



The Evolution of Zero Trust

Protecting your most sensitive systems without storing a single credential—anywhere. Simplify your security environment, control vendor risk, and eliminate single points of failure.

THE PROBLEM

Security tools everywhere, control nowhere

The modern enterprise security environment is a cluttered mess. Enterprises typically rely on over 75 security tools (SSOs, IAMs, PAMs, vaults, and HSMs) creating a noisy, fragmented security stack competing for CISO time and attention.

Worse, these tools frequently come with a tradeoff between security and usability. The tools with the best security and regulatory claims might also be the highest maintenance.

THE SOLUTION

Simple, low maintenance, extremely secure

SplitSecure cuts through this noise. It is the simplest, lowest maintenance, and most secure secrets & access control tool in the industry. It allows enterprises to condense their security environment, reducing friction and overhead.

It can be deployed out of the box in as little as thirty minutes, but its security claims are suitable for even the most security-sensitive regulated enterprise.



Simple



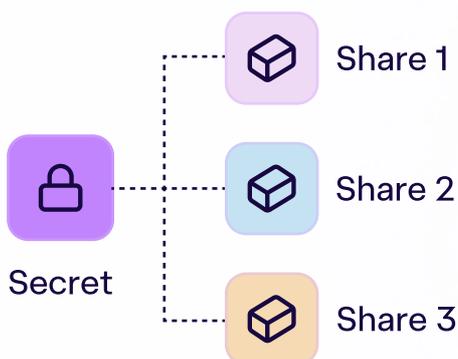
Efficient



Robust

HOW IT WORKS

Secrets are split, never stored



Nothing is ever stored.
Nothing can ever be extracted.



Secrets are split across devices

With SplitSecure, organizations can split secrets—such as passwords, credentials, or encryption keys—across multiple devices. Secrets still work normally, but they are never persisted or exposed on any device.



Compromise-resistant by design

Even if a device is fully compromised, attackers cannot extract the protected information because no device ever holds the complete secret.



Phishing-proof for employees

If an employee falls for a social engineering attack or clicks a malicious link, there is no way for them to reveal protected data.

This is the simplest and strongest of security claims: **an attacker cannot steal what is not there, and an employee cannot reveal what they do not know.**

USE CASES

This technology can be used throughout the enterprise:



Small Team PAM

For small security teams that need to secure access to sensitive accounts (like admin or infra accounts), SplitSecure eliminates single points of failure.



Self-Custody Vaultless Vault

SplitSecure's "vaultless vault" secrets manager is a full self-custody solution, making it a superior alternative to on-prem vault solutions.



PKI Management

SplitSecure can act as a certificate authority and supports PKI management as well as machine identity.



Tokenization

SplitSecure supports tokenization for sensitive data protection and payments processing.

THE FOUNDERS

Built by leaders in security engineering.

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 defense cybersecurity group.

Tristan Morris
Cofounder & CEO



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.

Marc Tremblay
Cofounder & CTO



Ready for security built on what
attackers *can't* access?

Email us directly at tristan@splitsecure.com

