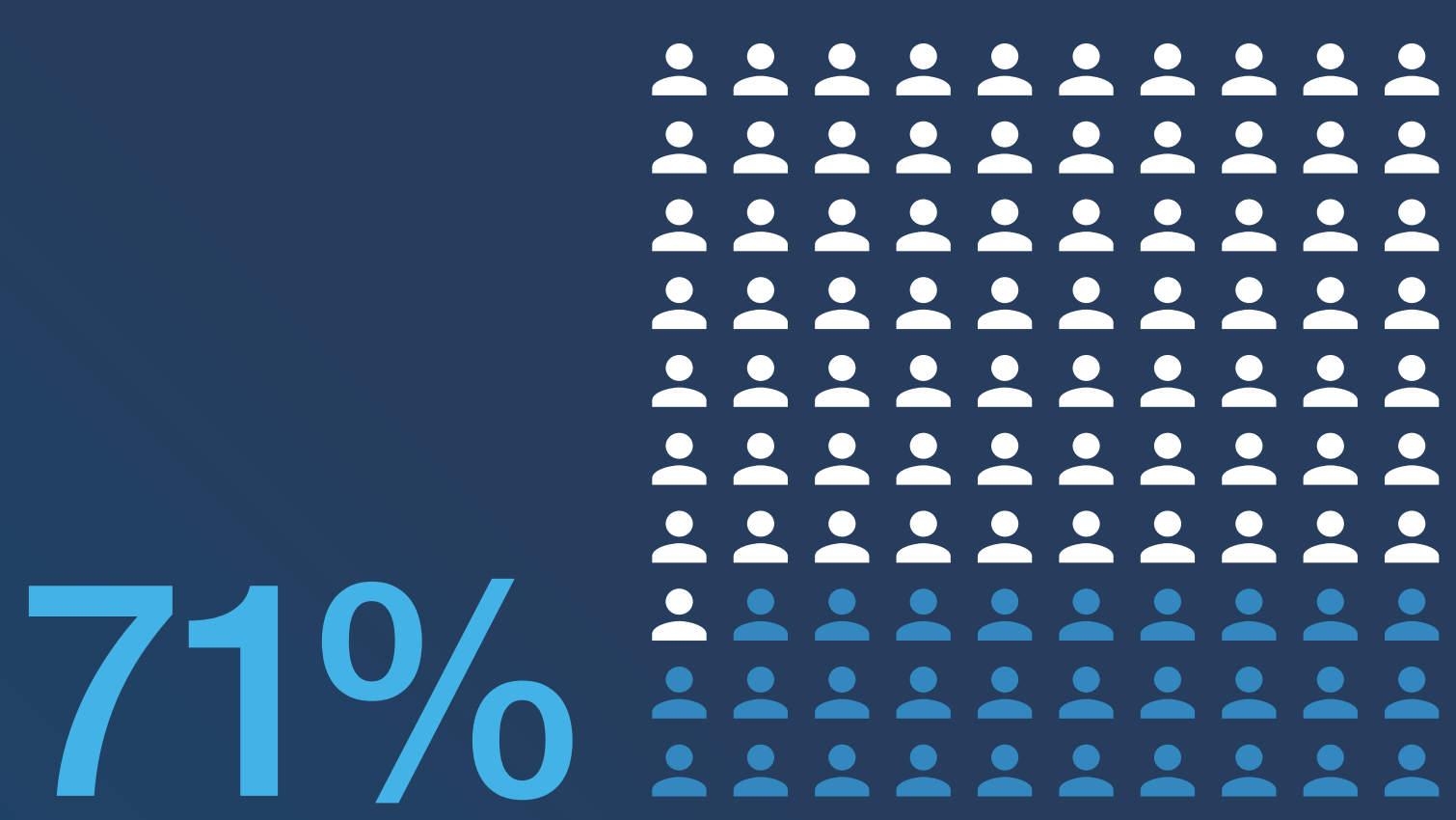


# Do You Know Who Has Access to Your Company's Collaboration Data?



**71%**

of Fortune 500 CXOs say cybersecurity is their **MOST significant business challenge**.<sup>1</sup>



**4%**

of data breaches **are made useless by encryption**.<sup>2</sup>



Collaboration platforms encrypt data **at rest** and **in motion**. In the cloud, your data is **repeatedly being decrypted** for processing.

