



# InSync SafePoint:

*Safeguarding your Endpoints With Data Loss Prevention*

Chandar Venkataraman  
Chief Product Officer, Druva

(c) Druva Software 2011 June 11

# EndPoint Data: Most Critical, yet Least Protected

“One laptop is stolen every 53 seconds in the U.S. You have a 1 in 10 chance of having your laptop stolen this year”

- Gartner Group

"Laptops are always consistently the greatest risk in any given security assessment.”

- “The Billion Dollar Lost Laptop Problem”,  
Intel, Sep 2010



## High Economic Impact

• **\$49,246**

= the cost of a lost, unprotected laptop\*

### Costs include:

Replacement cost

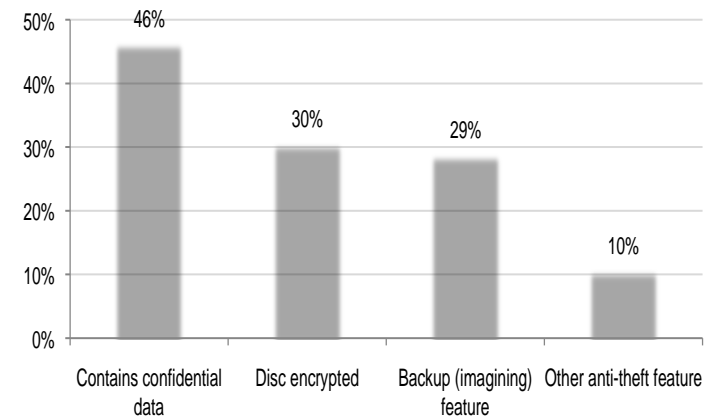
Detection, forensics

**data breach (80% of total costs)**

lost IP costs

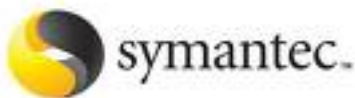
lost productivity

legal, consulting and regulatory expenses



# Existing Solutions Ineffective

- **Excessive Costs to Purchase and Deploy** – Most DLP solutions are out of reach in terms of cost to purchase, deploy, and maintain
- **Complexity of Deployment** – It's difficult for IT to implement centralized policies across many point solutions (backup, restore, encryption, data shredding, etc.)
- Point solutions are **at odds with end-user productivity** (too heavyweight, slows performance, obtrusive, makes normal operations difficult, etc.)



“Symantec, the dominant vendor in the market, relies on its consulting partners to guide its deployment and selling processes. This strategy relies on selling DLP as a methodology on par with ERP or CRM.”

*Andrew Jaquith, Data Leak Prevention Suites, Q4 2010  
Forrester Research*

# Druva inSync SafePoint

- **Simple, lightweight, effective** data loss prevention solution for laptops and mobile devices
- Seamlessly integrates with Druva InSync
- **Centralized, policy-based**
- Offers **multi-layered data loss prevention** meeting NSA security standards:
  - Data Encryption
  - Data Delete
  - Device Trace



