Mitigate Ransomware Extortion with File Encryption

Ransomware, doxware, exfiltration, extortion, whatever the attack may be called, at the end of the day it results in an unauthorized third-party gaining access to your company's data. These attacks have evolved from locking up your data to stealing customer files with threat of exposure. Atakama's file level encryption can mitigate the worst of these attacks -- file exfiltration.

What's changed?

Past attacks focused on preventing the organization from accessing its own data by introducing malicious software that encrypted files across the organization. Unable to carry on its daily business, the company would either attempt to decrypt the files on its own, or be forced to pay the attacker a ransom to obtain the decryption key. No company wants to be in that situation. But, unfortunately for security practitioners, the adversary has gotten smarter and meaner. Realizing the pain point could be made way worse than simply preventing the company from accessing its own data, the threat of stealing and threatening to publish customer files has become more lucrative. Being unable to access your own files stinks, but the thought of your customer files that have been entrusted to you made public is way worse. From the harm to reputation, to the regulatory nightmare, and the financial recourse, the stakes are now higher.

What hasn't changed?

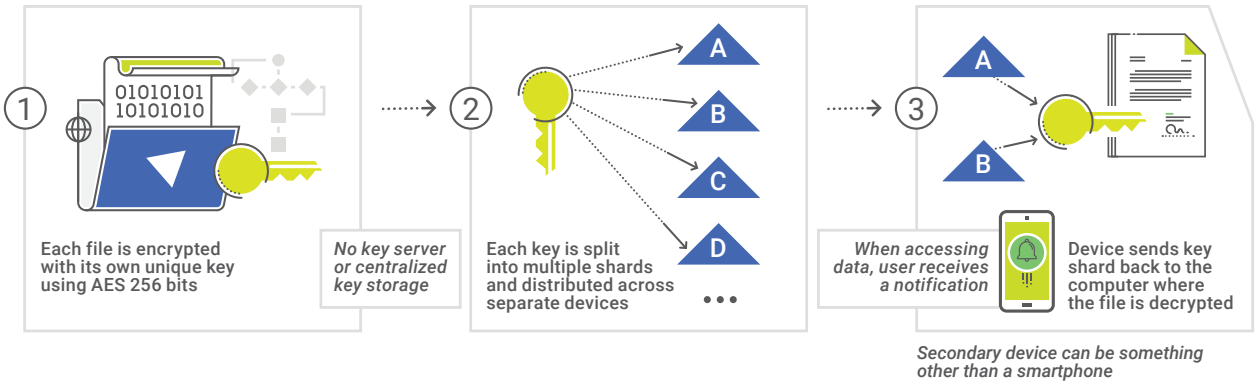
Continued reliance on identity and access management (IAM) controls. Too often, organizations are overly reliant on passwords and multi-factor authentication to defeat breaches. We're not saying IAM is not important, of course it is! However, relying solely on IAM is no longer sufficient. Social engineering attacks are increasing at an exponential rate. They have also become more unpredictable and more difficult to detect. Atakama's file level encryption is disconnected from IAM, so that even if someone is able to break into a system or network, individual files would largely remain inaccessible.

File Level Encryption to Thwart the Attack

Traditional encryption solutions are heavily dependent on identity and access management controls. Login credentials, which allow authorized users to access encrypted data, represent a single point of failure. Atakama enables the encryption of files at a granular 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 separate 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 by those individuals or groups it is intended for. And Atakama accomplishes all of this without disrupting existing workflows or creating user frictions.

Atakama goes beyond traditional encryption solutions. Where other encryption bulk decrypts the instant a user (or adversary) is authenticated, Atakama’s approach is to separate file encryption from user authentication. Without reliance on traditional authentication mechanisms files always remain encrypted when at rest, even to an adversary who is able to gain access to the network. The only thing the adversary would be able to exfiltrate are encrypted files, but because those files are Atakama encrypted they are rendered useless in the attack. By doing so, Atakama nullifies any attempt to ransom or otherwise extort company files.

How it Works



Visit www.atakama.com, or contact info@atakama.com to learn more about how Atakama’s multifactor file level encryption can help you mitigate the threat of file exfiltration.