SOLUTION OVERVIEW

CYBERSECURITY

Enhanced Information Security Through Multi-Factor Encryption

Traditional encryption solutions are heavily dependent on identity and access management controls. User-credentialed applications, group privileges, and third-party data entitlements all require login credentials, which when successfully entered allow the "authorized" user to access everything they have been permissioned to see. Organizations that continue to associate these access controls with information security will eventually experience devastating results. Technologent and Atakama's multi-factor encryption is far more secure than the standard tools.

Multi-factor file Encryption Made Easy

- No usernames or passwords
- Decentralized key architecture with no central key server to attack
- OS-native interface for file access
- Optimized to integrate with existing network and cloud storage locations

Protect Your Bottom Line With Technologent And Atakama's Data Security Software

Regulatory Compliance

Most cybersecurity regulations now require encryption of data at rest. And it's what customers have come to expect.

Secure Confidential Information

Encrypt files that need to be secured: earnings reports, HR, M&A, IP, legal, risk, regulatory, PII, etc.

Mitigate Ransomware

Ransomware attacks that involve doxxing are on the rise. Our team can help nullify the harm from an attack and eliminate the threat of doxware.

Cloud Enablement

Switching from on-prem to cloud has never been safer. We ensure that only encrypted versions of files live in the cloud.

How It Works

Location-based encryption without passwords. Simply drag and drop to encrypt files. This convenient user experience makes it easy and selfexplanatory for employee adoption.

Distributed key management. Each file saved to the Atakama-enabled location is automatically encrypted using AES with a 256 bit key. The unique key for each file is then automatically fragmented into "key shards" and distributed to users' physical devices.

Untethered from identity and access management. Users open files using their mobile device. Simply tap approve and the file opens. Or launch a session during which multiple files can be opened without the need to tap approve for each file.

Seamless integration and deployment. Whether your business stores files on a network drive, in the cloud, or a hybrid of the two, Atakama is easily deployed and installed within your existing environment.

