BEACHHEAD
Solutions Brief

PC Encryption; Eyes Wide Open
Considerations for a well-informed PC encryption deployment

Cam Roberson
Scott Pierson

In The Beginning...

A Historical Perspective

Before we dive into the current state of encryption and reveal the issues that require consideration it would be helpful to first understand the historical perspective. In other words, let's answer the question, "How did encryption evolve to its current state?"

Businesses embraced the personal computer in the mid 80's, finally convinced of the productivity it brought to its employees and the competitive rewards that would ultimately be realized. Employees were empowered to work better, faster and more efficiently with computing power on their desk to analyze, process and develop data. The personal computer forever changed how employees worked and *all was good.*

In the early 90's, advancements in computing technology and lower prices brought widespread adoption of portable, "laptop" computers. Nearly equal in computing horsepower to their desktop brethren, employees were even more productive, bringing this computing power to the field; laptops were now in front of prospects, customers and business partners. Proposals, presentations, analysis, modeling, hypothetical metrics – all of it done right there, right then. *All was even better*.

This data, now outside the physical confines of locked doors and internal networks, was at risk. The exposure of trade secrets and intellectual property most certainly posed a risk to competitive advantage. But there was an even bigger problem. The possible exposure of consumer personal and financial data got the attention of federal regulators, state government, consumer advocacy groups and the press. The theft of a Veterans Administration PC containing the personal information of over 28 million US Veterans in May of 2006 was viewed by many as the final straw – a sobering realization that enterprises, both private and public, must protect PC data.

It wasn't as if PC data encryption wasn't already available. It was. In 1991 Philip Zimmermann developed PGP (Pretty Good Privacy (PGP), free open source file encryption. In 1993, Microsoft incorporated Encrypting File System (EFS) into several versions of its NT operating system. Used correctly and diligently, these tools offered a perfectly reasonable way to shield sensitive data on a lost or stolen PC. Problem solved, right? Not quite. These tools relied on the individual user's diligence to be effective. The business entity, whose reputation and profitability was at stake, had no control, instead living with the hope that users, its employees, were following policy. We should know by now that users don't always follow policy, particularly when confronted with productivity trade-offs. Because of this, these methods of encryption were predictably ineffective and not embraced by mainstream business.

The Rise of Software-Based Full Disk Encryption (FDE)

Early attempts to manage PC data encryption accross the enterprise

State data breach disclosure requirements[1], avoidance of press coverage embarrassment, and most importantly the financial impact of customer defection applied tremendous pressure on businesses to protect their PC data.

It became apparent in the late 90's that encryption of sensitive PC data was necessary but business leaders also recognized that control had to be removed from employees. As a result, an effective encryption technique gained momentum and was widely adopted by responsible businesses; software-based full disk encryption (FDE). Though not graceful, FDE ensured compliance somewhat by brute-force. Generally installed by an IT professional, the software enforces encryption of a disk drive's entire contents, including the operating system, applications and

other non-sensitive data. As a result the computer is effectively not operational until the OS is first decrypted. This lock-down approach introduces some of the important issues and considerations that follow in this whitepaper. Nonetheless, because FDE represented an acceptable way to enforce PC data encryption, it took hold as the de-facto standard.

FDE, with very slight differentiation, is offered by many vendors. Years ago, this brand of security came with recognized, and in many cases, acceptable trade-offs around system performance, compatibility and employee productivity.

Today, a decision to deploy FDE has an even longer list of trade-offs to consider. It is no longer the simple, easy decision. New hardware and software developments and emerging trends in computing architecture may offer better, more effective delivery of encryption. Further, there is a growing list of recognized incompatibilities between new technologies and the disk drive lock-down approach of FDE. Will the security benefits of FDE outweigh being left out of the possible adoption of these new tools? As FDE is increasingly commoditized, one can certainly expect even further price reductions, but will the cost savings be enough to raise overall value against what is clearly diminishing utility?

Consider the following when deciding whether FDE is right for your business.

1.   FDE Installation
Time, effort and the "unanticipated"

There are many factors within your environment that will determine the time and effort required to install FDE on your inventory of PCs. Best-case-scenarios are almost always used to estimate time required for installation and this is particularly suspect because it is really hard to objectively benchmark. The number-one determinant of the time required for this process is the size of the disk drive(s).

