This report provides information needed to assess the impact of SonicWall cloud-based solutions on overall General Data Protection Regulation ("GDPR") privacy posture by detailing how personal data may be captured, processed and stored by and within these products.

**Capture Advanced Threat Protection**

**Product Summary**

SonicWall Capture ATP is a cloud-based security service available with SonicWall next-gen firewalls, email security, endpoint clients and secure mobile access (SMA) solutions. The service detects and can block advanced threats at the gateway until verdict. This service is the only advanced threat-detection offering that combines multi-layer sandboxing, including real-time deep memory inspection (RTDMMITM), full system emulation and virtualization techniques, to analyze suspicious code behavior. This powerful combination detects more threats than single-engine sandbox solutions, which are compute environment specific and susceptible to evasion.

**Information Processed**

The SonicWall Capture ATP service protects against emerging zero-day attacks and ransomware with cloud-based sandboxing technology. The solution scans a broad range of email attachment types and performs dynamic URL analysis to detect advanced threats, analyze them in a multi-engine sandbox and block threats before they reach your inbox.

**Customer Privacy Options**

As defined by the GDPR, SonicWall is a data processor and the customer is a data controller. SonicWall shall only process personal data as determined or defined by the customer, the data controller when their customers use Capture ATP service for their defined business purposes. The customer shall typically rely on various legal bases for data processing. SonicWall contractually encourages customers to provide a privacy notice/policy on how the product may collect and process their end user’s personal data, this privacy policy/notice shall provide clear and accurate information about what personal data Capture ATP may collect, how the company uses the personal data, and the individual rights that may apply to the end users.

**Access to Data**

SonicWall does share any data with third parties in providing Capture Cloud Sandbox service. Access to the personal data collected is limited to when SonicWall as the data processor may transfer or use the personal data to complete problem or software/code bug resolution.

**Retention**

SonicWall stores personal and system data within the SonicWall infrastructure located in data centers around the world – United States, Amsterdam or Japan. As the data controller, the customer can choose the datacenter location for data processing as per legal basis. The
personal and system data may include IP address of the customer’s gateway, Media Access Control (MAC) address of the gateway and email address of the customer’s end user (data subject). As a data processor, SonicWall only stores the personal and system data in accordance with the contractual terms outlined in the customer agreement.

**Security of Data**
SonicWall as a data controller, stores personal and system data in the United States. As defined above, the personal data may include; IP address, Media Access Control (MAC) address, end user name, application usage, geolocation and security behaviors and only stores the personal and system data for up to 6 months as stated in the SonicWall’s data retention policy.

When SonicWall is a data processor, they shall retain personal and system data in accordance with the contractual terms outlined in the customer agreement.

**Hosted Email Security**

**Product Summary**
SonicWall Hosted Email Security with Capture Advance Threat Protection service dynamically scans all suspicious email attachments and URLs, analyzes them in a multi-engine sandbox, and blocks dangerous files or URLs before they reach the network.

**Information Processed**
SonicWall Hosted Email Security with Capture ATP delivers advanced attachment and URL protection to protect against ransomware and targeted phishing attacks. The RTDMI engine proactively detects and blocks mass market, zero-day threats and unknown malware by inspecting directly in memory.

**Customer Privacy Options**
As defined by the GDPR, SonicWall is a data processor and the customer is a data controller. SonicWall shall only process personal data as determined or defined by the customer, the data controller when their customers use Hosted Email Security service for their defined business purposes. SonicWall contractually encourages customers to provide a privacy notice/policy on how the product may collect and process their end user’s personal data, this privacy policy/notice shall provide clear and accurate information about what personal data Hosted Email Security may collect, how the company uses the personal data, and the individual rights that may apply to the end users.

**Access to Data**
SonicWall does not share data with third parties in providing Hosted Email Security service. Access to the personal data collected is limited to when SonicWall as the data processor may transfer or use the personal data to complete problem or software/code bug resolution.

**Retention**
SonicWall stores personal and system data within the SonicWall infrastructure located in the United States, Amsterdam or Japan. As the data controller, the customer can choose the datacenter location for data processing as per legal basis. The personal and system data may include IP address, user name, personal name and email address of the customer’s end user (data subject). As a data processor, SonicWall only stores the personal and system data in accordance with the contractual terms outlined in the customer agreement.

