SOLUTION OVERVIEW

Atakama integration with Spirion

Data is being created and shared at a rate at which traditional security controls can no longer keep up. Increased cloud adoption and modern remote work policies have obliterated the perimeter, requiring new strategies for data protection. Further complicating matters is the need to safeguard sensitive data without over-burdening end users with timeconsuming workflows and guidelines for which they were not trained.

Re-inventing Rights Management

A common way to protect sensitive data is to restrict access to only the specific individuals that require it. Rights management, or encryption, solutions can define groups based on their department, role, security clearance, geography, or any combination of these parameters and more. Encryption solutions excel at keeping prying eyes away from unauthorized data but can often fall short in a number of ways. Atakama and Spirion have teamed up to re-invent rights management to meet modern requirements.

It begins with Data Identification

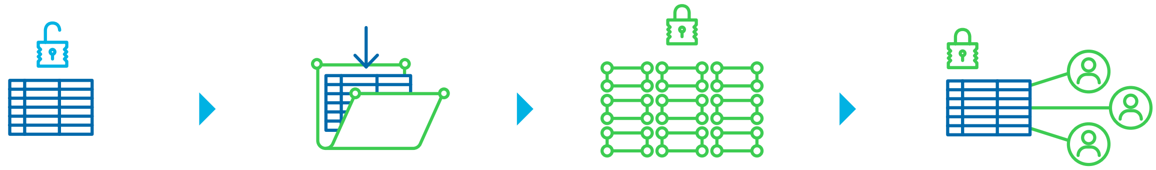
One area where traditional security misses the mark is in understanding which data requires which level of protection. Spirion simplifies rights management by enabling the appropriate level of encryption based on the sensitivity of the data; not the opinion of an end-user untrained in the ways of information security. The unparalleled accuracy of Spirion discovery and identification allows organizations to eliminate end-user error and leverage protection that is optimized for the sensitivity of the data.

Multi-Factor Encryption to Achieve a Zero Trust Posture

Traditional encryption solutions are heavily dependent on identity and access management controls. Login credentials, which allow the authorized users to access encrypted data, represent a single point of failure. Atakama enables the encryption of files on an individual level without reliance on usernames and passwords. The Atakama solution encrypts at the file level with each file receiving its own unique AES-256 bit key. Each key is then fragmented into “shards,” with the shards distributed across physically separated devices, included, but not limited to, users’ workstations and their smartphones. The single point of failure has been removed and the data remains accessible only to those individuals or groups it is intended for. And Atakama accomplishes all of this without disrupting existing workflows or creating worker frictions.

How it works

SPIRION ATAKAMA



Spirion scans and identifies

on-premises, in the cloud, even endpoints

Sensitive data discovered

files are quarantined automatically as per policy

Atakama applies AES 256-bit encryption

and elimiates the single point of failure by splitting the key into shards

The file is available only to authorized users

unlocked using familiar multi-factor authentication tools

Better together

Atakama and Spirion are helping organizations stay ahead of shifts in the modern threat landscape by delivering solutions that focus directly on the data without reliance on an increasingly porus perimeter. Contact us to learn more about how Spirion's accurate data identification combined with multi-factor file-level encryption from Atakama can help you.

Contact us

Atakama
info@atakama.com
atakama.com

Spirion
expert@spirion.com
spirion.com

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion has relentlessly solved real data protection problems since 2006 with accurate, contextual discovery of structured and unstructured data; purposeful classification; automated real-time risk remediation; and powerful analytics and dashboards to give organizations greater visibility into their most at-risk data and assets. Visit us at spirion.com