druva inSync Battle Card

Elevator Pitch: Druva inSync addresses the enterprise's need to achieve data visibility, recoverability and manageability of dispersed data across endpoints and cloud applications including Office 365 (OneDrive and Exchange Online), Google Apps for Work (Google Drive, Gmail and Google Docs) and Box. As an integrated converged data protection solution, inSync provides availability and governance capabilities to ensure the highest level of protection and safeguards to the enterprise, delivered on a highly elastic cloud infrastructure. With inSync, companies regain visibility and control of corporate data, minimizing data threats, while facilitating business continuity, and employee productivity.

Sweet Spots

	Data Center Backup	✓	Ransomware Recovery
✓	Endpoint Backup	✓	Search and Audit
✓	Cloud Apps Backup	✓	eDiscovery Enablement (Legal Hold)
✓	Long Term Archival	✓	Automated Compliance Management
✓	File Sync and Share	✓	Data Loss Prevention

Technical Buyer:

Frontline IT Manager

Role: Technical Evaluation

Goals and Triggers:

- End-User satisfaction
- Ease of rollout/deployment
- Reduction in helpdesk tickets
- Higher product functionality and performance
- In charge of day-to-day activities

Strategic Buyer:

CIO/CISO/Legal/Compliance

Role: Strategic Project Initiator

Goals and Triggers:

- Prevent risks and ensure compliance
- Sensitive data protection
- Ensures data policies (compliance) are met
- Ensure legal defensibility
- Minimize eDiscovery costs

Opportunity and Qualification

Pain Point	Qualifying Questions	Anxiety Questions	Solution - Druva inSync
Data Breach and Security Risk on endpoints (BYOD)	• How do you prevent data breach on lost/stolen devices? • How do you address data protection on endpoints?	• What happens if your sensitive data is lost on an end point? • Is your customers' data at risk on mobile devices? Do you protect it?	• Integrated DLP to eliminate data breach on lost/stolen devices by encrypting endpoint data, enabling admins to remotely wipe corporate data or automatically wiping data if the devices does not connect • Data encryption prevents any 3rd party data access, including Druva.
Availability: Data access with no risk to data loss (ransomware, accidental/malicious data deletion or data corruption)	• Do you backup & archive corporate data on endpoints and cloud apps?	• Have you ever lost critical user data on endpoints and/or cloud applications?	• Mobile containerization, Data Backup, archival and recoverability for mobile and cloud apps so enterprises never lose data accidentally or maliciously while ensuring end-user privacy and not productivity loss
IT Governance: Search & audit, legal hold (eDiscovery enablement) and regulated data compliance management	• How do you collect and preserve data (perform legal hold) on endpoints and cloud apps? • How do you proactively manage	• What is your process for placing legal holds on files on mobile devices if audited or presented with litigation? • How do you ensure your users are not violating any data regulations?	• Integrated governance for endpoints and cloud apps • Built-in legal hold workflow for eDiscovery to quickly collect and preserve data in place for investigative or litigation needs • Automated compliance management powered with full text search capabilities and built-in compliance templates (e.g. HIPAA, GLBA, PHI/PII related) to monitor for potential data risks and easily meet data regulations • Federated search to quickly locate files

druva inSync Battle Card

Key inSync Differentiators

Data Governance including Investigative Audit & Search, Automated Compliance Management and eDiscovery Enablement for Endpoint and Cloud Apps

inSync is the industry's first integrated solution to combine user data across laptops, mobile and cloud apps like Office 365 (OneDrive and Exchange Online), Google Apps for Work (Gmail, Google Drive and Google Docs) and Box to provide enterprises with centralized visibility and control to meet their data governance requirements. With a single dashboard for governance, inSync provides a unified platform for IT and legal administrators to easily manage legal holds, provide secure data access for eDiscovery and monitor (automated compliance management) for potential data risks (e.g. HIPAA, PHI/PII related) to easily meet data regulations.

Up to 80% Savings in Data Storage and Bandwidth

Unlike other solutions that only eliminate data redundancy on each device, inSync's patented global deduplication delivers high-speed, lightweight backups with savings up to 80% on storage and bandwidth. inSync achieves this by deduplicating data at the block level globally across all users/devices/cloud apps so that only unique data blocks are transferred and stored.

Security and Data Privacy

Druva's approach to storing enterprise data, utilizing both an advanced data scrambling algorithm and a unique envelop-based encryption model, where the data and meta data are decoupled and encrypted, guarantees that your data is only accessible by your company. Under no circumstance can Druva provide access to your data — a critical component to meeting today's stringent global data privacy regulations.

Global Availability and Durability

Natively built for the public cloud, inSync provides global organizations with multiple data centers to meet their varied regional data privacy requirements within a single cloud solution. inSync's cloud data center replication and multi zone redundancy provides the highest availability and data durability (99.5% Availability, 99.99999% Data Durability). Furthermore, the data centers utilized by Druva not only carry extensive certifications for securing and protecting stored data but are also compliant with national privacy laws.

Opportunity and Qualification

Objection	Response
1. "I don't need a backup solution" or "I already have a file sync and share solution"	File Sync and Share (EFFS) is not backup. Although sync can complement backup, it's not a substitute because services like Box or OneDrive aren't designed to protect data over time, especially in regards to rogue/accidental deletion or when data needs to be archived and stored when an employee leaves because the data might be regulatory in nature or subject to legal investigation. In addition, syncing only makes a subset of your files available to other devices or people, where as backup solutions securely backs up and keeps all your files safe so you can restore when needed.
2. "For OS migration, I have USMT and it's free"	Most tools like USMT from Microsoft are time-intensive, complex to configure, offer no bandwidth reduction and are designed for small scale migrations. But as organizations deal with larger volumes of devices, OS migrations become unmanageable. Because deduplication is not addressed with custom coding, high storage requirements increases the cost of the migration process with USMT. Limited reports and alerts make monitoring backups or restores for thousands of devices extremely difficult. Other drawbacks of USMT include no access to files during migration (i.e. no file sharing) and costly in terms of storage and bandwidth.
3. "Our employees collect and preserve their own data"	If left in the hands of employees, visibility and control can end up being completely out of organization reach and can increase the risk to data spoliation. inSync automates the legal hold process and ensures IT governance of endpoint and cloud app data with its comprehensive policies and audit trails. Regardless of how frequently your business is involved in litigation, two questions to answer are: a) do we have data on laptops, mobile devices and cloud applications included in our legal holds; and b) how do we ensure that there is no accidental deletion or incomplete preservation of data?