Signal Sciences

Privacy

What data gets sent to the Signal Sciences backend?

Not all traffic is sent to the Signal Sciences backend. The agent pre-filters locally to determine if the request contains an attack. Only requests that are marked as attacks or anomalies are then sent to the Signal Sciences backend, and only after additional filtering and sanitizing are completed.

Once the agent identifies a potential attack or anomaly in a request, the agent sends only the individual parameter of the request which contains the attack payload, as well as a few other non-sensitive or benign portions of the request, such as client IP, user agent, URI, etc.

The entire request is never sent to the Signal Sciences backend. In addition, certain portions of the request are explicitly never sent to the backend, such as session tokens or tracking cookies.

KEY TAKEAWAYS

- Signal Sciences is committed to providing the highest level of privacy and security of your corporate data.
- Our system collects and stores as little as possible while maintaining our solution's ability to provide high fidelity application security visibility and blocking.
- Ultimately, the level of privacy is up to you. We allow custom data redaction and full transparency on all data sent to the Signal Sciences servers.

How is my corporate data redacted?

The agent sanitizes common sensitive data types such as credit card numbers, SSNs, GUIDs, etc. For example, if a request containing a SQL injection attack also contained a 16-digit credit card integer in the same parameter as the attack, all the digits of the credit card number would marked out as redacted before being sent to the Signal Sciences backend.

How can I verify what data is being relayed to the cloud?

In the management console and API, we provide mechanisms to verify all our claims on privacy by viewing the raw data being sent from the agent up to the Signal Sciences backend.

What about fields that are specific to my application?

We provide a configuration mechanism in the management console to add additional fields which will always be filtered. For example, if your password field is named “passwd” instead of “password,” we will redact that field in the agent before it’s sent to our backend.

How does Signal Sciences use the data it collects?

Signal Sciences only uses your data to provide visibility and make decisions about blocking attacks to your application. We’ll never attribute any data back to your organization or end users.

What happens if I want to scrub something after the fact?

See something in the raw data that you’d rather delete? Submit a support request for Signal Sciences automated tools to go through and scrub our database of your requested field.

What response data does the Signal Sciences backend see?

Signal Sciences only collects the response’s metadata, i.e. response codes, sizes, and times.

The World’s Top Companies Trust Signal Sciences

DOORDASH Glossier. DUO vimeo

tenable® SHINOLA DETROIT UNDER ARMOUR one medical