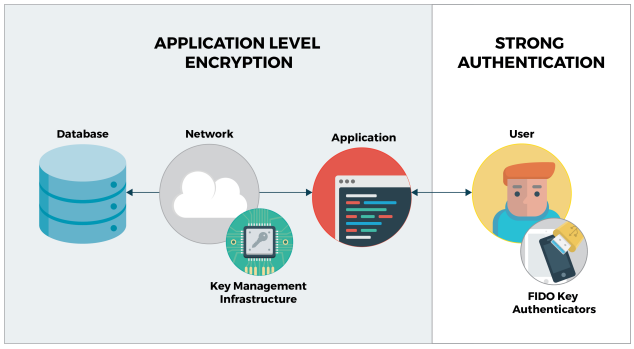
STRONGKEY

How can you mitigate the risk of a data breach?

Application Level Encryption & Strong Authentication (ALESA)



While we all recognize that encrypting sensitive data can protect you, most people—even those in the security business—don't realize that not all encryption is equal. Even if using NIST-approved algorithms with the largest key sizes available, data can still get breached. How is that possible?

When encrypting data, all else being equal from a cryptographic point-of-view, two design decisions matter most:

1. Where is data being cryptographically processed?
2. How are cryptographic keys managed?

If data is encrypted/decrypted in any part of the system (hard disk, operating system, database, etc.) other than the business application using that data, significant residual risks remain despite the encryption. An attacker need only compromise a software layer above the encrypting layer to see unencrypted (plaintext) data. Since the application layer is the highest layer in the technology stack, this makes it the most logical place to protect sensitive data as it affords the attacker the smallest target. This also ensures that, once data leaves the application layer, it is protected no matter where it goes (and conversely, must come back to the application layer to be decrypted).

The second design decision of encryption is how to protect cryptographic keys. If you use a general-purpose file, keystore, database, or device to store your keys, this would be the equivalent of leaving company cash in a desk or drawer. Much like the need for a safe to store cash in a company, you need a purpose-built key management solution designed with hardened security requirements to protect cryptographic keys. These solutions have controls to ensure that, even if someone gains physical access to the device, they will find it very difficult (near impossible) to access the keys. If the key management system cannot present sufficiently high barriers, even billion-dollar companies can fail to protect sensitive data.

While cryptography tends to get complex and the details might seem burdensome, it is important to recognize that **an encryption solution provides the last bastion of defense** against determined attackers; it is well worth a company's time to give it the proper attention and not attempt to invent it themselves.

Conversely, **the first line of defense should be strong authentication.** Strong authentication is the ability to use different cryptographic keys combined with secure hardware (in the possession of the user) to confirm that the user is who they claim to be. While digital certificates on smartcards provided such capability for over two decades, they are expensive and not easy to use or support, even in highly technical environments. A standards group (fidoalliance.org) has simplified this problem and made FIDO authentication easily available today. StrongKey provides a FIDO server that removes both the burden and insecurity of passwords from applications.

Between application level encryption on the back end and strong authentication on the front end, an attacker will have little wiggle room to compromise sensitive data, even if they manage to slip past network defenses. While no security technology is absolutely foolproof, when implemented correctly, ALESA raises the bar sufficiently high to encourage the vast majority of attackers to move on to easier targets.

STRONGKEY'S VALUE PROPOSITION

Company	Based in Silicon Valley, CA and Durham, NC, StrongKey brings: • A 17-year history in enterprise data solutions development • Customers on six (6) continents • 100% open-source solutions
What we do	We protect access to web-applications using new industry-standard protocols from **FIDO Alliance** while eliminating user ID-passwords, and sensitive data, including: • Personally-identifiable information (PII) • Healthcare data (HER, lab reports, X-rays, MRIs, prescriptions, etc.) • Financial data (bank, credit card, pension, mortgages, statements, etc.) • Backups of databases, archived records, and files • Other files (images, blueprints, audio, video, ISO/OVA files, etc.) • Cryptographic keys for self-encrypting drives (SSL/SSH keys, etc.)
Our products	StrongKey Tellaro T100 – Medium Enterprise Solution StrongKey Tellaro E1000 – Enterprise Appliance
Encryption & Tokenization	Enable encryption, tokenization, cryptographic key management, and ANSI DUKPT processing for card-present transactions
Authentication	Leverage a FIDO Certified server for managing tens of millions of FIDO U2F public keys for strong authentication.
Internal File Protection	Use a FIDO-enabled web application to encrypt files within closely controlled ecosystems, providing centralized key management and integrated with AD and OAM for authorization management
PKI2FIDO	Register a FIDO key after strongly authenticating with an X.509 digital certificate in a TLS ClientAuth session, thus leveraging existing level of assurance process
Document and File Encryption	Orchestrate the encryption and decryption of millions of files by using a private cloud of StrongKey software.
Site Certificate Management	Acquire free TLS certificates with the click of a button from LetsEncrypt.org and manage all TLS certificates centrally

StrongKey
Durham, NC & Cupertino, CA
Phone: +1 408-331-2000
E-mail: getsecure@strongkey.com
Web: strongkey.com