WATCHGUARD NETWORK SECURITY
PRIVACY GUIDE

Last updated: July 2024

WatchGuard has created this Privacy Guide to provide our customers with important information about how we process personal information in connection with WatchGuard Network Security Services. Our Network Security Services include our Support license, Basic Security Suite, Total Security Suite, and services offered as a part of these solutions, including Firebox management and network configuration through the WatchGuard Cloud, WatchGuard Dimension, and WatchGuard System Manager.

This Privacy Guide does not describe how WatchGuard processes personal information in the context of any of its other products and services or broader WatchGuard business operations (e.g., across our websites, in the process of licensing, training, events, etc.).

For further information about how we process personal information in connection with our services, including WatchGuard Network Security Services, please consult our Privacy Policy and Data Processing Addendum. Our Trust Center also provides a one-stop-shop for everything privacy and security related.

OVERVIEW OF THE NETWORK SECURITY SERVICES

WatchGuard offers two tiers of network security services in addition to the standard Support license that comes with our Firebox appliances. The Basic Security Suite includes traditional intrusion prevention, antivirus, and URL filtering services. The Total Security Suite adds features like AI-powered malware protection, ThreatSync (XDR), and Cloud sandboxing. A more detailed description of these services can be found here.

WATHCHGUARD'S DATA PROCESSING ROLE

WatchGuard primarily acts as a service provider and a processor when providing Network Security Services to customers. This means we process personal information on behalf of our customers in accordance with their instructions. We may also process personal information on our own behalf for our business purposes as a controller, such as to administer and manage the customer relationship, to secure the services, or to make product improvements, including by means of statistical analysis of usage, log or telemetry data.

WHAT PERSONAL INFORMATION WE COLLECT AND WHY

The table below lists the personal information (or technical information that may potentially include or constitute personal information) collected by WatchGuard in connection with our Network Security Services and our processing purposes. Such information is usually provided directly by individual end users when they use Network Security Services or by the customer account administrator when they create and manage a WatchGuard account and configure services on behalf of the customer organization and its end users. We also collect certain information automatically in the process of providing Network Security Services.

Firebox administrators or WatchGuard Cloud Operators may be asked to provide additional personal information to manage Network Security Services on behalf of the customer organization.

Additionally, we automatically collect certain Service Data (described below) for troubleshooting, to ensure we comply with our legal obligations, and to ensure and improve the security of our services.

Service	Categories of Personal Information	Processing Purposes
Firebox/Fireware	Firebox serial number Firebox IP address Firebox geolocation data based on IP address Customer-assigned license keys Customer unique IDs such as WatchGuard Account IDs/Account Number Basic Device Feedback Advanced Device Feedback Firebox configuration data Fault Reports that may include Firebox model, firmware version, crash timestamp, traffic and event logs at the time of the crash, processed IP addresses, and Firebox configuration data Threat Telemetry (also known as “proxy reporting”) that may include source and destination IP addresses and PDF stats that include PDF names Authenticated user information (username) Service timestamps Additional data specific to the services as described below	Provide and operate the services Detect, analyze and mitigate threats and secure the services Improve and develop WatchGuard products and services Conduct analysis and reporting of product usage patterns and trends Provide customer technical support and troubleshooting Comply with legal obligations
Authentication Services	Username and password User authentication type (Firebox-DB, Radius, Active Directory, LDAP, SAML)	Provide and operate the services Provide customer technical support and troubleshooting
VPN	*For MUVPN:* - MUVPN End User IP address - Phase I and II settings (crypto, shared secrets, IP addresses) *For BOVPN:* - User email address - Certificate (if user imported the certificate) - Firebox version (if the peer is also a Firebox)	Provide and maintain VPN service Provide customer technical support and troubleshooting
Networking and SD-WAN	Network IP addresses PPPoE username and password End user information: - End user IP address - MAC addresses - Host names	Provide and maintain the service of WAN connection monitoring Increase application availability and performance Provide customer technical support and troubleshooting
Access Portal	SAML configuration Auth server IP addresses End user information: - Username and password - IP addresses - MAC addresses - User group info - Client OS type - User login/logout event - Names of applications used by end users	Provide and maintain the service by enabling secure remote access Provide customer technical support and troubleshooting
Intrusion	Source and destination IP addresses	Provide and maintain the service

