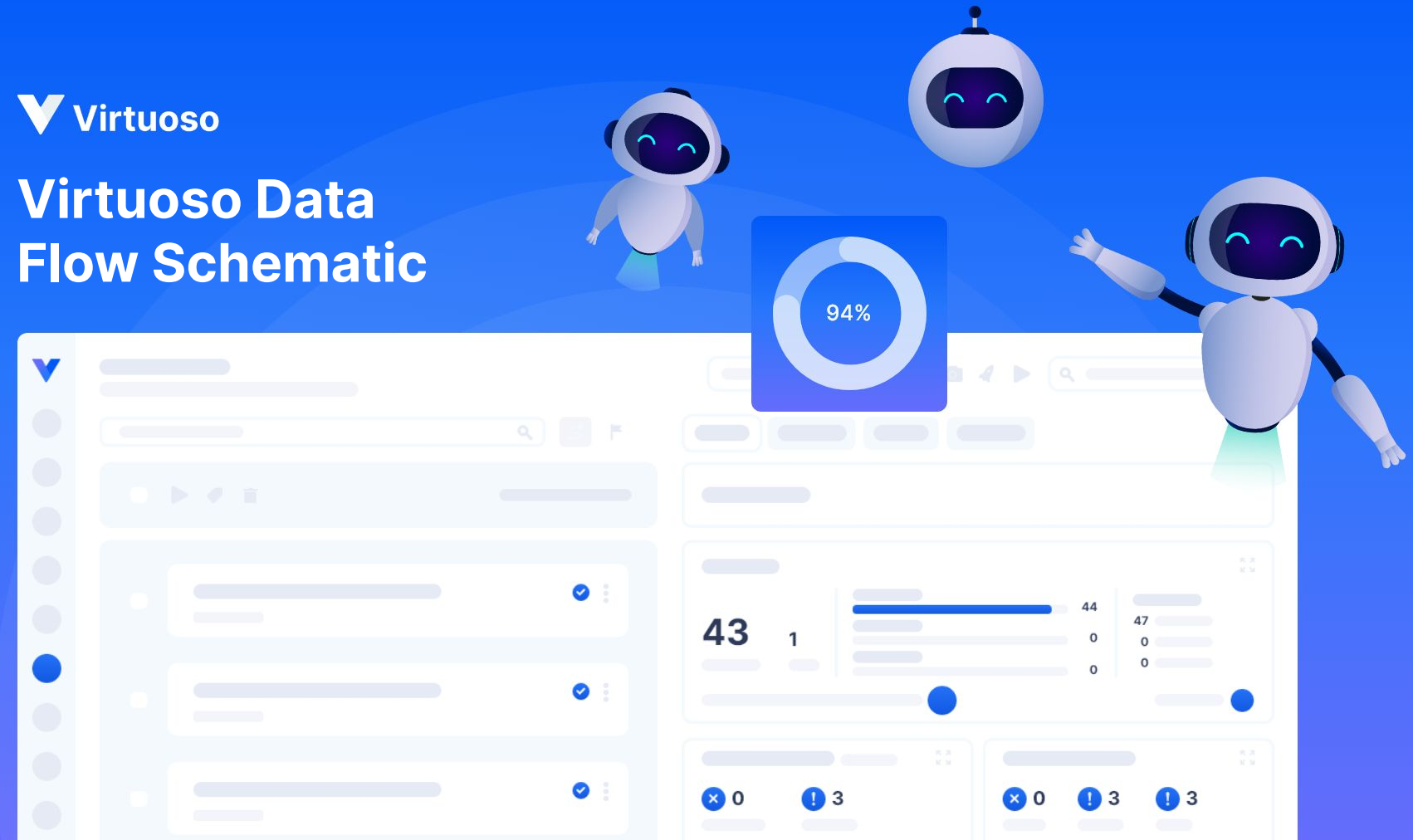
Virtuoso

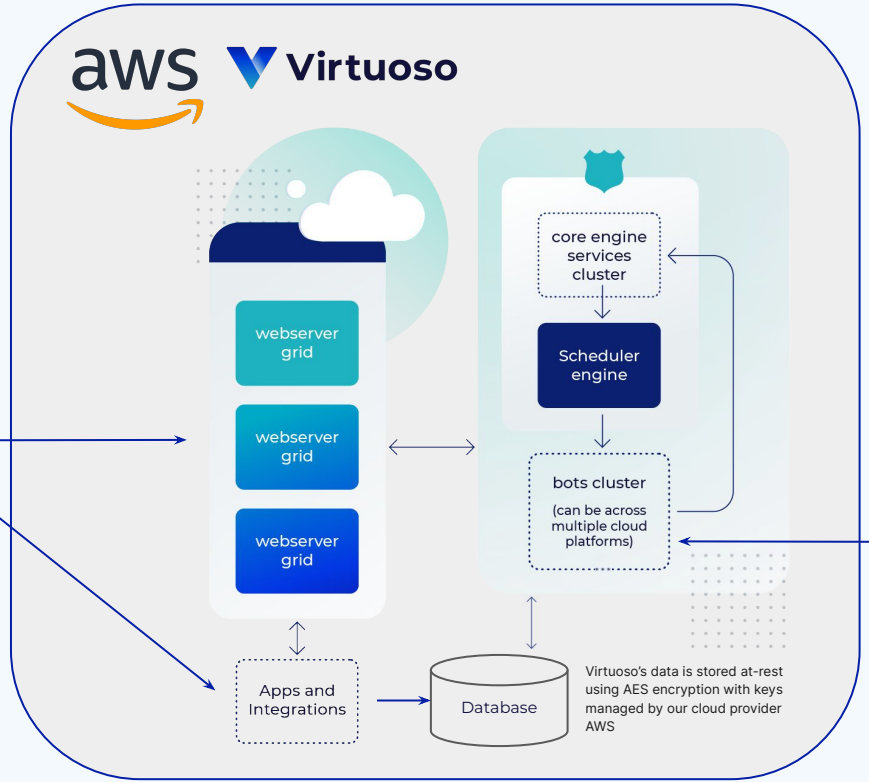
Virtuoso Data Flow Schematic



Virtuoso Data Flow Schematic

Passwords are individually salted and stored using PBKDF2 with HMAC-SHA256 with 65536 iterations, per NIST guidelines on memorised secrets. Clients can only use Virtuoso over TLS, and traffic is encrypted between your browser and our load balancer

