Capabilities	ARMORTEXT
True End-to-End Encryption (For Client-Eyes-Only)	✓
Secure Messaging & Fileshare (Any OS, Device, Tablet & Desktop)	✓
Secure 1-on-1 & Group Messaging	✓
Enterprise Controls	✓
Information Lifecycle Controls	✓
Compartmented Communications & Risk Reduction Strategy	✓
Admin w/o Read Access (No Snowden Effect)	✓
Cryptographically Enforced Scopes of Review	✓
No Proprietary Hardware or Infrastructure Requirements	✓
Encrypted Voice	**Q2 2018** - In Beta
Encrypted Video Conferencing	**Q3 2018** - In Beta
Archive Integrity Verification	**Q4 2018** - In Beta

Your business conversations, videos, and files encrypted end-to-end.

Available on any major desktop or mobile device. ArmorText can't decrypt or read customer data. Built for Defense & Government Advisory Services, Energy & Utilities, Legal, Healthcare, and Financial Services. With Enterprise Governance, Data Retention & Review, and Information Lifecycle Controls.

No other platform provides all of the ***essential elements*** for Risk Reduction, Regulatory Compliance, Internal Accountability, and Verification of Document Authenticity

Guards against unintended disclosures (plain view doctrine)

Patent Pending

To discern the difference between ArmorText and our competitors all you have to do is ask the right questions.

Encryption & Security

- What is the nature of encryption involved? SSL/TLS? End-to-End Encryption? Ramifications?
- If encrypted end-to-end, where are keys stored / managed? What infrastructure is required to operate?
- For cloud-based solutions, are communications at any time decrypted or available in plain text to the provider?

Governance, Review, and Remediation

- If encrypted end-to-end, can communications be reviewed by internal compliance, governance, general counsel, or other specific roles? If so, how?
- Is there a clear segregation of duties between administrators and those with review capabilities to help address insider threats?
- Do actions such as remote-wipe or device lockout require an MDM? What capabilities are built-in to address lost, stolen, or compromised devices?
- Can various jurisdictions / markets be independently administered and or reviewed while still enabling communications between each market?

End-User Experience

- What file types are supported? What are the size limitations for attachments?
- Is the solution available across commonly used desktop & mobile devices? E.g. Windows, Mac, Linux, iOS, and Android?
- What is the upper limit per conversation for participants? 10? 20? 30? 40? 50?
- How many devices can a user have? E.g. tablet, desktop, and phone? Does the number of devices impact max group conversation size?
- Are messages sent & received by users visible to them across their various devices?
- What other communications capabilities besides messaging & file sharing are supported? How are these secured?