers in the United States and throughout the world. We and our service providers may transfer your Customer Information to, or access it from, countries other than the one in which you are located. These countries may have data protection laws different from those of the country which you are located. We will maintain administrative, physical, and technical safeguards to protect the Customer Information for instance by entering into agreements such as standard contractual clauses approved by an applicable regulator. See European Privacy Supplement below for additional information.

EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Notice

Arctic Wolf complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States but does not rely on such programs to overcome restrictions on the international transfer of personal data. Arctic Wolf has certified to the Department of Commerce that it adheres to these Privacy Shield Principles. Arctic Wolf may process some personal data from individuals or companies via other compliance mechanisms, including data processing agreements based on the EU Standard Contractual Clauses. To learn more about the Privacy Shield program and view our certification, visit the U.S. Department of Commerce's Privacy Shield site at [Privacy Shield](#).

Arctic Wolf is responsible for the processing of the personal data it receives under each Privacy Shield Framework and subsequently transfers to a third party acting as an agent on its behalf. Arctic Wolf complies with the Privacy Shield Principles for all onward transfers of personal data from the EU, Switzerland and United Kingdom, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Arctic Wolf is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we are required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the Privacy Shield Principles, Arctic Wolf commits to resolve complaints about our collection or use of your personal data. EU, Swiss, and UK individuals with inquiries or complaints regarding our Privacy Notice should submit a request at [Data Protection](#) or you may also call +1 (888) 286-6726.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at <https://www.jamsadr.com/eu-us-privacy-shield>.

Under certain conditions, more fully described on the Privacy Shield website, you may be entitled to invoke binding arbitration by going to [Submitting a Complaint](#) on the Privacy Shield website when other dispute resolution procedures have been exhausted.

Supplemental Privacy Policy Terms

Canada

- **Consent**

By using our Solutions, or otherwise interacting with us, you consent to the collection, use and disclosure of Customer Information in accordance with the terms of and for the purposes set out in this Privacy Notice. Arctic Wolf may seek consent to use and disclose Customer Information after it has been collected in those cases where we wish to use the information for a new or different purpose, where consent as not already been obtained for such use or disclosure.

If you submit personal information about an individual (i.e., your employees, personnel, account administrators, authorized resources, etc.) in connection with the use of of the Solutions, you represent that you have obtained the requisite consent and/or provided appropriate notifications, as required under applicable privacy laws, including such consent and/or notifications as may be required for the transfer of personal information outside of Canada.

- **Privacy Rights**

Subject to limited exceptions under applicable law, Users may have the right to access, update and correct inaccuracies on their Customer Information. To exercise these rights, please submit a request at [Data Protection](#) or you may also call +1 (888) 286-6726. Please be as specific as possible in relation to the Customer Information you wish to access. Once Arctic Wolf receives your request, Arctic Wolf will review it, determine whether Arctic Wolf

can verify your identity, and process the request accordingly. If Arctic Wolf needs additional information to verify your identity, Arctic Wolf will let you know.

Please be advised that in the delivery of the Solutions to you, Arctic Wolf acts as data processor/service provider to process personal information and do so on behalf of our Customer under the terms of a Solution Agreement, or in certain instances, a Partner Agreement, and the information you have requested therefore is under the control of such Customer. Accordingly, we will direct your request for access, withdrawal of consent, data deletion, or all such other related inquiries to our Customer and will assist our Customer in its response to your request as per our Customer's instructions and in accordance with the terms of our agreement with them.

If you have any questions or complaints about our handling of Customer Information including personal information, or rights with respect to the foregoing, please submit a request at [Data Protection](#), and we will address your question or complaint, and otherwise further advise you of any rights you may have to complain to the relevant privacy commissioner(s).

California Consumer Privacy Act

The California Consumer Privacy Act ("CCPA"), which is effective as of January 1, 2020, regulates how Arctic Wolf handles personal information of California residents and gives California residents certain rights with respect to their personal information.

Arctic Wolf is a "service provider" under the CCPA. The following supplemental privacy policy applies to information Arctic Wolf collects in its role as a service provider. If you would like more information about how your personal information is processed by such other companies, including companies that engage Arctic Wolf as a service provider, please contact those companies directly.

This provision is effective as of January 1, 2020, shall apply only to residents of California, and may be subject to change. The general privacy policy shall continue to apply to the extent that it applies to you as a resident of California; however, if you are a resident of California, Arctic Wolf also is required to disclose certain uses and disclosures in a certain format, as well as to inform you of certain rights you may have. Any capitalized terms used in this supplemental privacy notice shall have the same meaning as in the general privacy notice.

Information Arctic Wolf May Collect:

We may collect the following categories of information:

- Point of Contact Information which may include the following data: first name, last name, corporate email address, phone number, job title, address, and organization hierarchy.
- Solutions Data may include: first name, last name, IP (Internet Protocol) Addresses, geolocation, usernames, passwords, and email addresses. Arctic Wolf does not require any special categories of data to deliver the Solutions.

For each category of information, Arctic Wolf collects the information from a variety of sources, including directly from you, from your devices, and/or from your third party providers. Arctic Wolf collects the information to:

- provide you with support on the Solutions,
- deliver the Solutions to you,
- protect Arctic Wolf (including the Solutions) and its customers,
- communicate with you regarding our Solutions and terms and conditions,
- conduct internal marketing activities, and
- improve our Solutions.