Service	Categories of Personal Information	Processing Purposes
Prevention Service (IPS)	URLs accessed by end users	Detect, analyze and mitigate threats Provide customer technical support and troubleshooting
Application Control	Source and destination IP addresses Applications accessed by end users Application identification report: - Top Applications by User - Top Application by Host - Top Clients by Application Usage - Top Clients by Blocked Applications	Provide and maintain the service of network monitoring and control Detect, analyze and mitigate threats Provide customer technical support and troubleshooting
WebBlocker	URLs accessed by the end users End User username End User IP address Password set by Admin to override the service	Provide and maintain the service of Internet browsing control Provide customer technical support and troubleshooting
spamBlocker	Sender and recipient name, email address, IP address Content of the emails and attachments (processed by WatchGuard but stored in the quarantine server on customer's network)	Provide and maintain the service of spam message blocking Conduct data analysis and scoring Provide customer technical support and troubleshooting
Gateway AntiVirus	Files (and objects) that are scanned for known malware	Provide and maintain the service Detect, analyze and mitigate threats Provide customer technical support and troubleshooting
Reputation Enabled Defense	Source and destination IP address Geolocation (country specific) URLs accessed by end users	Provide and maintain the service by blocking specific sites after detecting the geographic locations of connections to and from customer's network Conduct data analysis and scoring of the websites for product improvement Provide customer technical support and troubleshooting
Network Discovery	Customer devices map End user information: Username (if the user is authenticated on the device) - Device IP address - Device host name - Device MAC address - Device Operating system and services - Device open network ports - Mobile compliance status if the devices are Mobile Security devices	Provide and maintain the service by discovering devices on customer's network and displaying discovered devices on a network map Provide customer technical support and troubleshooting
APT Blocker	End User IP address Files (or objects) that are scanned for malware and zero-day exploits (WatchGuard looks for links and attachments to the files. Only file signature (but not the file itself) is stored if there is a detection.)	Provide and maintain the service Detect, analyze and mitigate threats Improve and develop the product Provide customer technical support and troubleshooting
DNSWatch	Connection information including network protocol End user information: - Username	Provide and maintain the service Detect, analyze and mitigate threats Improve and develop the product to

Service	Categories of Personal Information	Processing Purposes
	- Email address - IP Address	improve efficacy of the service Provide customer technical support and troubleshooting
IntelligentAV	End User IP address [Files](#) (or objects) that are scanned for known and unknown malware	Provide and maintain the service Detect, analyze and mitigate threats Provide customer technical support and troubleshooting
ThreatSync (XDR)	End user information: - Username - IP address - Device data (such as hostname, MAC address, device identifiers) - Usage data (such as features used, number of users) - User-generated content (such as file paths and information contained in files) Other technical information that may potentially include personal information such as process IDs, process trees, file system events, windows registry events	Provide and maintain the service Detect, analyze and mitigate threats Improve and develop the product Provide customer technical support and troubleshooting
EDR Core	End user information: - Name (as part of paths and document names) - Username - Email address - IP address - Device data (such as hostname, MAC address, hardware details, device identifiers) - Visited URLs	Provide and maintain the service Detect, analyze and mitigate threats Improve and develop the product Provide customer technical support and troubleshooting
Data Loss Prevention	End user information: - Username - IP address - Data in customer files Service logs (which includes DLP rule/pattern that was matched and file name, but not the file or data within the file)	Provide and maintain the service Detect, analyze and mitigate threats Provide customer technical support and troubleshooting
Support	Any information provided by customer's administrator	Provide technical support as requested by the customer

Management System	Categories of Personal Information	Processing Purposes
WatchGuard Cloud (WGC)	**WGC Account Details:** Includes the following information of WGC Operators: - Full name - Email address - Username - IP address - Company name - Company telephone number - Access credentials **WGC Services Visibility Information:** Configurations, connections and logs that could include personal data of Customer's end users such as: - IP addresses for End Users - Username - File name	Provide and maintain the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting Comply with legal obligations

Management System	Categories of Personal Information	Processing Purposes
	- URLs and Apps used - URLs and Apps visited by a specific end user - Depending on configuration, end user actions and/or passwords **WGC Audit Logs:** WGC Operators Information: - Account ID/Account Number - Username - IP Address - Time/Date of access - Source (product interacted with) - Actions taken **Diagnostic Tools:** If Diagnostic Tools are used within WGC, TCP packets can contain any personal data processed as a part of network packets processed by the services.	
WatchGuard Dimension	Dimension Feedback: - Dimension IP address (ISP IP address) and geolocation - Linked Fireboxes serial numbers WatchGuard Dimension is installed and managed locally by the customer. WatchGuard has no access to services visibility data through WatchGuard Dimension unless the customer requests technical support and provides access.	Provide and maintain the service Detect, analyze and mitigate threats Analyze and report product usage patterns and trends Provide customer technical support and troubleshooting
WatchGuard System Manager	WatchGuard System Manager is installed and managed locally by the customer. WatchGuard has no access to services visibility data through WatchGuard System Manager unless the customer requests technical support and provides access.	Provide customer technical support and troubleshooting

SERVICE DATA COLLECTED BY WATCHGUARD

During our customers’ use of Network Security Products and Services, WatchGuard automatically collects certain device, log and usage data (we call this "**Service Data**") (further described below). This data is used by WatchGuard to provide, maintain and support the services, as well as for its own business purposes, such as to manage customer licenses, troubleshoot, improve, develop new products and services, comply with legal obligations such as export control rules, and conduct analysis and reporting of product usage patterns and trends.

Diagnostic application logs. WatchGuard collects application logs to diagnose and troubleshoot issues with the services, raised either by our systems or those of our customers, and to further improve our products and services. Information collected as a part of internal application logs may contain data that could be considered personal information such as WatchGuard account and user IDs, or IP addresses. We take steps to process this data in an anonymized form or where that is technically not possible, in a de-identified and aggregated form, and in all cases the data is secured at the level of production data. Collection of diagnostic application logs cannot be disabled.