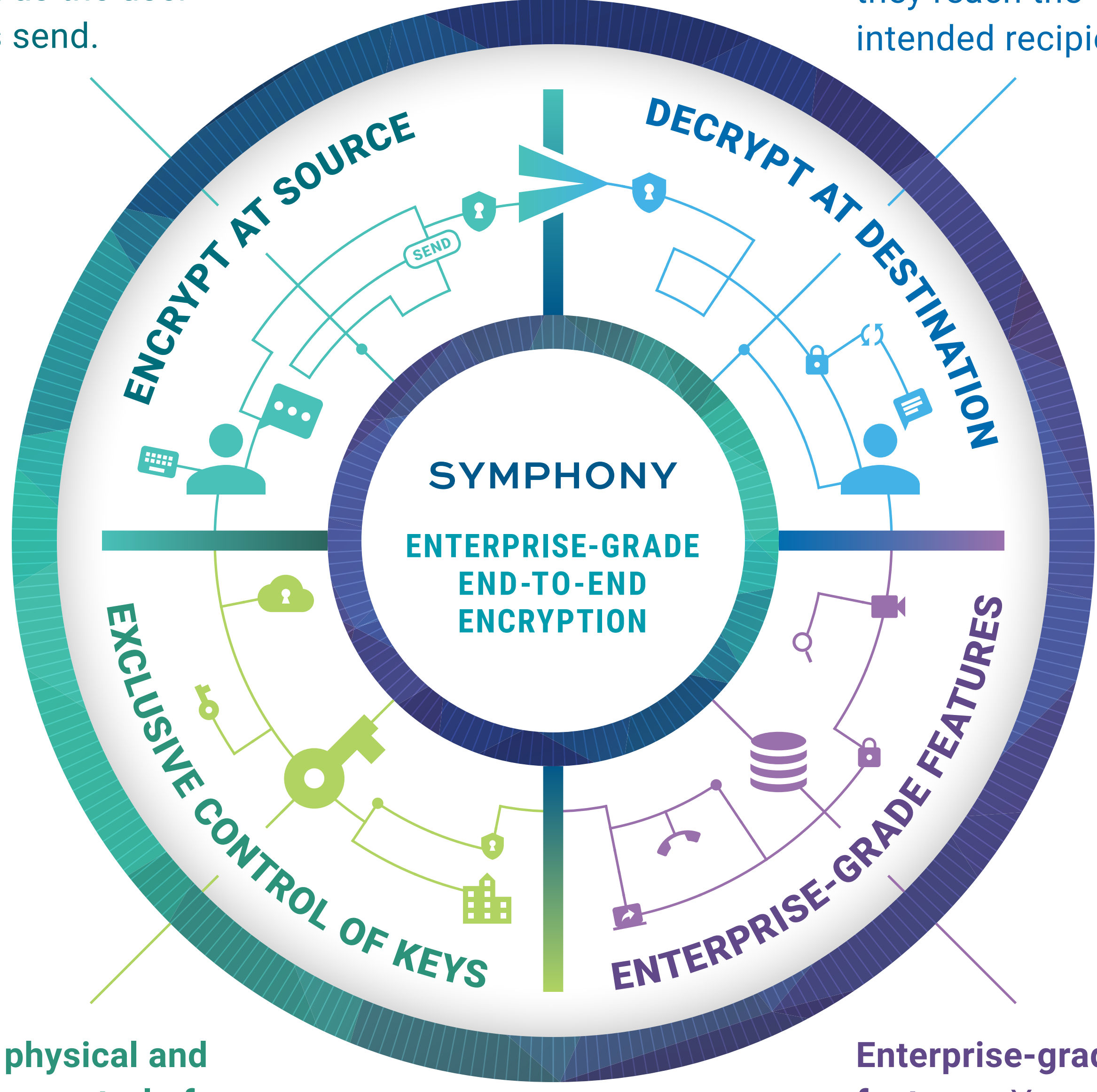


Once decrypted, **your data can be scraped, shared, used or hacked** by service providers and hackers alike.

## COLLABORATE WITH CONFIDENCE – PROTECT YOUR INFORMATION WITH SYMPHONY'S ENTERPRISE-GRADE END-TO-END ENCRYPTION

**Encrypt at source.** Messages are encrypted as soon as the user presses send.

**Decrypt at destination.** Messages are never decrypted until they reach the intended recipients.



**Get full physical and exclusive control of encryption keys.** This means Symphony or hackers cannot decrypt your data in the cloud.

**Enterprise-grade features.** You still get record retention, encrypted search, and real-time audio/video.

### 👍 THE UPSIDE?

IF YOUR COLLABORATION CONTENT IS BREACHED IN THE CLOUD, IT CONTINUES TO BE **ENCRYPTED AND CANNOT BE READ.**

All encryption is not created equal. Insist on end-to-end encryption for **SECURE TEAM COLLABORATION.**

LEARN MORE AT [SYMPHONY.COM/SECURITY](https://www.symphony.com/security)

FOLLOW US ON

Note: Some features require the Symphony Enterprise offer. Data sources accessed on 30 May 2018.  
 1 <https://www.baesystems.com/en/cybersecurity/feature/cyber-defence-monitor-2017-intelligence-disconnect>  
 2 <https://breachlevelindex.com/>