|

Business Benefits

Regulatory Compliance

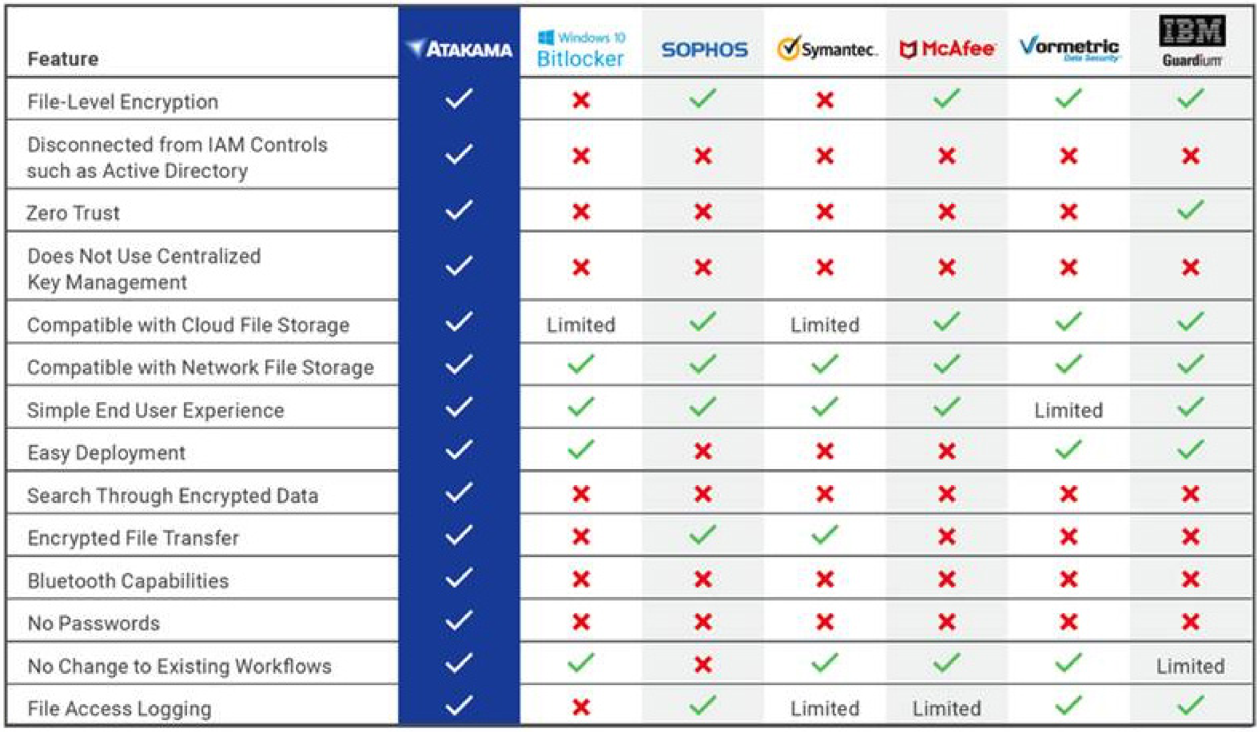
Zero Trust

Cloud Security

Endpoint Security

Stop File Exfiltration

Technologent & Atakama Vs The Competition



Feature	ATAKAMA	Windows 10 Bitlocker	SOPHOS	Symantec.	McAfee	Vormetric Data Security	IBM Guardium
File-Level Encryption	✓	✗	✓	✗	✓	✓	✓
Disconnected from IAM Controls such as Active Directory	✓	✗	✗	✗	✗	✗	✗
Zero Trust	✓	✗	✗	✗	✗	✗	✓
Does Not Use Centralized Key Management	✓	✗	✗	✗	✗	✗	✗
Compatible with Cloud File Storage	✓	Limited	✓	Limited	✓	✓	✓
Compatible with Network File Storage	✓	✓	✓	✓	✓	✓	✓
Simple End User Experience	✓	✓	✓	✓	✓	Limited	✓
Easy Deployment	✓	✓	✗	✗	✗	✓	✓
Search Through Encrypted Data	✓	✗	✗	✗	✗	✗	✗
Encrypted File Transfer	✓	✗	✓	✓	✗	✗	✗
Bluetooth Capabilities	✓	✗	✗	✗	✗	✗	✗
No Passwords	✓	✗	✗	✗	✗	✗	✗
No Change to Existing Workflows	✓	✓	✗	✓	✓	✓	Limited
File Access Logging	✓	✗	✓	Limited	Limited	✓	✓

The Technical Details

Technologent and Atakama enable the encryption of files on an individual level without reliance on usernames and passwords. Atakama is deployed for users as a light-weight endpoint agent. The agent creates a mount point, where all files are encrypted with their own unique AES-256 bit key. Each key is fragmented into shards, with the shards distributed across physically separated devices, included, but not limited to, users' workstations and their smartphones. Shard fragmentation uses threshold cryptography: an M-of-N process, in which the total number of shards (N) and the required number of shards (M) for decryption are parameters that can be customized by an administrator. There are no usernames, passwords, or other memorized secrets for our team to operate.

Automatic Encryption And Decryption For Authorized Users

New key generation occurs automatically upon saving or moving files to the Atakama-enabled location. Shards of the new key are distributed instantly once the file is encrypted. Decryption occurs seamlessly, with a user clicking on a file and receiving a notification on their smartphone. The notification is a request for the smartphone to provide the relevant shards to decrypt the file.

Initiate Customized User Sessions

Users can also request and open multiple files at once or launch a session during which files can be decrypted without the user receiving prompts for each file. The admin may designate the length of time and the maximum number of files that can be opened during the session.

With the use of sessions, users need not access their mobile devices more than once per day, yet data remains encrypted until accessed by the user.

The UX is much like SSO or 2FA. The underlying security, however, is far more powerful, as it is not permission-based, but encryption-based and with no central points of failure.

Seamless Network And Cloud Integration

Underlying encrypted data (the AES-256 encrypted data seen by the user within the Atakama mountpoint) can reside within a network drive or within a cloud storage provider such as Box, Dropbox, Google Drive, OneDrive, or a private cloud.

Technologent and Atakama's cloud integration enables cloud-stored data to remain encrypted at all times, thus never having to rely on a cloud provider's authentication or security infrastructure.

Unlike other encryption software, our security solution does not interfere with or interrupt existing and expected user behaviors and workflows:

- Users can share files via network mounts and cloud storage providers just as they have in the past.
- Users can search through their encrypted data without decrypting it, using our patent-pending version of Searchable Symmetric Encryption.
- Visual cues within the native file explorer window are always available to indicate to the user whether a particular file is encrypted.
- Users can replace lost devices effortlessly without any friction to the user experience.

About Atakama

Atakama provides unparalleled data protection for businesses without any disruption to users' expected workflows. Users have all of the advantages of traditional file systems, and by removing all barriers that would have prevented an enterprise from relying on object-level encryption, there is no reason not to deploy the strongest possible security: file-level encryption.

About Technologent

Technologent is a Global Provider of Edge-to-Edge™ Information Technology solutions and services for Fortune 1000 companies. We help our clients outpace the new digital economy by creating IT environments that are agile, flexible, efficient, transparent and secure. Without these characteristics, companies will miss the opportunity to optimally scale. Technologent mobilizes the power of technology to turn our clients' vision into reality, enabling them to focus on driving innovation, increasing productivity and outperforming the market.