



# Symantec Endpoint Encryption Deployment Best Practices and Roadmap

**Jon Allen**

Baylor University  
Chief Information Security Officer &  
Assistant Vice President

**Rene Kolga**

Symantec  
Principle Product Manager  
Encryption

# Baylor University

Waco, Texas



- Chartered in 1845
- Largest Baptist University in the world
- 15,000 Students
- 2,500 Full Time Employees
- Over 7,000 Baylor owned computers

# Agenda

1 Background

2 Deployment Lessons Learned

3 The Future

4 Q&A

# Background

INFORMATION TECHNOLOGY SERVICES



# Reasons for Encryption



- Offices have now become mobile
  - Laptops are the standard
  - Large percentage of data losses involve laptop theft/loss
- 46 states have enacted privacy legislation requiring notification if breached data is not encrypted
- Migration from using SSN did not eliminate old stores of information

# 2013 – The Year of the Mega Breach



- The total number of breaches in 2013 was **62% greater than in 2012**
- 8 of the breaches reported in 2013 exposed **over 10 Million Identities**
- Roughly **552 Million Identities** were breached in 2013
- **The loss of a laptop continues to be the leading cause of a data breach**

# Types of Encryption: Overview



## Manual

- Tools that allow users to manually encrypt and decrypt files and folders

## Automatic (Folder Level)

- Tools that allow users to define folders or virtual drives that are automatically encrypted

## Whole Disk

- Boot time software that provides real-time encryption/decryption below the OS level. Encrypts the entire volume or disk

# Why Symantec Drive Encryption



- Cross Platform (Mac, Windows, Linux)
- Centralized platform
- Proven encryption technology



# Deployment

INFORMATION TECHNOLOGY SERVICES



BAYLOR  
UNIVERSITY

# Implementation



## Installation

- Manual vs. Automatic

## Setting up central server

- Backup to an SFTP server, offsite rotation for server backup
- Runs great as a VM (1 CPU core, 2 GM ram)

## Internal Q/A procedure

- Working SED into our system workflow
- Only disk encryption, not mail for most users

# Data We're Concerned About



## Texas Privacy Legislation

- SSN, CC#, Driver's License, Bank Accounts

## FERPA Records

## PCI (Payment Card Industry)

## Texas HB 300 and HIPAA

# Risks to Success



## Workstation Configuration

- Backups
- Screensavers
- Hibernation vs. Standby

## Authentication Method

- Single Sign-on
- Unified authentication
- Separate Credentials

## Administrative Tasks

- Handling forgotten passphrases
- Updating SED versions

## Forensics\E-Discovery

## System deployment

# The Apple Challenge



- Apple will change the EFI in even minor patches
  - Means patching must be managed to prevent bricking
- New hardware generally requires latest OS
- Security patches only available for latest major release of an OS

# Public Relations



- Administration Buy-in
- Thorough testing to up front
- Respond quickly to concerns
- Exhaustively test new versions
  - do not feel compelled to upgrade until testing is complete

# Lessons Learned

INFORMATION TECHNOLOGY SERVICES



BAYLOR  
UNIVERSITY

# Today



- Over 1400 clients deployed
  - Of those over 90% are laptops
- Require all faculty/staff laptops be encrypted
- Include both Mac and Linux installations
- ½ FTE dedicated to Symantec Drive Encryption rollout and maintenance



# In Retrospect



- Do we think we made the right choice?
  - Whole disk
  - Symantec Drive Encryption
- What would we have done differently
  - More resources
    - QA resources
    - Deployment resources
  - More realistic timelines
  - Make sure users understand the why of encryption

# The Future



- Encryption included with software
  - OS (FileVault v2, BitLocker)
  - Databases ( Oracle and MSSQL)
- Federal Privacy Legislation
- Opal v2 for managing hardware encryption



# Symantec Encryption Portfolio Update

**Rene Kolga**

Principle Product Manager

# Agenda

1 Current Portfolio

2 Encryption Trends

3 Symantec's Encryption Strategy

4 What's Coming

5 A Sneak Peak

# Safe Harbor Statement

Any information regarding pre-release Symantec offerings, future updates or other planned modifications is subject to ongoing evaluation by Symantec and therefore subject to change. This information is provided without warranty of any kind, express or implied. Customers who purchase Symantec offerings should make their purchase decision based upon features that are currently available.

