DATA SHEET

Data Privacy Practices

Fortinet Products and Services

This document aims to assist our customers in their assessment of Fortinet's privacy protection and compliance by highlighting how personal information is handled by our products and services. The topics mentioned here include:

Fortinet Products Communication with Fortinet Services

During normal everyday operation, Fortinet's products regularly communicate with FortiGuard, FortiCare, and FortiCloud servers. This communication allows these products to confirm licensing and receive services.

FortiGuard Information Collection

FortiGuard collects information about malware encountered by Fortinet products to enable tracking threats in the wild in real time. Fortinet may make anonymized versions of this information available to other security organizations.

Information Storage and Protection on Cloud Services

We use industry standard physical and system administration best practices to protect customer data stored on Fortinet's cloud services. Data retained for log analysis is also completely deleted according to service term agreements.

Overview

Protecting Personal Data with Fortinet Products and Services

To protect personal data, it is essential to know what data is collected, how the data is collected, and what the data is collected for. Knowing how and where the collected data is stored is equally useful in understanding how deployed solutions can implicate data privacy.

For organizations that enforce General Data Protection Regulation (GDPR), it is even more critical that network infrastructure guarantees their data is safeguarded. Data collected, processed and stored by Fortinet products and services that may contain personal information typically comes in the form of detailed activity logs and/or computed statistics. Personal data may be broadly categorized as:

- **User information:** username (collected from authentication services or log ins to public services) and email address
- **Device information:** host name, machine address (MAC), IP address and operating system version
- **User activities:** application usage, file download/upload and URLs visited
- **Threat activities:** malware, host vulnerabilities and attacks detected

GDPR makes it essential to precisely locate all instances of an individual's personal data across the entire infrastructure. Personal data handled by Fortinet products and services may reside on:

- **Local disks:** Logs are stored on devices that have built-in disks. Detailed logs are essential for tackling threat incidents and understanding network security status.
- **External syslog servers and network management systems:** Logs and monitoring statistics can be exported out of Fortinet devices to support organization-wide systems such as SIEM.
- **FortiCloud:** Logs and statistics are stored on our servers hosted in our own secure data centers.
- **FortiGuard Research Labs:** Anonymized statistics and device information may be captured for service improvements.
- **FortiCare System**: Fortinet's registered customer's personal information is stored on our FortiCare servers, located in one of our secure data centers.

HIGHLIGHTS

Fortinet Products Communication with Fortinet Servers

Fortinet products regularly communicate with FortiGuard and FortiCare servers for license verification and to receive update services. Some products also interact with FortiCloud servers for management and security functions.

DESCRIPTION	PROTOCOL	ENCRYPTION	FREQUENCY	DIRECTION	CAN BE DISABLED
FortiGuard update server (update.fortiguard.net)					
Download AntiVirus, IPS, and other updates	SSL-encrypted Fortinet proprietary protocol	SSL with a 2048-bit BIOS-generated certificate	Scheduled updates or push updates on demand	Download to OS	Yes
Upload Malware (from AV, IPS and application control detection) and Botnet IP list statistics	SSL-encrypted Fortinet proprietary protocol	SSL with a 2048-bit BIOS-generated certificate	Hourly by default, configurable	Upload to server	Yes
FortiGuard query server (service.fortiguard.net)					
FortiGuard Web Filter, AntiSpam signature, Virus Outbreak, and IP reputation URL lookups	UDP on port 8888 or port 53 (configurable) and HTTP on port 80	XOR encryption	On Demand	Query request and response	Yes
FortiCare registration server (directregistration.fortinet.com)					
FortiOS license and registration checking	HTTPS on port 443	SSL with a 2048-bit BIOS-generated certificate	On Demand	Download to OS	No
FortiToken license and registration checking	HTTPS on port 443	SSL with a 2048-bit BIOS-generated certificate	At startup, every 5 minutes, on demand	Download to OS	No
FortiCare registration server (directregistration.fortinet.com)					
Initial contact with FortiCloud, license check, addresses of FortiCloud servers	HTTPS on port 443	SSL with a 2048-bit BIOS-generated certificate	On startup or reboot, periodically (usually every 24 hours) during operation	Download to OS, upload to server	No

