WATCHGUARD ENDPOINT 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 Endpoint Security Services. WatchGuard Endpoint Security Services include WatchGuard EPP, EDR, EPDR, Advanced EPDR, as well as add-on security modules such as WatchGuard Patch Management, Full Encryption, Advanced Reporting Tool, and Data Control as described here.

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 Endpoint 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.

This Privacy Guide does not cover Email Protection and PCMS. If you have questions about these products, please reach out to privacy@watchguard.com.

OVERVIEW OF THE ENDPOINT SECURITY SERVICES

WatchGuard offers a layered approach to endpoint security through its WatchGuard Endpoint Security suite, delivered via WatchGuard Cloud for centralized management. The suite includes the WatchGuard Endpoint Protection Platform (EPP), a cloud-native solution providing next-generation antivirus protection for desktops, laptops, servers, and mobile devices (Android & iOS). The WatchGuard Endpoint Detection & Response (EDR) employs AI to detect and respond to advanced threats and zero-day attacks, complementing traditional antivirus solutions. The WatchGuard Endpoint Protection Detection & Response (EPDR) combines the strengths of EPP and EDR for comprehensive protection against known and unknown threats, including malwareless attacks. Advanced EPDR builds upon EPDR with additional features for security operations teams, enabling deep threat hunting and faster incident response. Add-on endpoint security modules include WatchGuard Patch Management, which simplifies patching vulnerabilities across endpoints, Full Encryption for sensitive data, an Advanced Reporting Tool offering detailed insights into security activities, and Data Control for restricting data transfer and preventing data loss. A more detailed description of these services and modules can be found here.

WATHCHGUARD’S DATA PROCESSING ROLE

WatchGuard primarily acts as a service provider and a processor when providing Endpoint 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 Endpoint Security Services and our processing purposes. Such information is usually provided directly by individual end users when they use Endpoint 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 Endpoint Security Services.

WatchGuard Cloud Operators may also be asked to provide additional personal information to manage Endpoint 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
EPP, EDR, EPDR, Advanced EPDR	End user name (as part of paths and document names) End user username End user and their sender's/recipient's email addresses End user IP address End user Device data such as hostname, MAC address, hardware details, other unique device identifiers URLs	Provide and operate the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting
DNS Watch GO	End user username End user email address End user IP address End user device data such as hostname, MAC address, hardware details, other unique device identifiers Diagnostic data reports (hostname, username, timestamps)	Provide and operate the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting
SIEMFeeder	End user name (as part of paths and document names) End user username End user IP address End user device data such as hostname, MAC address, hardware details, other unique device identifiers URLs (usually limited to domains only)	Provide and operate the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting
Patch Management	End user name (as part of paths and document names) End user IP address End user device name (that can include the username)	Provide and operate the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting
Full Encryption	End user name (as part of paths and document names) End user IP address End user device name (that can include the username)	Provide and operate the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting
Advanced Reporting Tool (ART)	End user name (as part of paths and document names) End user username End user IP address End user device data such as hostname, MAC address, hardware details, other unique device identifiers	Provide and operate the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting
Data Control	End user name (as part of paths and document names) End user username End user email address End user IP address End user device data such as hostname, MAC address, hardware details, other unique device identifiers	Provide and operate the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting

Service	Categories of Personal Information	Processing Purposes
	Operator’s search inputs that may contain any personal data	
Remote Control (Advanced EPDR only)	Operator’s queries and commands that may contain personal data are stored as a part of service logs Operators have access to endpoint details and management (including the ability to download endpoint files). Data is sent through a secure channel that can be initiated only by the Customer and is not stored or accessed by WatchGuard.	Provide and operate the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting

Management System	Data Categories	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:** Connections and logs that could include personal data of Customer’s end users and operators as described above. Status data that shows service errors on specific devices and may include device and the last logged user details. **WGC Audit Logs:** - WGC Operators Information: - Account ID/Account Number/User ID - Username - IP Address - Hostname - Time/Date of access - Source (product interacted with) - Actions taken	Provide and operate the service Detect, analyze and mitigate threats and secure the services Provide customer technical support and troubleshooting

SERVICE DATA COLLECTED BY WATCHGUARD

During our customers’ use of Endpoint 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 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, IP addresses, or device identifiers. 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.

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 Endpoint 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).