



WALLARM PRIVACY FAQ

Q. IS WALLARM A CLOUD OR AN ON-PREMISES SOLUTION?

A. Wallarm is a hybrid solution that includes on-premise filtering nodes and a cloud service. With this unique hybrid approach, requests and application responses are analyzed locally with Wallarm Nodes that are deployed in the customer's on-premises infrastructure while sophisticated analytics and AI/ML algorithms run in parallel in the Wallarm Cloud.

Q. HOW DOES WALLARM ENSURE DATA SECURITY AND PRIVACY?

A. As a security vendor, Wallarm puts the highest level of priority on the security of the solution and the privacy of customer data. Data are processed as close to the source as possible. Best practices in handling data, including access controls, encryption, and data separation, are applied to both data at rest and data in motion. This is true for both on-premises filtering nodes and the cloud service. In addition, the solution undergoes periodic security audits, including penetration testing, to ensure there are no known vulnerabilities.

Q. WHAT PART OF THE SOLUTION HAS ACCESS TO THE APPLICATION INGRESS AND EGRESS TRAFFIC?

A. Only the local filtering node has access to the L7 application traffic, both for the incoming and for the outgoing application calls.

Q. WHAT TYPES OF DATA ARE SENT TO WALLARM CLOUD?

A. Wallarm application protection relies on its ability to apply machine learning algorithms to derive application logic and create custom security rules in addition to the ability to actively verify potential threats. To be able to do this, Wallarm Nodes communicate some of the anonymized application and traffic metrics to Wallarm Cloud. The following types of data are sent to the cloud:

- Statistical metrics of L7 requests. These metrics do not contain the content of specific application calls or personally identifiable information; a typical size of metrics data set per 100Mbps of data is under 3Kbp. For example, some application calls include a hash of password fields inside a JSON; a Wallarm Node will send some metrics about the "average" hash to the Wallarm Cloud, including its minimum and maximum length. It would be impossible to reconstruct any single password from this data.
- Requests identified as malicious by security rules already in place.
- Statistical metrics of the L7 application responses. Similar to the metrics of requests, these metrics do not contain individual application calls or private information.
- Analytics on the traffic intensity and potentially bad activity, including RPS (requests per second) and APS (attacks per second).

Q. WHAT KIND OF ENCRYPTION IS APPLIED TO DATA IN FLIGHT?

A. We use only secure ciphers and TLS 1.3 encryption.

Q. WHAT ADDITIONAL SECURITY MEASURES ARE TAKEN TO AVOID POSSIBLE COMPROMISE?

A. Wallarm takes extra care to never communicate security artifacts outside the immediate operational environment. Wallarm never knowingly sends PII information to the cloud. However, in environments with heightened security, such as FinTech companies, we have enabled an additional filter to detect possible session tokens, cookies, or credit card numbers, and can mask those out to reduce possible exposure.

Q. IS WALLARM PCI COMPLIANT?

A. Wallarm does not store or communicate payment card information, thus it is not technically subject to PCI DSS. However, because many customers use our solution to satisfy PCI DSS paragraph 3.6, we adhere to the recommendation of this body.

Q. WHAT KIND OF SECURITY PRACTICES ARE IN PLACE IN WALLARM CLOUD?

A. Wallarm Cloud is deployed and operated in accordance with the industry's best practices. Both the infrastructure and the application are secured and hardened. Software development is subject to regular security code reviews, and security tests are included during every release cycle. Corporate Security Policy, including change management, is in place and is followed by all personnel.

Q. CAN WALLARM'S BACKEND CAN BE DEPLOYED ON PREMISE?

A. Yes, Wallarm backend can be deployed on premise as a part of the Wallarm Standalone product. We can also deploy a private cloud for customers in AWS or the cloud provider of their choice.

<https://wallarm.com>

155 Constitution Dr., Menlo Park, CA, 94025
(415) 940-7077