Arctic Wolf may share personal information with Third Parties as the term is defined under the CCPA.

Additional Disclosures:

Arctic Wolf engages certain trusted third parties to perform functions and provide services to us, including auditing, marketing, hosting and maintenance, error monitoring, debugging, performance monitoring, and other short term uses. We may share your Customer Information with these third parties, but only to the extent necessary to perform these functions and provide such services. We require these third parties to maintain the privacy and security of the Customer Information they process on our behalf.

Arctic Wolf has disclosed the following categories of personal information for business purposes and valuable consideration in the 12 months prior to this Privacy Notice’s last update:

A. Identifiers (names, email addresses, phone numbers, mailing address)	YES
B. Commercial Information (Solution information)	YES
F. Internet or Other Electronic Network Activity Information (IP address, device identifier, information provided in URL string, internet service provider, browser used, operating system and other device identifications and configurations, locale and language preference)	YES
Geolocation Data	YES

Do Not Sell My Personal Information:

Arctic Wolf does not sell, as defined under the CCPA, personal information of any individual, including personal information of minors under 16 years of age.

Your Rights:

You may have certain rights with respect to your personal information, including:

- The right to access, including the right to know the categories and specific pieces of personal information Arctic Wolf collects;
- The right to deletion of your personal information, subject to certain limitations under applicable law;
- The right to request disclosure of information collected;
- The right to disclosure of information disclosed for valuable consideration; and
- The right not to be discriminated against for exercising certain rights under California law.

To exercise these rights, please submit a request at [Data Protection](#) or you may also call +1 (888) 286-6726. Please be as specific as possible in relation to the personal information you wish to access. Once Arctic Wolf receives your request, Arctic Wolf will review it, determine whether Arctic Wolf can verify your identity, and process the request accordingly. If Arctic Wolf needs additional information to verify your identity, Arctic Wolf will let you know. Arctic Wolf will respond to your request within 45 days of receipt or notify you if Arctic Wolf requires additional time.

If you would prefer, you may designate an authorized agent to make a request on your behalf.

European Privacy Supplement

Arctic Wolf acts as a data processor in the delivery of the Solutions, and in limited circumstances as a data controller as it relates to Point of Contact Information. Accordingly, Arctic Wolf provides these additional and different disclosures about its data processing practices to data subjects in the EEA, Switzerland, and the UK (EEA+). If you are accessing the Solutions from within the EEA+, this European Privacy Supplement applies to you in addition to the Privacy Notice.

Legal Bases for the Processing.

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

- Based on necessity to perform contracts with you (see Article 6(1)(b) of the GDPR): When you access, use or register for our Solutions, you form a contract with Arctic Wolf based on the applicable Solutions Agreement. We need to process your personal data to discharge our obligations in any such contract, fulfill your requests and orders, answer questions and requests from you, and provide tailored customer support and search results to you.
- Based on compliance with legal obligations (see Article 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 process.
- With respect to Point of Contact Information where we are acting as a controller, based on our legitimate interests (see Article 6(1)(f) of the GDPR): We process your personal

data to send you invitations to relevant Arctic Wolf offerings (unless you have opted out), newsletters (unless you have opted out), invitations to relevant surveys (unless you have opted out), to understand which products and services may be relevant to you, and to improve our products, services and business practices.

Personal data we collect, as defined in the EU General Data Protection Regulation, may be stored and processed in the United States or any other country in which we or our service providers operate in. To the extent we transfer personal data out of the EEA+ to countries that do not benefit from an adequacy decision based on mechanisms such as approved Standard Contractual Clauses and other contractual measures to ensure that adequate safeguards are in place with respect to the personal data.

Changes to this Privacy Notice

We reserve the right to modify this Privacy Notice at any time in accordance with the terms of the Solutions Agreement or Partner Agreement, if applicable, we have in place with you. Updates to the Privacy Notice will be posted on the [Arctic Wolf Website](#) with an indication of when it has been updated. We encourage you to periodically review this Privacy Notice for any changes.

Additional Information

Questions regarding this Privacy Notice or about the manner in which we or our service providers treat your Customer Information can be directed to us by submitting a request at [Data Protection](#) or by regular mail or email addressed to:

Arctic Wolf Networks, Inc.
Attn: Legal Department
P.O. Box 46390
Eden Prairie, MN 55344 U.S.A.
legal@arcticwolf.com

Pursuant to Article 27 of the UK GDPR, Arctic Wolf Networks, Inc. has appointed EDPO UK Ltd as its GDPR representative in the UK. You can contact EDPO UK regarding matters pertaining to the UK GDPR:

- by using EDPO's online request form: <https://edpo.com/uk-gdpr-data-request/>
- by writing to EDPO UK at 8 Northumberland Avenue, London WC2N 5BY, United Kingdom

Pursuant to Article 27 of the EEA GDPR, Arctic Wolf Networks, Inc. has appointed IITR Cert GmbH as its GDPR representative in the EEA. You can contact IITR Cert GmbH regarding matters pertaining to the EEA GDPR:

- by writing to ITR Cert GmbH, Dr. Sebastian Kraska, Data Protection Representative, Eschenrieder Str 62c, 82194 Groebenzell, Germany
- by email to email@itr.de