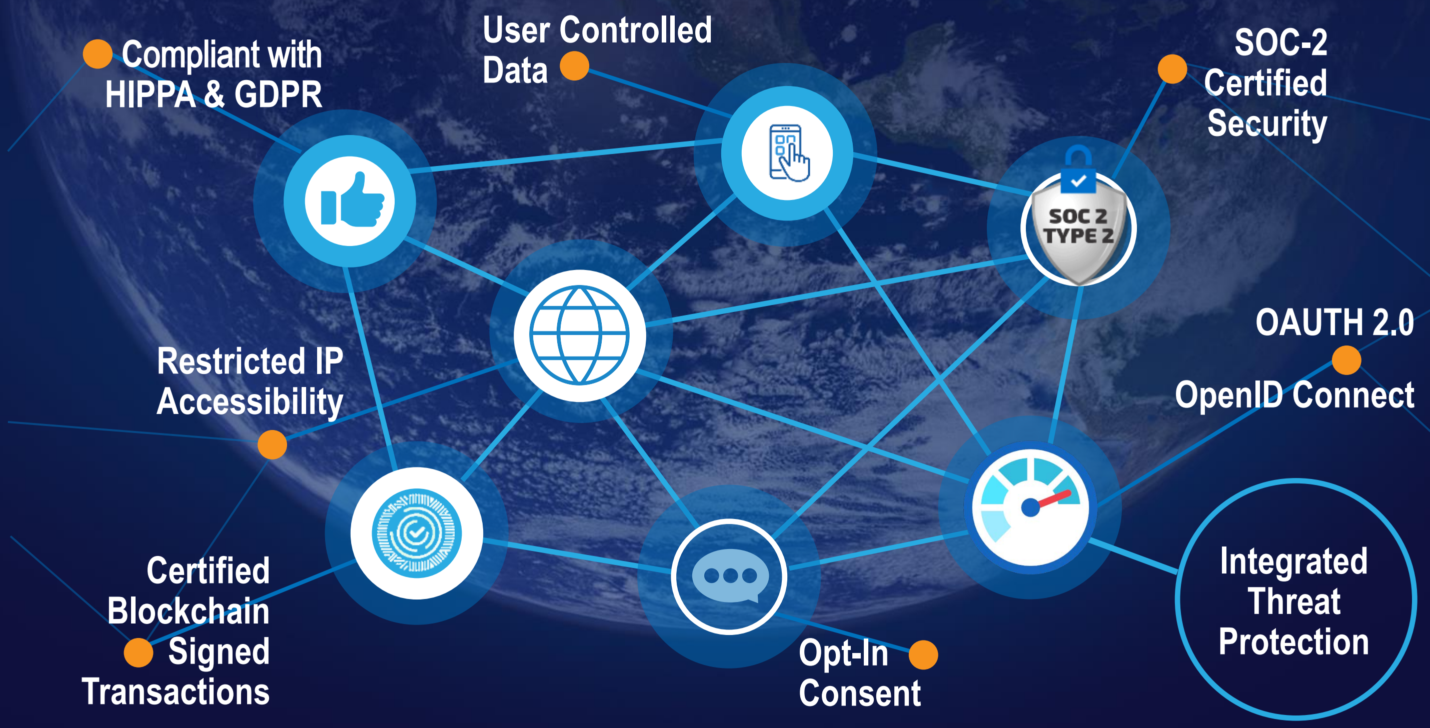
Vaxtrac

Security Model

THE AGE OF
Sharing
Responsibly



Compliant with HIPPA & GDPR

User Controlled Data

SOC-2 Certified Security

Restricted IP Accessibility

OAUTH 2.0

OpenID Connect

Certified Blockchain Signed Transactions

Opt-In Consent

Integrated Threat Protection

2.7 million Transactions Per minute can be analyzed

All DATA IS ENCRYPTED AT REST AND IN TRANSIT

When we move data, it is not just encrypted through TLS. We deploy another layer of FIPS-140.2 strong encryption to each transaction. All data at rest is secured by via strong cloud service providers with their rotating keys on our data vaults. All Data in our Chips with the Travel Card are EAL5+ Certified and built to ICAO standards.

Zero-Trust Model

A zero-trust model is a security framework that fortifies the enterprise by removing implicit trust and enforcing strict user and device authentication throughout the network.

By limiting which parties have privileged access to each segment of a network, or each machine in the Vaxtrac Ecosystem the number of opportunities for a hacker to gain access to secure content is greatly reduced. No direct access to the data is allowed, all requests are validated 1st for authority and then tokenized for a singular session and access is granted based on a pre-establish RBAC list. Specific Events are logged for both traffic and breech analysis.

Defense-in-Depth

Defense-in-depth is the practice of using controls at all layers of the information architecture. In cloud architectures, the need to follow this philosophy is critical. Our focus for Vaxtrac includes client-side hardware (mobile devices and external servers), operating system instances, virtual machines, containers, storage, database, application servers, REST Apps, Networks Perimeters, web portals, and the administrative interfaces for cloud automation and management.