**Security of Data**
SonicWall as a data controller, stores personal and system data in the United States. As defined above, the personal data may include; IP address, Media Access Control (MAC) address, end user...
name, application usage, geolocation and security behaviors and only stores the personal and system data for up to 6 months as stated in the SonicWall’s data retention policy.

When SonicWall is a data processor, they shall retain personal and system data in accordance with the contractual terms outlined in the customer agreement.

Capture Security Center - Management & Analytics

Product Summary
SonicWall Capture Security Center is a scalable cloud security management software delivered as a cost-effective as-a-service offering. Gain the ultimate in visibility, agility and capacity to govern the entire SonicWall security operations and services with greater clarity, precision and speed – all from a cloud interface that can be accessed from any location and any web-enabled device.

SonicWall Management and Analytics is an intelligence-driven analytic engine that automates the aggregation, normalization, correlation, and contextualization of security data flowing through the firewall. It gives real-time insights into everything that is happening in the network security environment. Actionable analytics empowers security teams, analysts and stakeholders to discover, interpret and prioritize security data, in order to make informed decisions and take appropriate defensive actions.

Information Processed
The SonicWall Cloud Management service provides Single Sign-On access to license, provision and manage all network, endpoint and cloud security services, under one integration-friendly management framework. SonicWall Analytics is an intelligence driven big data analysis engine that automates the aggregation, normalization, correlation, and contextualization of security data flowing through all managed firewalls.

Customer Privacy Options
As a data controller, SonicWall has overall control and ownership over the why and the how of the data processing activities. This includes how SonicWall: i) collects the personal data in the first place and the legal basis for doing so; ii) which items of personal data to collect, i.e. the content of the data; iii) the purpose or purposes the data are to be used for; iv) which individuals to collect data about; v) whether to disclose the data, and if so, who to; vi) whether subject access and other individuals rights apply i.e. the application of exemptions; and vii) how long to retain the data or whether to make non-routine amendments to the data; viii) the method for ensuring a retention schedule is adhered to; and ix) the means used to delete or dispose of the data.

As defined by the GDPR, SonicWall is a data processor and the customer is a data controller. SonicWall shall only process personal data as determined or defined by the customer, the data controller when their customers use Cloud Management and Analytics service for their defined business purposes. The customer shall typically rely on various legal bases for data processing. SonicWall contractually encourages customers to provide a privacy notice/policy on how the product may collect and process their end user’s personal data, this privacy policy/notice shall provide clear and accurate information about what personal data Cloud Management and Analytics may collect, how the company uses the data, and what individual rights the end users may have.

SonicWall’s management of privacy rights, such as to receive or not receive (personal choice) marketing communications from SonicWall, can enable customers to provide their preference, or to change or modify choice previously provided or delete inaccuracies, by contacting SonicWall at listmaster@SonicWall.com.
Access to Data
SonicWall does not currently use third parties to assist in providing cloud-based Management and Analytics service. Access to the personal data collected is limited to when SonicWall is the data controller, or in the event that when SonicWall is the data processor, access to personal data may be limited to complete problem or software/code bug resolution.

Retention
SonicWall stores personal and system data in the United States. As defined above, the personal data may include; IP address, Media Access Control (MAC) address, end user name, application usage, geolocation and security behaviors as a data controller and only stores the personal and system data for up to 6 months as stated in the SonicWall’s data retention policy. When SonicWall is a data processor, they shall retain personal and system data in accordance with the contractual terms outlined in the customer agreement.

Additional Resources
SonicWall has conducted a Data Protection Impact Assessment (“DPIA”) on all of these products and can provide a copy at customer request. Contact the SonicWall Privacy Office for more information about Cloud Security solutions and data privacy at: listmaster@SonicWall.com, view our full privacy statement at https://www.sonicwall.com/en-us/privacy.

About this document
The information contained herein is based upon document reviews and interviews with relevant subject matter experts involved in the development and operation of the services described. The discovery process relied upon the good faith accuracy of the information provided; TrustArc has not undertaken an independent audit and does not certify the information contained in this datasheet. However, the information contained herein was believed to be accurate and complete as of the time this datasheet was first published. Please note that the information provided with this paper, concerning technical or professional subject matters, is for general awareness only, may be subject to change and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

About SonicWall
SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award-winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.