SSO Support is also available via AWS Cognito for various protocol support



Users access the frontend application, API, and integrations via industry standard TLS1.2+ encryption (HTTPS)

Type of Data Transmitted:

DOM level elements for all elements tested
DOM (page source) for all pages tested
Page network requests for all pages tested
Page console logs for all page tested
Screenshots of pages tested for all elements/steps tested

All data sent over the internet between users and application servers is secured in transit using industry standard TLS encryption. Virtuoso's internal systems can only be accessed with transport encryption in place with suitable authorisation.

Logs

Virtuoso's application logs are aggregated and sent securely to Datadog and retained for 15 days. We store application-level access logs and also maintain system-level logs from our infrastructure. We maintain an archive of all logs which encrypted at-rest using AES with keys managed by our cloud provider AWS.

We also make use of Sentry for error event tracking and application monitoring from the frontend, which stores data encrypted at-rest and transmits via HTTPS from the user's browser.

All communication with Virtuoso is https/TLS 1.2 encrypted
Encryption as required by APIs/microservices under test(Bearer token, key, password etc)

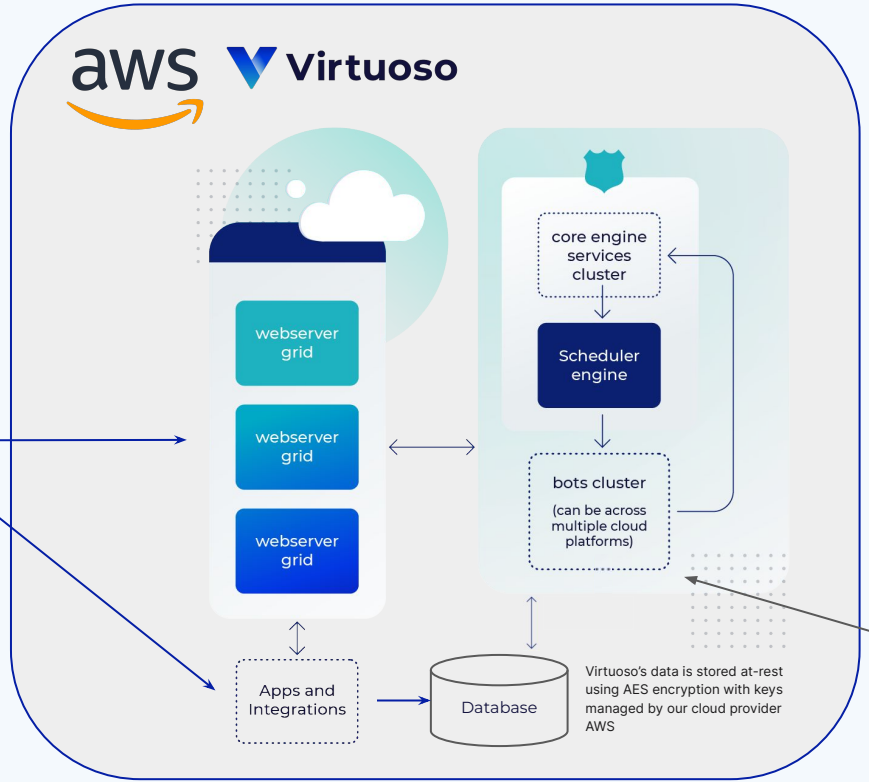
Target Web Based Application

Virtuoso Data Flow Schematic - with Bridge

Passwords are individually salted and stored using PBKDF2 with HMAC-SHA256 with 65536 iterations, per NIST guidelines on memorised secrets. Clients can only use Virtuoso over TLS, and traffic is encrypted between your browser and our load balancer

SSO Support is also available via AWS Cognito for various protocol support

Users access the frontend application, API, and integrations via industry standard TLS1.2+ encryption (HTTPS)



Type of Data Transmitted:

DOM level elements for all elements tested
DOM (page source) for all pages tested
Page network requests for all pages tested
Page console logs for all page tested
Screenshots of pages tested for all elements/steps tested

All data sent over the internet between users and application servers is secured in transit using industry standard TLS encryption. Virtuoso's internal systems can only be accessed with transport encryption in place with suitable authorisation.

Logs

Virtuoso's application logs are aggregated and sent securely to Datadog and retained for 15 days. We store application-level access logs and also maintain system-level logs from our infrastructure. We maintain an archive of all logs which encrypted at-rest using AES with keys managed by our cloud provider AWS.

We also make use of Sentry for error event tracking and application monitoring from the frontend, which stores data encrypted at-rest and transmits via HTTPS from the user's browser.

The Virtuoso Bridge creates an encrypted tunnel.
All communication with Virtuoso is https/TLS 1.2 encrypted
Encryption as required by APIs/microservices under test(Bearer token, key, password etc)