SOLUTION BRIEF

MOVE BEYOND THE SHORTCOMINGS OF ENCRYPTION WITH ALTR

ALTR eliminates the false sense of security created by encryption solutions

To most, encryption is synonymous with ironclad protection for data exchanged and stored at rest. Modern data encryption is extraordinarily complex, with keys that theoretically can't be brute-force cracked in less than a billion years (though quantum computing may soon reduce the time).[1]

While the concept of encryption has been around for most of human civilization, today's encryption makes Renaissance-era cipher disks and the Enigma machine look like toy decoder rings. Still, the principle remains relatively the same as it always has: scramble a message with a secret key, hand off the message, and rest assured that anyone who might intercept the message will have little chance of making sense of it without the key. This simple approach gets more complex with modern computing power, and 256-bit encryption is considered essentially unbreakable.

So what's the problem? Why are there any data breaches at this point? As with all things security, there are vulnerabilities and shortcomings that keep encryption from being the security cure-all it purports to be.

THE HUMAN FACTOR

On paper, encryption sounds bulletproof, but — as with basically all forms of security — the biggest flaw is that the encryption is implemented and used by humans.

Encryption is only as secure as the key. If you have the key, you have the data. If an end-user has an encrypted laptop but keeps their password on a sticky note, the encryption is meaningless.

Likewise, while corporate policies requiring encryption may seem like surefire ways to ensure security, a policy is only useful so much as it can be implemented. Consider Coca-Cola. The company has a reputation for carefully safeguarding its secret formula and its corporate data. Nevertheless, in 2014 a data breach compromised the sensitive data of 70,000 employees following the theft of multiple laptops by a former employee. The company had a strict policy requiring the encryption of end-user devices, but the stolen laptops were unencrypted.[2] Policies calling for encryption are useless if all end-users aren't adhering to them.

LACK OF ADOPTION AND REQUIREMENT

Even with the prevalence of encryption products on the market, one of the biggest problems for encryption is the fact that it's often not used in business. A surprising amount of sensitive corporate data is completely unencrypted. Only 45% of enterprises report applying encryption consistently across their organization,[3] and more than 90% of IoT communications within enterprises are completely unencrypted.[4]

Only 45% of enterprises report applying encryption consistently across their organization.

Many assume encryption is required by recent privacy law changes. In actuality, there are few laws and regulations in place that explicitly require encryption, despite the popular misconception. Regulations like GDPR (the EU's General Data Protection Regulation) and CCPA (the California Consumer Privacy Act) have impacted organizations across industries and the world, and while both call for using reasonable measures to protect data, both fall short of specifically requiring it.

However, it's important to remember laws and requirements are written from a position of common language and known technologies, and the intent and spirit of the requirements are the most important aspect. As for CCPA, the language reads: "Any consumer whose nonencrypted or nonredacted personal information…", and the GDPR mentions "pseudonymization and encryption." Ultimately, the solution does not have to be encryption.

THE COSTS OF ENCRYPTION

Even in organizations where encryption is available and actually used, there are several common reasons end-users break the system. Encryption comes at a cost that can make it impractical to use.

Managing keys is complex and performing decryption can be too much of a hit to performance and availability. Encryption can impact the usage of data too much, stifling workloads and creating performance bottlenecks, especially with larger datasets. The more data used, the more massive the processing load — and the cost.

Another problem? Data is often decrypted for use and then left unprotected when developers, marketers, or data scientists working with data decrypt and copy it somewhere unprotected — often in the cloud. Given the choice of security or speed and ease, users typically opt for speed.

Encryption can work in simple scenarios where data isn't used often (like in cold storage), and isn't shared often (minimizing key management pains). It also works better for data that doesn't have long-lived value to thieves. With encryption, the source (sensitive) data is still there within the encrypted value. This is why it's still dangerous — it can be broken and accessed later. Encrypted datasets can be brute-force decrypted over time or when technology becomes available — a serious problem as quantum computing becomes more accessible.

SIMPLE, PERFORMANT PROTECTION

The solution is to find a powerful way to protect data that is so painless to implement that your organization doesn't even realize it's in place. It can't affect

performance, it needs to be usable for the business, and it must not have a key that can be stolen.

ALTR makes it possible for organizations to keep sensitive data secure — simply, cost-effectively, and without creating bottlenecks.

ALTR offers a comprehensive suite of services designed to mitigate the risk of direct access to data. Sensitive data is stored in a cloud vault that encodes and fragments data across a distributed datastore based on blockchain technology. ALTR monitors all data requested and accessed, providing a real-time immutable audit trail. This means no one can put the data back together without going on the record.

While encryption puts a lockbox around your source data, the sensitive date is still inside and able to be accessed down the line. Unlike encryption, ALTR has no keys or maps to steal and can't be broken with math, now or in the future. By using tokenization, ALTR ensures there is no source data to access — the tokens are useless to would-be thieves.

ALTR's protection is conveniently available as a service, meaning security can be applied anywhere across multiple parties without compromise. Similar to the tokenization that is used in the payment industry, ALTR's superior performance and speed is ideal for transactional data, and added governance capabilities ensures that data can't be accessed or copied without express permission.

ALTR also protects data in other instances where encryption solutions may leave it vulnerable. Encryption often exposes data in use because you can't operate on encrypted data. To get around this, many encryption products decrypt the data and hold it in memory, leaving it unprotected. The stored data may still be encrypted, but the entire dataset is right there on the server waiting to be stolen. Because ALTR is so performant, this workaround isn't necessary.

When referring to ALTR's unique approach to security UHY, ALTR's compliance service provider, says, "As a consultant, [we] have the privilege of meeting and seeing clients in many different industries and in various states of distress related to cybersecurity ... We see numerous successful strategies and products that are helping our clients meet compliance objectives and improving their security postures. We've seen the success of one of our own clients providing a security solution that is easing compliance obligations in healthcare, card payments, and privacy in ALTR. We believe all our clients with compliance and data protection obligations should explore the ALTR solution as a solution with strong possibilities for reducing scope and reducing risk in the organization."

For most businesses, encryption can simply be too costly, complex, and vulnerable. ALTR offers security-conscious organizations a simple and superior alternative to encryption.

Watch ALTR customer Q2 discuss best practices for keeping sensitive financial data safe.

Contact us to learn more about how we can help your organization move past the inherent problems with encryption.