# Data Encryption

## 1. Central Encryption Policy

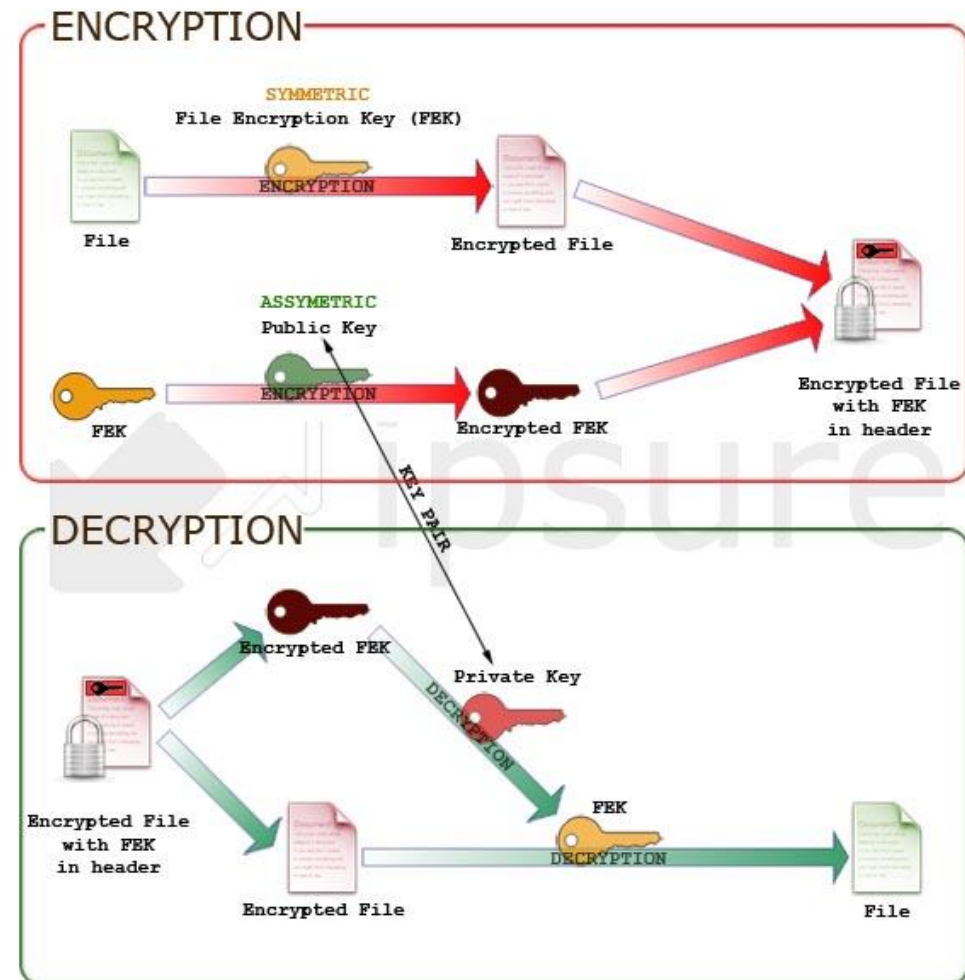
- A simple policy that automatically encrypts files selected for backup
- Same inclusion/exclusion criteria as backup
- Easy to administer, but powerful

## 2. File-level encryption

- Uses Encrypting File System (EFS) for file-level encryption on an NTFS volume
- 256-bit AES algorithm for encryption/decryption

### 1. User-Transparent

- Completely transparent to end-users



# Remote Data Delete

## 1. Remote Decommission

- Admin-initiated decommission to remotely wipe out data on lost/stolen devices
- Activated through console
- Completed when device comes online

## 2. Auto Decommission

- Optional, time-based triggers
- inSync agent self-destructs device data (already securely backed up)

## 3. Time-based Alerts

- Configurable time-based triggers if device is not reachable on network

Search user name:  GO

Name	Last Known Location	Encryption Level	Data Delete	Status	Details
<a href="#">Ashley D'souza</a>	London	High	Enabled	Normal	Manage Disable
<a href="#">James Wiseman</a>	Mumbai	Low	Enabled	On Alert	Manage Disable
<a href="#">Nathan Sobel</a>	Pune	High	Enabled	On Hold	Manage Disable
<a href="#">Susan Blake</a>	Sunnyvale	High	Enabled	Decommission started	Manage Disable

« First Previous 1 of 1 Next » Last Page Size: 25



# Geo-Tracking for Laptops

## 1. Geo-location

- Instant view of your device location as last seen online
- IP address, street, city, region/state, country

Last connected IP address	115.252.100.168
City	PUNE
Region	MAHARASHTRA
Country Name	INDIA

## 2. Google-maps mashup

- Quick view of coordinates
- Zoom in/out



## 3. Theft Deterrent

# Complete Enterprise EndPoint Protection

- 1-stop shop for simple, lightweight, effective endpoint data protection:
  - Automated Backup
  - Instant Restore
  - Data loss prevention
  - Data encryption
  - Device Trace
  - Remote/Auto Data Delete





**druva**