The Secure Application Builder

PRODUCT BRIEF | APRIL 2018

Matthew Erickson

Dir. of Client Services and Technology
matt@spideroak-inc.com
+1 866.432.9888 x703

SpiderOak, Inc.

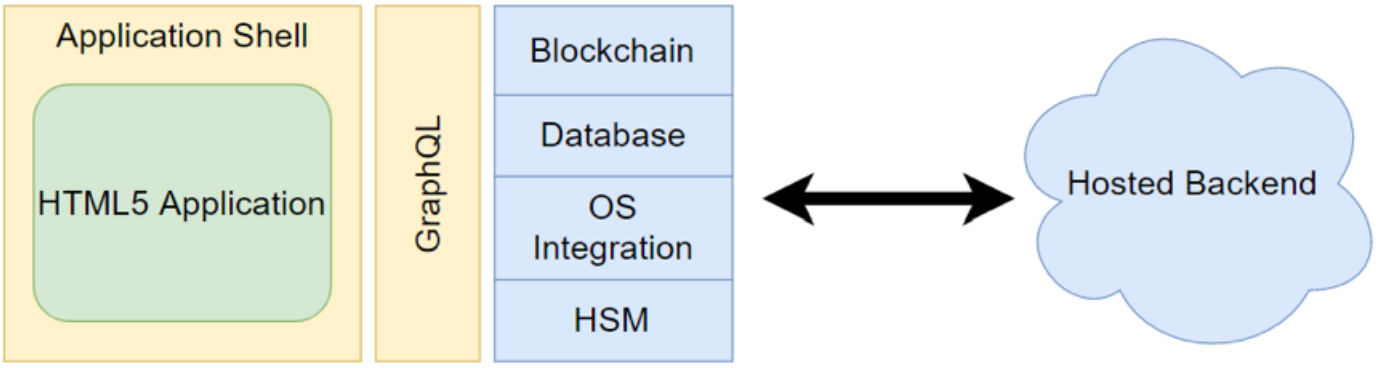
5920 Nall Ave., Suite 200, Mission, KS 66202
+1 866.432.9888 | info@spideroak-inc.com

Rapidly Develop and Deploy Secure Applications

What is the Secure Application Builder?

The SpiderOak secure application builder will allow you to build, test, and deploy new application software at fractions of the time and cost of traditional methods while protecting your data with better-than-best-practices security.

SpiderOak has created a fundamentally different approach to software that gives organizations strong control over their security – which enables confidence in assessing risk. This approach removes responsibility for authority, identity, and integrity from your infrastructure, greatly simplifying your threat model and establishing organizational control.



What is included in the Builder?

The builder includes a tool-chain that lets developers use HTML5 to write once and build for iOS, Android, MacOS, Windows, and Linux. This is paired with an easy to use Graph-QL-based API that lets you take advantage of end to end cryptography and private blockchain technology. Electron for the desktop and Apache Cordova for mobile are used as the application shells.

Provided APIs in the SDK include:

- Users and roles
- Device management
- Flexible rule-based security polices
- An object store
- A set data type (Add, Delete, Enumerate)
- End-to-end encrypted group message channels

Software Approach.

Data messaging and storage is handled through client-based end-to-end encryption for confidentiality, with the use of blockchain for managing identity, integrity and authority. Accounts are identified by private key material held only by the user, and data is encrypted against device-specific keys held within device TPMs, HSMs, and SEs where available. Data flows are segmented first by teams within a platform instance, and then further by channels within teams. Each segmentation is cryptographically enforced, so that users within each grouping are unable to view data in another segmentation.

Administrative authority within a team does not imply any capabilities within channels, including capabilities to read or write. Only entities that have been “invited” to participate within a channel can do so, and the record of team and

channel authority and membership is recorded and managed via blockchain. This use of blockchain provides an irrefutable record of which entities are allowed to administer or participate within a channel, without requiring any central point of authority to dictate these rights.

In addition, the platform supports optional features such as secure deletion, retention polices, LDAP integration, and escrow for message data and objects when it is needed for regulatory compliance.

More information.

If you're interested in helping accelerate your company's software development while cutting your attack surface in half, please reach out and we'll be happy to continue the discussion.

Brad Kropf

bkropf@spideroak-inc.com
+1 915.579.4334

Matthew Erickson

matt@spideroak-inc.com
+1 866.432.9888 x703