

All current trend-lines lead to more data breaches. As agencies are investing security dollars to extend the life of the antiquated breach prevention strategy, adversaries are continuing to innovate and thrive. Furthermore, the extension into the cloud and into the tactical field is greatly increasing the potential attack surface and likelihood of accidental data exposure or loss. These trends all point to a consistent theme: security needs to be attached to the data, so agencies can maintain control of the data from the core to the cloud to the field. Trying to keep today's adversaries out of the organization through breach prevention is a fool's errand.

Session attendees will learn how to create a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. This session will discuss:

- Encryption strategies to protect data and rest and in motion from the core to the cloud to the field
- Importance of protecting and managing cryptographic keys
- Best practices for controlling access to data
- How to securely share mission critical information while ensuring the exchange of correct and authorized data with authorized recipients