# Symantec Encryption Portfolio

## Endpoint Encryption



Renders data-at-rest inaccessible to unauthorized parties on devices such as laptops, removable media, desktops

## Email Encryption



Protects email in transit and at-rest from unauthorized parties

## File & Folder Encryption



Protects individual files in transit and at-rest from unauthorized parties, allowing secure collaboration

## Endpoint Management

Renders data-at-rest inaccessible to unauthorized parties on devices such as laptops, removable media, desktops

# Encryption Trends

## Convergence of Endpoint Security Solutions



## Native OS Encryption



## Tablets



## Self-Encrypting Drives

# Encryption Strategy

Enable customers to seamlessly protect sensitive information, *wherever* it resides, with Symantec Encryption



Single Endpoint  
Encryption  
Offering



3rd Party  
Encryption  
Management



Encryption  
Center of  
Excellence



Next  
Generation  
Encryption



# Darwin 2<sup>nd</sup> Half CY14 (Projected)

The endpoint combination you've been waiting for...



Drive Encryption

**GuardianEdge**

Removable Storage

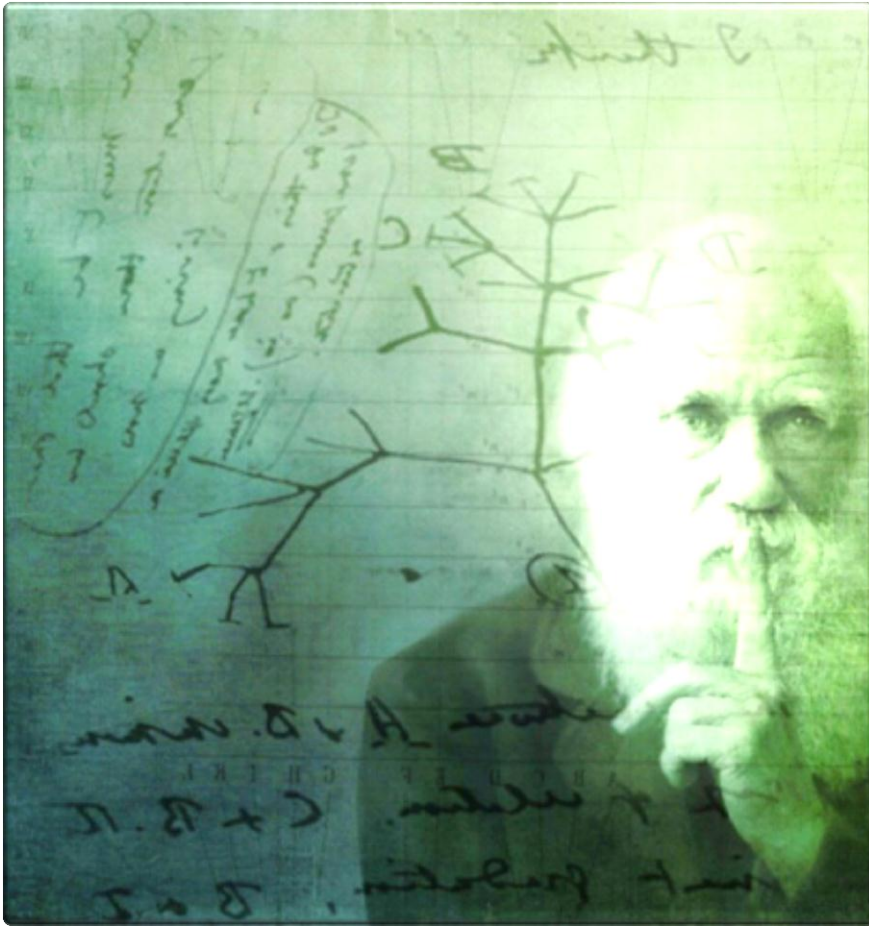
Encryption Management



---

Drive Encryption  
Removable Storage  
Encryption Management

# More Anticipated Highlights from Darwin

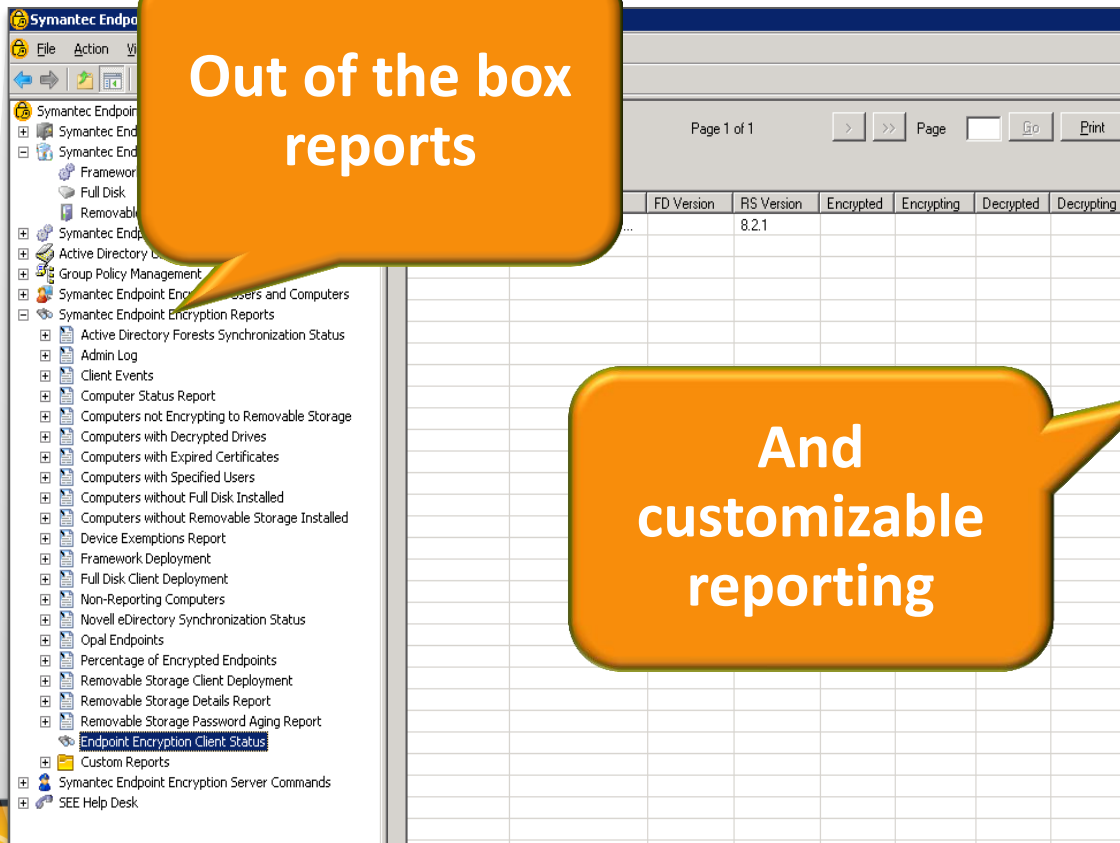


- Robust customizable reporting and extensive out-of-box reporting
- A simpler user experience by eliminating the need for enrollment
- Support for multi-user endpoints and non-AD environments
- Roughly doubling endpoint scalability
- Removable media encryption support
- Streamlined server architecture to allow faster innovation and engineering

# A Glance at Reporting

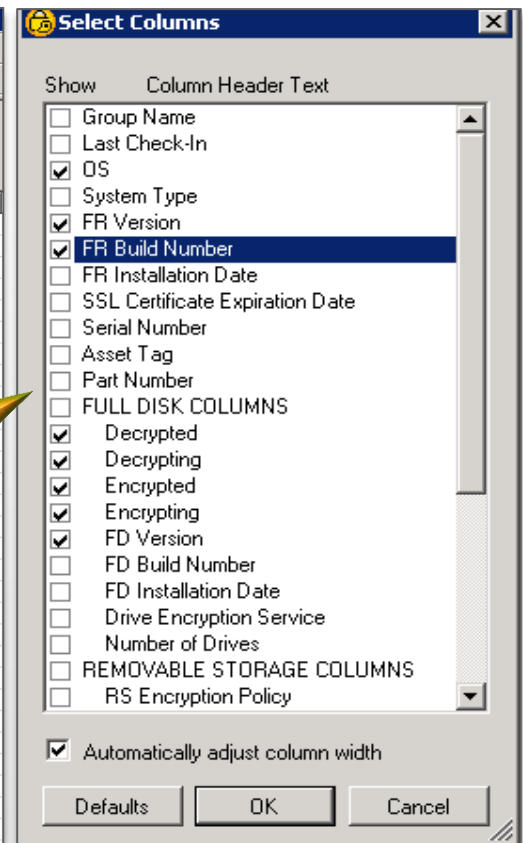
Out of the box reports

And customizable reporting



The screenshot shows the Symantec Endpoint Encryption Client Status report. The left pane displays a tree view of reports, with 'Endpoint Encryption Client Status' selected. The main pane shows a table with the following columns: FD Version, RS Version, Encrypted, Encrypting, Decrypted, and Decrypting. The first row of data shows '8.2.1' under the 'RS Version' column. The table is on 'Page 1 of 1'.

