SplitSecure

Overview of Use Cases

SplitSecure is a new kind of access management platform, based on a concept of distributed secrets. Its simple yet powerful architecture offers an elegant solution to many long-standing problems in enterprise cybersecurity.

With SplitSecure, organizations can split secrets (such as passwords, credentials, encryption keys, etc) across multiple devices. Secrets split this way can be used normally, but they are never persisted on any device and never exposed. That means that even if a device is fully compromised, it is not possible for the attacker to extract the protected information. It also means that if an employee falls for a social engineering attack (or clicks on a link in an email) there is no way for them to expose the protected data.

This architecture has numerous applications:

USE CASE

Future-Proof, Zero-Day Resistant PAM

When used as a PAM tool, SplitSecure eliminates persistent credentials and makes the organization resistant to social engineering. No compromised employee or device can reveal protected information. This also offers resistance to zero-days (as one compromised device does not reveal the secret), and our algorithm protects against quantum computing attacks.

USE CASE

Managed Service Provider (MSP) Tooling

SplitSecure is the secrets and access management platform designed to work across multiple companies that do not share common IT infrastructure. This means that with SplitSecure, MSPs and their clients can share access to critical systems or accounts. Credentials are never duplicated, never exposed, and always monitored, making it easy for the MSP and customer alike to enforce policy and ensure access is always used appropriately.

USE CASE

Cryptographic Sovereignty

Cryptographic sovereignty regulations are impacting every industry and geography, making enterprises responsible for control over their information. SplitSecure gives enterprises full custody/sovereignty over their information, without technical complexity or burdensome overhead. We have the security claims of an on-prem solution, paired with the simplicity and convenience of a cloud solution.

USE CASE

Digital Asset Custody

Adoption of digital assets is accelerating, but with increased adoption comes increasing regulatory scrutiny and implementation challenges. SplitSecure allows any financial institution to adopt digital assets in a framework that is compliant-by-default and inexpensive to implement. No large or sophisticated cybersecurity team required – we are easy to deploy and manage and integrate with all of your existing tools.

USE CASE

Financial Regulatory Compliance

SplitSecure allows any bank or financial institution to achieve cryptographic sovereignty, and to easily demonstrate regulatory compliance. No more manual work showing compliance in the handling of keys and other secrets. SplitSecure makes organizations compliant by default, and generates one-click compliance reports.

THE FOUNDERS

Built by leaders in security engineering.

Tristan Morris
Cofounder & CEO

Tristan Morris is a security engineering prodigy who started attending college at age 12. After graduating from Cornell, he went on to lead Federal Security at KNOX, Samsung's military and intelligence cybersecurity group.

Marc Trembley
Cofounder & CTO

Marc Tremblay has been a security engineer on some of the most capable and prestigious security teams in the world, including the core security teams of Netflix and Stripe. He has six patents for security technology.

Ready for simple and effective cybersecurity?

Email us directly at **tristan@splitsecure.com**