SpiderOak

White Paper | February 2018

The Trusted Application Platform.

Matthew Erickson

Dir. of Client Services and Technology
matt@spideroak-inc.com
+1.866.432.9888 x703

SpiderOak, Inc.

4741 Central St #324, Kansas City, MO 64112
+1.866.432.9888 | info@spideroak-inc.com

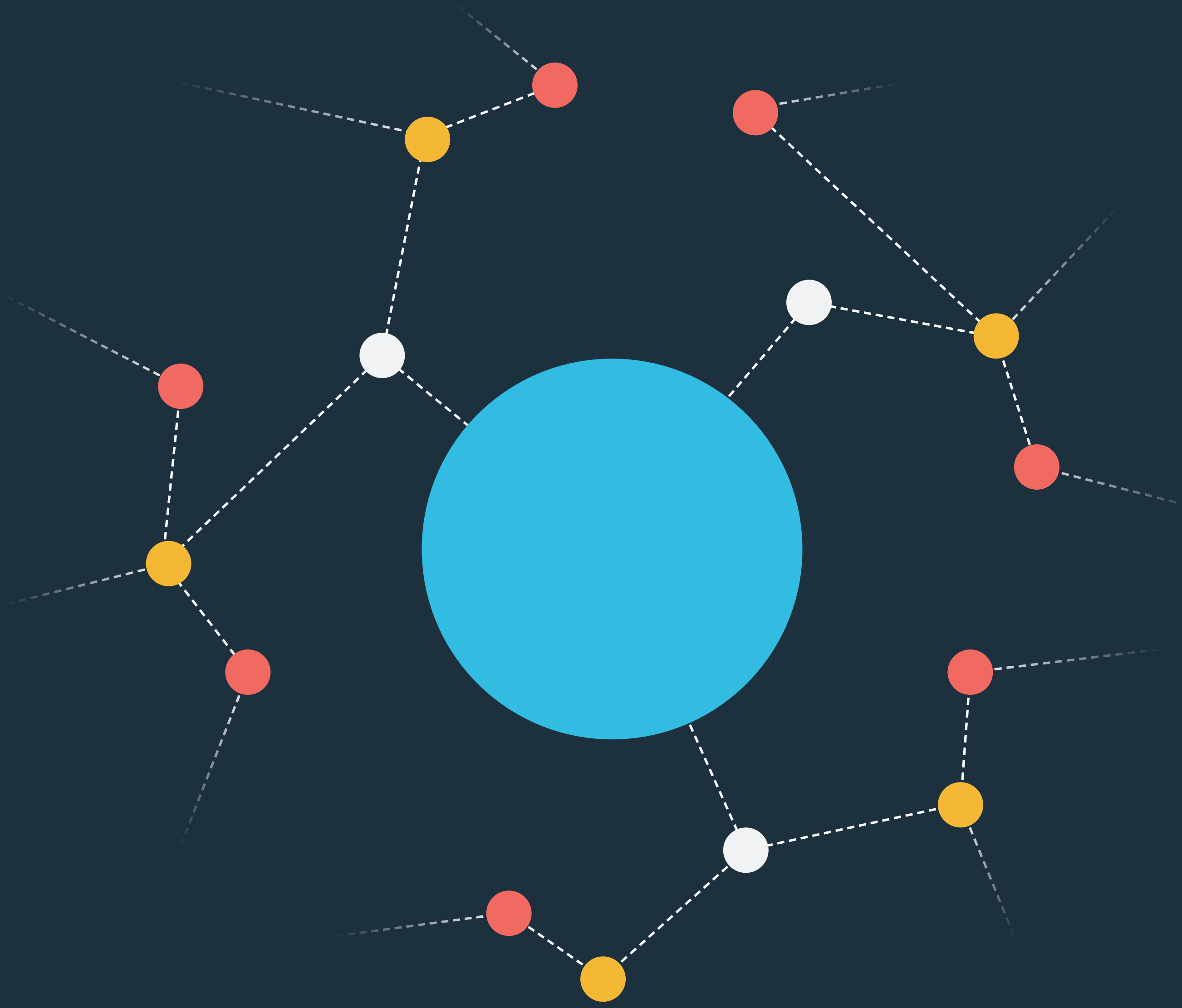
Why do breaches keep happening?

Every day brings news of a new breach or new critical vulnerability. Why does this keep happening?

At its core, the current client server architecture is broken. In today's applications the server is at the center of trust and authority. To trust the server, you have to trust the millions of lines of code that form these servers and the operating systems they depend on. Far worse, we also have to depend on all the people that maintain the systems and the systems those people depend on, and so on. *(see figure 1.1)*

Supply chain attacks, 0-day exploits, and rogue employees are all risks to the integrity of the server's centralized authority. Given this situation one should ask: Why do we trust the server at all?