FD Version	RS Version	Encrypted	Encrypting	Decrypted	Decrypting
	8.2.1				



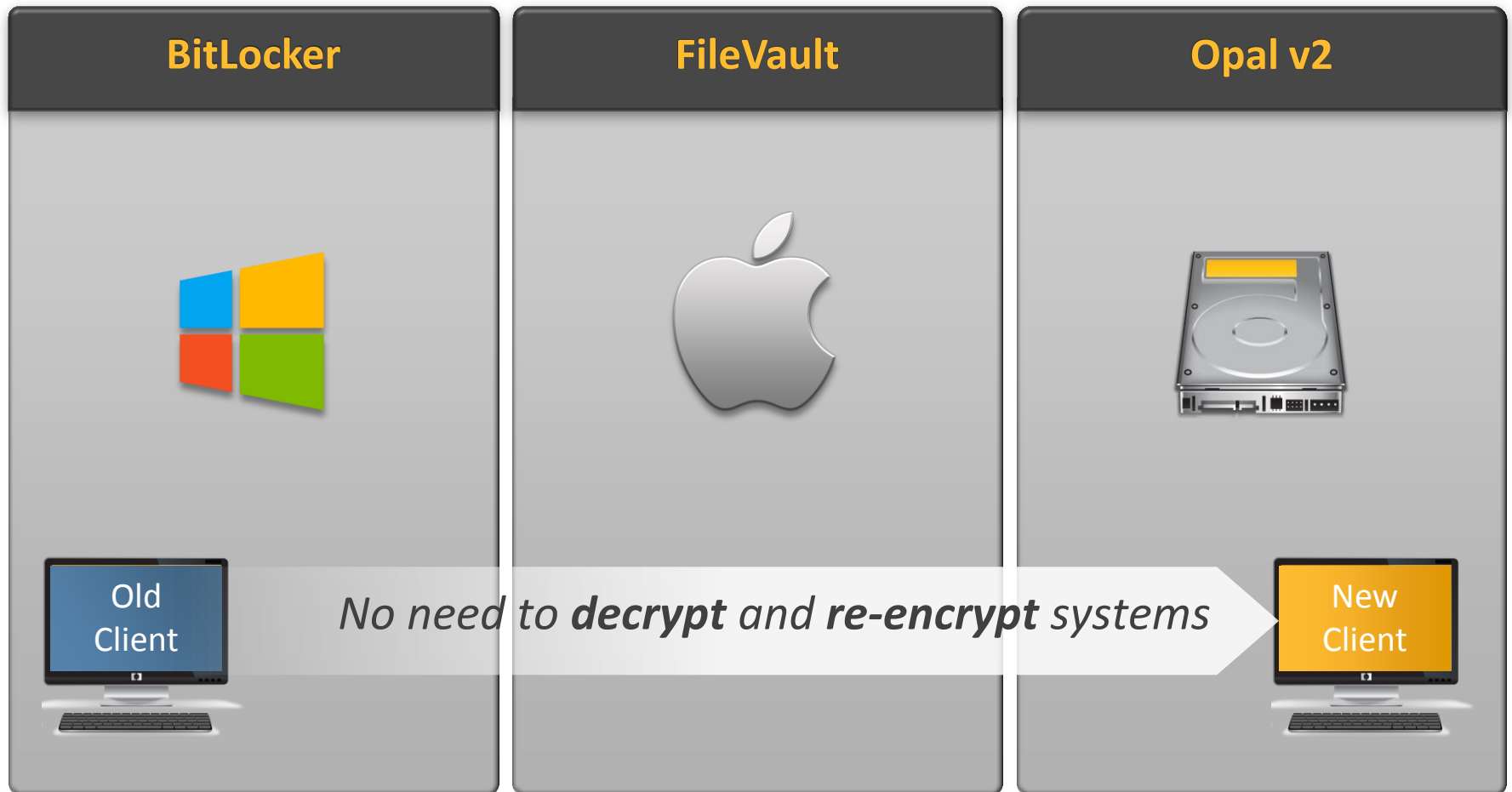
The 'Select Columns' dialog box is shown, allowing users to customize the report columns. The 'Show' column is checked for the following items:

- Group Name
- Last Check-In
- OS
- System Type
- FR Version
- FR Build Number
- FR Installation Date
- SSL Certificate Expiration Date
- Serial Number
- Asset Tag
- Part Number
- FULL DISK COLUMNS
- Decrypted
- Decrypting
- Encrypted
- Encrypting
- FD Version
- FD Build Number
- FD Installation Date
- Drive Encryption Service
- Number of Drives
- REMOVABLE STORAGE COLUMNS
- RS Encryption Policy

The 'Automatically adjust column width' checkbox is also checked. Buttons for 'Defaults', 'OK', and 'Cancel' are at the bottom.

# Hercules 1<sup>st</sup> Half of CY15 (Projected)

More robust management capabilities and easy migrations...



# More Anticipated Highlights from Hercules



- Managing Self-encrypting Drives (Opal v2)
- Managing Windows BitLocker and Mac OSX FileVault
- Policy-based pre-boot bypass
- Tablet support w/out keyboard
- Additional PIV/CAC card support

# A Sneak Peak

- Demo



# Thank you!

--Symantec Encryption Team--

**Copyright © 2014 Symantec Corporation. All rights reserved.** Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.