FDE vendors assert the time required to install and execute the first round of encryption to be between 2-3 hours – a fair claim when considering a 40GB drive. Today's production business-class PCs are often outfitted with 320 – 500 GB disks which require 8 or 10x the time claimed for a 40GB drive. Many computers now come with 1 Terabyte or larger drives, the encryption times of which will be measured not with a clock, but with a calendar...literally!

Most FDE solutions today allow remote installation representing a big improvement over previous versions but the processor & read/write-intensive encryption pass brings most computers to a frustrating grind. Imagine attempting to work during a full virus scan – or worse. Organizationally, be prepared for installation times in excess of what you might expect. Set expectations and consider re-directing the efforts of the affected employees.

Here are a couple other things to be aware of with an FDE installation. If remotely installed users may attempt to abort the installation to return to a more productive state, sometime even attempting a hard shutdown by depressing the power button. Some products handle this better than others, but avoid any issues by backing up the data and running a disk check prior to installation.

With FDE, every sector on the hard drive is encrypted including empty sectors and sectors that may never be used. Encryption writes a higher bit density on the drive surface because blank space is overwritten with random data in encrypted form. This can cause weak sectors to fail, often corrupting the file system. Most vendors offer a disclaimer and suggest a full data backup before installation while others, particularly with installation on older computers, recommend first running chkdsk.exe (check disk). Following these practices is certainly prudent, but you should expect longer-than-anticipated deployments.

2. PC Boot Times under FDE

FDE encrypts not only the sensitive data you desire to protect, but the OS, applications and other innocuous data. Resultantly, the OS must first be decrypted before the computer is operational. Further, during the boot process, parts of the OS may be written to the virtual memory space located on the hard drive. As this occurs, that data is again encrypted, further delaying bootup. This anomaly not only affects boot times but slows ongoing PC operations.

The boot time required to be able to load MS Outlook and have it connect to the server with a non-encrypted PC takes several minutes. In a test case on a reasonably configured, major-manufacturer laptop (1.8Ghz w/ 1Gb memory and a 46Gb HD) the boot was just under 5 minutes. Is a 10 or 15 minute boot time acceptable? Ultimately you'll need to determine if the security afforded by full disk encryption is worth whatever productivity impedance you'll realize. But you can and should expect significant boot slowdowns. Again, testing within your environment is highly recommended.

3. Application Performance with FDE
Data-Intensive applications introduce recognized performance slowdowns

Many applications make liberal use of hard disk-based virtual memory. Any application large enough to use the page file to store parts of the application or data will likely experience a hit to computing performance. More memory often helps, but depending on how many applications are open simultaneously, even small applications will be affected.

Recently, users within "Company A" using an enterprise-class CRM application and full disk encrypted laptops claimed painfully slow operations. So much so that the company's users began to rebel. The CRM vendor representative told the IT Staff at Company A that they should expect a 30% performance hit with encryption. This is not the kind of disclosure you typically see within FDE documentation.

The perception of this problem is not as severe if encryption is deployed before the application is loaded and used, but once users become comfortable with a certain level of performance, anything slower is frustrating. Application performance degradation varies so it is suggested that you first test full disk encryption in your environment to determine the actual impact.

4. Hard Drive Failure Recovery

The incidence of hard drive failures will increase (some estimates as high as 10x depending on equipment age) with FDE. When an unencrypted drive fails, the data can often be recovered by the corporate IT administrator mounting it as a slave – even if the OS won't boot. This is not possible with an FDE installation. Some vendors do, however, provide a "back door" method to recover data that disk recovery services can use to restore the data. These back door services may present a security risk and, on top of that, they're not cheap.

The first time this happens to an executive or someone with critical information, the IT Department will surely feel the heat. Again, a good backup program/process is highly recommended if you decide on FDE. And, ask your chosen FDE vendor how they suggest you handle the inevitable hard drive failures.