Device feedback. Device feedback helps WatchGuard troubleshoot and secure our services, assess the threat landscape, and comply with our legal obligations such as export control rules. It is also used to improve our products and services. Device feedback can include information about how Firebox is used and issues our customers encounter with Fireboxes but does not include any information about our customers and their end users or any customer data that is sent through the Firebox. Because of this, device feedback mainly consists of technical information and may include only limited (if any) personal information such as the Firebox serial number, IP address, and country-level geolocation. The Firebox sends two types of device feedback data to WatchGuard: (1) Basic

Device Feedback, that is always ON and cannot be disabled, and (2) Advanced Device Feedback our customers can turn OFF by opting out. You can learn more about device feedback and how to opt out of Advanced Device Feedback collection here.

Threat telemetry (also known as "proxy reporting"). WatchGuard collects threat telemetry to investigate the threats and conduct analysis of current threat landscape. We then use anonymous aggregated data to show threat detection trends in WatchGuard quarterly Internet Security Report and our Cybersecurity Hub page. Threat telemetry may include incident reports that contain limited personal information such as source and destination IP addresses and PDF file stats that include PDF files names (but not the contents of the files). Threat telemetry is collected only if you are a customer using Gateway Antivirus, Intelligent AV, APT Blocker, IPS services and only if your organization has *not* opted out of Advanced Device Feedback collection (see above).

Fault reports. WatchGuard collects fault reports to troubleshoot errors and improve our products and services. Information included in the fault reports can contain Firebox serial number, model, firmware version, crash timestamp, traffic and event logs at the time of the crash, processed IP addresses, and Firebox configuration. Some of this information may include or constitute personal information. Fault reports are sent only if you check "Send Fault Reports to WatchGuard" box.

WatchGuard Cloud Usage Data. We use a tool called **Pendo** to provide in-app guides for our WatchGuard Cloud users (customers' WatchGuard Cloud operators) and to collect usage data, which is used to generate statistical analytical data to help us better diagnose user issues and improve the user experience. Pendo records and captures user events so that we can monitor user actions like mouse clicks, movements, actions taken within the console, time spent on different pages, and anonymized unique visitors. Data collected is processed in an aggregated and de-identified form. If WatchGuard Cloud operator rejects the cookies within WatchGuard Cloud, their data will not be collected but they will lose access to the in-app guides. We also use **Google Analytics** to collect limited usage data directly from user browsers to better understand your use of the WatchGuard Cloud Services to diagnose and fix issues and improve the services. If WatchGuard Cloud operator rejects the cookies within WatchGuard Cloud, their data will not be collected.

HOW WE KEEP PERSONAL INFORMATION SECURE

WatchGuard has implemented technical and organizational measures designed to secure personal information from accidental loss and unauthorized access, use, alteration, and disclosure. We maintain a robust security and privacy program that addresses the management of security. WatchGuard has obtained ISO/IEC 27001:2013 certification of its information security management system (ISMS). ISO 27001 is a globally recognized standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS. The details of the certification are publicly available at https://www.schellman.com/certificate-directory. WatchGuard's security approach includes policies, procedures, and controls with the objective of maintaining the security, confidentiality, integrity, and availability of information stored within WatchGuard systems and networks.

COOKIES AND SIMILAR TECHNOLOGIES

We use common information gathering tools, such as cookies, web beacons and similar technologies to automatically collect certain information when customers use WatchGuard Cloud, including WatchGuard Cloud Usage Data (described above). WatchGuard Cloud operators have the right to refuse or delete cookies deployed on WatchGuard Cloud. If WatchGuard Cloud operator wishes to refuse the use of cookies on WatchGuard Cloud, they can disable them within the platform cookie banner by clicking "Manage Cookies". For more information about cookies and similar technologies in WatchGuard Cloud, please visit our WatchGuard Cloud Service Cookie Notice.

For information on our use of information gathering tools on our websites, please refer to our main Privacy Policy and Cookie Policy.

PROCESSING LOCATIONS AND DATA TRANSFERS

Personal information we collect will be stored and processed in the customer's region, in the United States or in any other country where we or our affiliates, subsidiaries or service providers maintain facilities. Please view the list of WatchGuard sub-processors and affiliates [LINK] for more information.

Regardless of processing location, we take steps to process personal information in accordance with this Privacy Guide, WatchGuard Privacy Policy, our Data Processing Addendum and applicable privacy laws. To learn more, please refer to WatchGuard Data Transfers FAQs [LINK].

DATA SUBJECT RIGHTS

Where WatchGuard is the controller, end users and any other individuals whose personal information is processed by the Network Security Services have the right to request access, rectification, suspension of processing or deletion of personal information processed by the service. Further information about how they can do this in included in the "Your Privacy Rights" section within WatchGuard Privacy Policy.

Where WatchGuard processes personal information as a processor, acting on behalf of and at the direction of its customer, individuals are directed to the relevant controller (our customer).