Transforming the Information Infrastructure: Build, Manage, Optimize.
LeanLogistics, Inc. Case Study:
Deploying Hardware Encryption for Improved Performance and Security

Andy Bass
VP Technology
How you can lose your laptop

But not lose sleep
Who am I?

• 25 Years IT Experience
• Entrepreneurial - involved in several startups & early-stage companies
• Leveraging Internet Technologies since early 1990’s
• Responsible for:
  – LeanLogistics Delivery Platform
  – Internal IT
Agenda

• Who/What is LeanLogistics?
• Describing our Business Issue
• Selecting and Implementing a Solution
• Benefits & Challenges
LeanLogistics: Leader in Global Transportation

Founded by Transportation Professionals (1999)
  • Headquartered in Holland, MI
  • Parent company: Brambles
  • Sister company: CHEP

One of the Industry’s Largest Transportation Networks
  • Billions in spend
  • Millions of loads
  • Tens of thousands of users
  • Delivered in a SaaS model
Innovative Solutions

TMS Technology
- On-Demand TMS®
- Procurement
- Planning
- Execution Management
- Appointment Scheduling
- Settlement
- Visibility
- Business Intelligence
- Supplier Inbound

Services
- Client Services
- Managed Transportation
- Benchmarking & Procurement
- GreenLanes™
- LLamasoft, Inc.

Self-Service Solutions
- LeanSource™ Procurement App
- LeanDex™ Benchmarking App
Technology Environment

Core Pillars: Security, Availability, Scalability

• Single-Instance, Multi-Tenant
• Oracle/EMC/RAMSan Data Environment
• Virtualized Linux (VMWare)
• Cisco Core Network
• Multiple Data Centers
Multi-Layered Security Profile

Physical Access
- Data Center Access
- Multi-layer Authorization

Logical Access Controls
- 2 Levels of Redundant Firewalls
- Real-Time Intrusion Detection
- Weekly Vulnerability Scanning

Data Transmission
- Session SSL
- File Encryption

Authentication
- Password Rules
- IP Restrictions
- SAML Support

Application Level Security
- Role-Based
- Data Visibility/User Actions

Annual SOC1 Audit
- Replacement for SAS70
So, What is the Business Issue?

Mobile Workforce
- Sales
- Implementation
- Development

Sensitive Data
- Internal
- External

Desire for Greater Efficiency
- Boot Time
- I/O-Centric Operations
Protecting Mobile Information

Data can be protected from inappropriate access and potential integrity disruption, but not from loss

Extend Multi-Layered Profile to Laptops

- Localized Virus Scanning
- Website/HTTP filtering
- Email Scanning
- Local Windows Firewall
- Laptop/Remote Backups
- Encrypted SSD
Pieces to the Puzzle

Solid State Disk
- Already being used in DB applications
- Thumb drives
- Phones/Tablets

Hardware Encryption
- To protect data against the loss/theft of a laptop
- Also - migration to SSD for improved throughput and productivity

Windows 7
- Optimized for SSD
- Auto-disable of:
  - Defragmentation Services
  - Superfetch
  - ReadyBoost
  - Other Boot/Prefetch Ops

Management Console
- Centralized access to manage disks
Requirements

• Seamless integration with Windows environments

• Quick setup and configuration

• Simple centralized access to data, if necessary

• Cost Effectiveness

• Performance
Evaluation

• We evaluated 7 vendors – both software and hardware based systems.

• Software-based solutions initially were generally slower to encrypt, and had varying levels of transparency and management capabilities.

• The self-encrypting hard drives provided the best performance and transparency.
High Performance

![Bar chart showing PassMark scores for HDD + Software Encryption (380), SSD + Software Encryption (591), and Self Encrypting SSD (1404).]
Implementation

Laptop Refresh
• 3 Year Cycle

Windows 7
• Transition from XP

Rollout Priority
• Executive Team
• Highly mobile groups
Challenges

Hardware Vendor Support
- Dell/Encrypted SSD drive availability
- Needing to deal with both SS and non-SS drives

Need to manage the SSD lifecycle appropriately
Results

1. Peace of Mind

2. Significant Speed Increases

Saving 2 minutes per boot = $36,000/year
Questions?