Figure 1.1



The centralized system.

In a centralized system, any compromise in any part of the maze of corporate staff, developers, and IT, and any vendors, or their vendors, and so on, can result in the compromise of all of an organization's data. Absolute trust must be extended to everyone involved in the enterprise, even if seemingly unrelated.

Decentralization.

The alternate solution to server based trust is the decentralized model. In a decentralized system, each part of the system is only given the ability to perform the actions required to complete its job *(see figure 1.2)*. The server is only responsible for relaying bytes between clients, and is not able to forge or modify messages from clients. Content is only accessible to parties who have permission to see them; even IT staff cannot read messages not meant for them. Source code not critical for the implementation of the security system is no longer critical to maintain security. A bug in the operating system, or a dependent software component, no longer can reveal comprehensible data to an attacker.

In a decentralized system it is still possible to implement all the required compliance and policies. Retention, escrow, and HR policies can be enforced and enacted in a way that gives stronger guarantees than are possible with the traditional systems. Using cryptographically-enforced decentralized authority, an organization can be sure of who has access to what data and for how long, who has the ability to take certain actions, and what actions have been taken by whom. With a decentralized approach, we gain the following advantages:

- The removal of millions of lines of code from the trust base.
- The removal of root authority from IT staff.
- The ability to keep our highest level permissions in a physical safe.
- The ability to create interlocks that require multiple parties to agree when performing important actions.
- The ability to know exactly who has visibility and control over what data with in your system.

These advantages allow your organization to remove whole classes of risk from your IT systems, and avoid being the next headline.

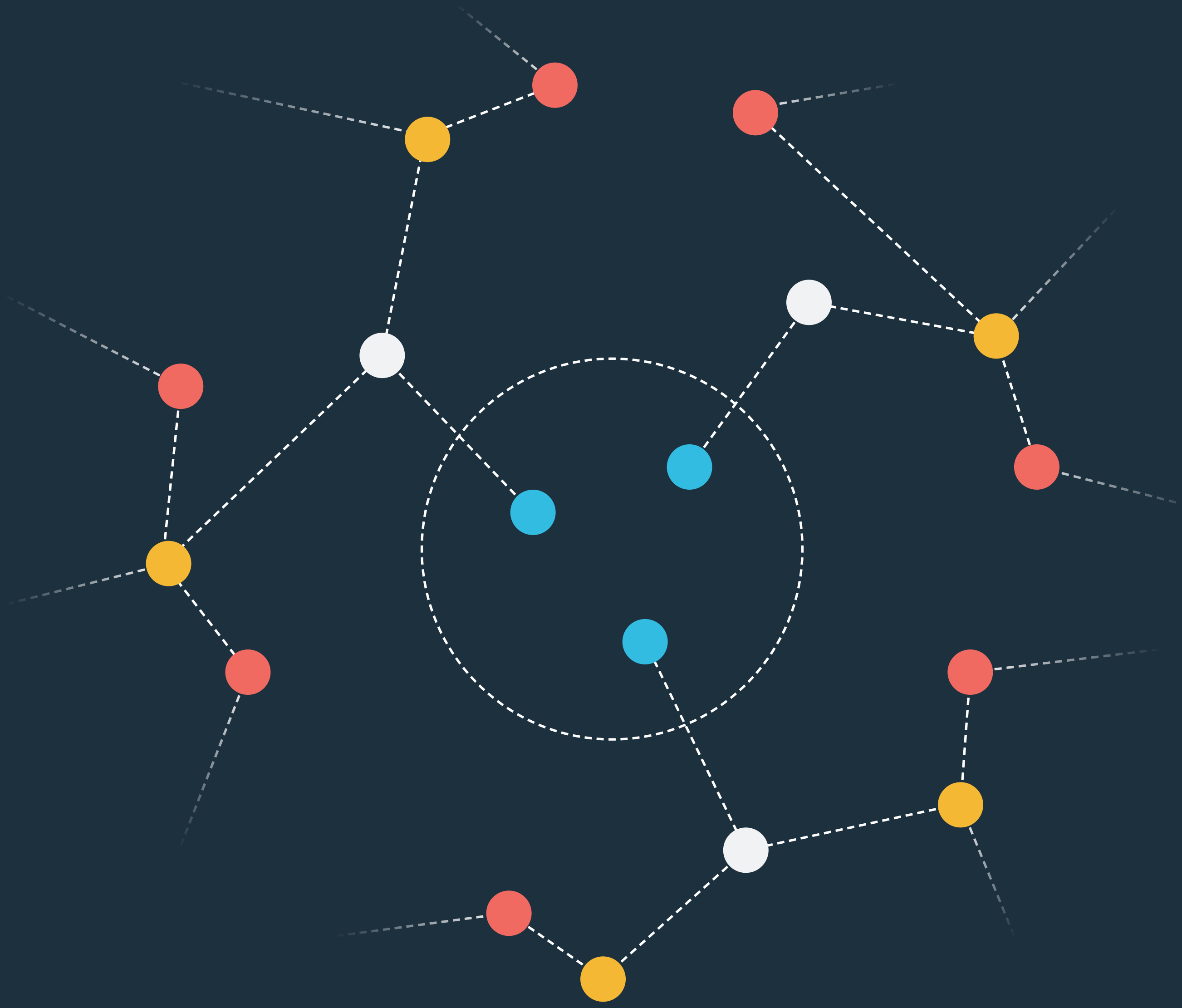
Blockchain.

