End-to-End Storage Security (ETESS)

Extenua created ETESS™ as a platform purpose built for today's hostile environments with the massive and destructive cyber-attacks companies face each day.

ETESS is significantly more hardened than the industry's end-to-end encryption (E2EE) method for secure communication.

- ✓ ETESS is <u>not susceptible</u> to common successful attacks such as man-in-the-middle MITM attacks
- ✓ ETESS is <u>not susceptible</u> to endpoint attacks which steal a stored encryption key

Nobody in between, be they an Internet service provider, application service provider or hacker, can read or tamper with data which is managed within our ETESS platform utilizing Cloud2Drive.

ETESS **Distinct Advantage**

ETESS never allows the actual encryption keys to be stored anywhere!

- ETESS generates keys and destroys keys dynamically in RAM at the moment the key is needed to encrypt or decrypt the chunk or slice of the data
- ETESS generated encryption Keys are always generated at the end node for absolute control
- ETESS is generating many unique keys developed based on a set of rules and circumstances that trigger a specific transformation of the random pool.
- ETESS uses a random data pool that resides in various locations, in the cloud, on-premise storage pool and the client machine. The random data pool is encrypted as well.
- ETESS uses Eliptic Curve Diffie-Hellman with our unique assembling and decrypting the random pool while calculating each transformation of the pool then extracting Initialization Vectors and Keys from the pool thus encrypting/decrypting the file chunks at each endpoint independently.