HIGHLIGHTS

DESCRIPTION	PROTOCOL	ENCRYPTION	FREQUENCY	DIRECTION	CAN BE DISABLED
FortiCloud Messenger (msgrctrl1.fortinet.com)					
FortiCloud license validation	HTTPS on port 443	SSL with a 2048-bit BIOS-generated certificate	On Demand	Download to OS, upload to server	No
FortiClient licensing and install server (forticlient.fortinet.net)					
FortiClient license validation	HTTPS on port 443	SSL with a 2048-bit BIOS-generated certificate	On Demand	Download to OS, upload to server	No
FortiCloud Manager (mgrctrl1.fortinet.com)					
FortiCloud Services (Logs, Configuration Files)	HTTPS on port 443	SSL with a 2048-bit BIOS-generated certificate	On Demand	Download to OS, upload to server	No
FortiCloud Sandbox (mgrctrl1.fortinet.com)					
FortiCloud Sandbox services	HTTPS on port 443	SSL with a 2048-bit BIOS-generated certificate	On Demand	Download to OS, upload to server	No
FortiGuard application icon server (www.fortiguard.com)					
Download application icons	HTTPS on port 80	None	On Demand	Download to OS	No
FortiGuard signature information (www.fortiguard.com)					
Download FortiGuard signature descriptions	HTTPS on port 80	None	On Demand	Download to OS	N/A

FortiGuard Services Information Collection

Through the following FortiGuard services, we may collect or process (sometimes just momentarily) a variety of information about our customers and their associated devices and networks.

DATA TYPE	DESCRIPTION	PURPOSE	APPLICABLE PRODUCTS
Product Information			
Product serial number	Serial number of product requesting FortiGuard services	For contract and entitlement management	All products that use FortiGuard services
Product IP address	IP address of product requesting FortiGuard services	To push FortiGuard updates and embargo country controls	All products that use FortiGuard services
Firmware version	Firmware version running on entity		All products that use FortiGuard services
Content Information			
Unrated URLs	Information about the URL, including the FQDN and IP address	To prioritize adding the URL to the FortiGuard Web Filtering database	Products with valid web filter subscriptions
AntiVirus, IPS and other malware statistics	Malware statistics	FortiGuard research team calculates statistics on threats used for service improvement	Products with valid threat protection subscriptions
Security Rating results	Security Rating value computed from Customer's Security Fabric	To compare with participating customers	FortiOS customers with the FortiGuard Security Rating subscription service

Subject to applicable contractual and legal restrictions, and depending on the Fortinet service at issue, Fortinet may use and disclose the information described in this document for the following additional purposes:

- To assist with technical support
- To enforce the legal terms that govern Fortinet Services
- To comply with applicable laws and protect rights and property
- For other purposes requested or authorized by our customers

Fortinet services may use automated technology to recognize and defend against security threats. To improve security, Fortinet may exchange threat indicators, such as virus signatures or techniques for detection of malicious activity, with other security organizations.

Fortinet products and services may also make certain information available to the customer that manages the product or service. If this customer is a service provider, the service provider would then have information from Fortinet about their customers. Customers of the service provider should contact the service provider for details.

We conduct the above activities on the basis of our legitimate interests in operating our business and protecting our customers. Where appropriate, these activities also are conducted on the basis of consent.

HIGHLIGHTS

Information Storage and Protection on Cloud Services

The following Fortinet hosted services may handle user data:

- **FortiCloud:** provides centralized reporting, traffic analysis, configuration management, WiFi access point management, and log retention without the need for additional hardware, software or management overhead.
- **FortiCloud Sandbox:** a proactive threat detection, mitigation and actionable threat insight solution. At its foundation, FortiCloud Sandbox is a dual-level sandboxing platform complemented by Fortinet's antimalware and integrated FortiGuard threat intelligence. FortiCloud Sandbox enables our customers to deploy sandboxing in a flexible, distributed architecture.
- **FortiMail Cloud:** secure cloud email gateway solution. Fully managed by Fortinet and FortiMail Cloud is available in Gateway or Server mode.

DATA TYPE	DESCRIPTION
FortiCloud (Log and Management)	▪ Device identifiers, IP addresses, and other information about computing systems, applications, and networks ▪ Information about activity on computing systems, applications, and networks ▪ Communication metadata ▪ Suspicious files sent by Fortinet products ▪ Logs used for FortiCloud report generation deleted according to terms of service ▪ Deletion and retention of configuration files managed by customers
FortiCloud Sandbox FortiSandbox Windows Cloud VM Service	▪ Device identifiers and IP addresses ▪ Suspicious URLs submitted for analysis, malicious URLs stored ▪ Suspicious files, communication content, metadata and checksums of malicious files ▪ All clean files deleted within 72 hours, malicious/suspicious files kept for up to 60 days
FortiMail Cloud	▪ In Gateway mode: sender and receiver email addresses and email subjects, message content not stored ▪ In Server mode: email addresses, aliases, distribution lists, message content, and attachments ▪ Quarantined files ▪ Suspicious files sent to FortiCloud Sandbox ▪ Malicious URLs sent to FortiCloud Sandbox

FORTINET

www.fortinet.com