The most well-known application of this distributed authority model is the blockchain. Using blockchains, servers are not trusted and every client can validate the ledger. While these principles can be applied to general applications without compromise, blockchains provide ready-to-go structures and tools to work with data in this manner. Leveraging blockchain technology enables applications where one can reason about user authority and access in a more nuanced and more secure manner.

These properties can be leveraged to manage trust within an organization. Access to data and processes can be managed without having to tie trust to a central database, and scope of access can be limited to those who actually need to be able to see the data in question to do their jobs. Key management, a critical component to securing data cryptographically, can be easily handled through blockchain.

While the early application of blockchain was providing secure means to transfer value via cryptocurrency, it is undergoing rapid evolution today as it is applied to other fields needing distributed authority, and we are confident that managing software security is a “killer app” for it in the forseeable future.

Figure 1.2



The decentralized system.

In a decentralized system, data access is cryptographically enforced on a need-to-know basis. A compromise of one individual within an organization can only expose, at worst, the data they've been granted the right to see. Through cryptography, the amount of data one needs to be able to see to perform their jobs is also greatly reduced. It separates the need to access systems for maintenance from being able to view the data on the system.

The SpiderOak Solution.

Secure App Builder.

With the Secure App Builder, you can make use of your existing HTML5-centric engineering talent to produce cross-platform desktop and mobile apps on the SpiderOak blockchain platform even if you have no experience building secure and scalable decentralized systems. Leveraging popular open technologies such as Electron and Adobe PhoneGap, we provide an easy-to-use API within an application shell that enables you to create anything from consumer apps to bespoke line-of-business software with front-end web talent.

The Secure App Builder provides a complete end-to-end solution for preventing attacks such as common server data breaches, misplaced trust, phishing, and digital supply chain attacks. Make use of the same tools we use to produce Semaphor, our trustworthy, blockchain-based team chat app.

Secure App Environment.

If you have more complex needs, from using native GUI toolkits to embedded software in connected devices, or wish to add additional secure capabilities to an existing piece of software, the Secure App Environment provides the platform you need to build upon. Embed our libraries into your products to get the same blockchain-based, end-to-end encrypted data storage and messaging that are used in SpiderOak's own products and the Secure App Builder. The core of the Secure App Environment scales up and down as you need, fitting in well from embedded 32-bit ARM environments up to securing data inside of and between massive server farms.

While the most secure implementations make use of the Secure App Environment as the basis for all data storage and messaging needs, it is easy to augment an existing application with additional capabilities incorporating our technology.

For example, a desktop application can embed our Secure App Environment to enable safe "cloud sync" of its data files securely on a blockchain without having to implement their own cloud synchronization platform and cryptography to keep user data safeguarded. Alternatively, industrial machines can have their command and control networking code augmented with the Secure App Environment, enabling strong assurances of proper authority of commands being sent to the machines.

Secure App Updater.

The foundation of trust with cryptography is based on being sure your deployed software hasn't been compromised. Digital supply chain attacks are an increasingly common means of attacking systems: if your software update mechanism is compromised, everything else you do is also compromised.

Our Secure App Updater is a set of tools, documentation, and training enabling your team to produce software updates strongly resistant to a wide variety of supply chain attacks. This system can be easily applied to new and existing products with any need for significant overhauls. If you are already

Secure App Updater.
(Continued)

using an HTTP-based update library, you can substitute in ours as the entirety of the software changes necessary to support it. SpiderOak will then help you set up multiple, disconnected authorities to ensure that even in the compromise of one authority, malicious updates still cannot be pushed.

More information.

To learn more how to use the Trusted Application Platform to enable complete control over your digital supply chain, reach out to us and we'll be happy to help you out.

Christopher Skinner

cskinner@spideroak-inc.com
+504.259.6700

Matthew Erickson

matt@spideroak-inc.com
+1.866.432.9888 x703