5.   Architectural Incompatibilities with Device Management Tools

The utility and value of remote-management of PCs through the "Cloud" is quickly emerging as an important IT tool. In fact, BusinessWeek in July 2009 said "Cloud Computing is one of the most significant advances in the computing universe in decades." IT tools such as patch-, asset-, and power-management on remote devices are increasingly important, particularly to larger organizations spread over wide geographies. Because FDE applications surround the operating system with what is essentially its own operating system, Windows OS functionality cannot be accessed and unattended communications with that PC to perform these important tasks becomes impossible. Only with full coordination, support and participation of the PC user are these tools effective.

For example, managing a remote patch management requires that the user leave the device turned on and connected to the network. This very process invites tremendous security risk. In an FDE scenario, once authenticated, the data is available in an unencrypted state available for anyone to see.

What's on the PC Development Horizon?

Clearly, the choice of encryption for deployment is not one to be made lightly and there's more to consider than what you'll read in the sales literature or product documentation. The good news is that competitive pressures coupled with new and better encryption techniques are driving the cost of FDE down while new options emerge.

New and better encryption techniques you ask? Yes! The key becomes how to manage them across the enterprise.

Many versions of Microsoft Vista and Windows 7 include BitLocker, an alternative disk encryption technique to FDE. Rather than encrypting the entire disk drive, BitLocker encrypts everything except components of the OS necessary to ensure a secure and speedy boot up. Because encryption is handled by the OS, there aren't application performance issues. This approach represents a clear improvement to full disk encryption and its architecture facilitates many of the capabilities not possible with an FDE implementation.

Many of the latest generation personal computers now coming off the production line include Intel's vPro chip that will include hardware-based encryption processing. This alternative allows swift encryption/decryption, addressing previous performance problems. Future developments suggest that enhancements to the chip's functionality will be added by integrators/computer manufacturers. The vPro chip also provides a very interesting capability: the ability to actually power the computer up unattended and remotely – while the data remains encrypted. Imagine the control and IT management possibilities afforded by this capability.

These OS and hardware encryption methods are available to a great many of us today. Adoption and full utilization of these methods are in the very early stages. Development for the vPro chip is in the infancy stage. These methods represent a tremendous future for PC security, data control and IT management of distributed computing assets. FDE is not compatible with these software and hardware technologies and as a result, deployment of FDE today must be made in recognition that the capabilities afforded by these technologies will be delayed or forgone.

Forward-Looking PC Disk Encryption Considerations

The first few pages of this whitepaper have covered the issues associated with an FDE deployment and the realities that aren't covered in FDE sales sheets – though who could blame these vendors for the omission. Advis-

ing prospects that FDE is incompatible with emerging technologies that will improve, perhaps even transform, personal computing, is marketing suicide.

So what should be your considerations when selecting tools to encrypt and protect your organization's PC data?

1. **Business Control.** It is the business entity whose reputation is at risk and who'll bear the financial pain of a data breach. It is critical that the organization have control of PC data security policy. Specifically:

   - Encryption must be "Enforced." This cannot be an option set by users.

   - The effectiveness of the security cannot depend on the diligence of users to adhere to policy, because they won't.

   - Select tools that ensure data is safe, irrespective of user behavior. Users may do things unwittingly to undermine security. Still others may not always be loyal and/or authorized to have access to business data. Organizations must protect against these scenarios.

2. **Work within new, remotely managed IT infrastructures.** Be sure that your solution is integrated with the PC and does not interfere with basic operational processes.

3. **Be able to manage a variety of encryption modules (encryption agnostic).** Your organization will likely have a blend of old and new PCs. The newer PCs will have multiple encryption options available and you will need to secure the older ones too. Your solution should activate and manage the best encryption available without creating multiple management consoles and standards. Look for a solution which can adapt to new standards as new PCs get added to your portfolio.

4. **Understand and minimize the effects on IT and your users.** While this may seem obvious it is often underestimated. For IT, don't assume that the time, effort and support ends with installation because it doesn't. For users, understand the impact on productivity. Tools that adversely affect productivity may prompt side-stepping, rejection or even rebellion.

5. **Select security that can protect where encryption can't.** When the password is known or knowable (e.g., stolen along with the computer), encryption offers no protection. Select a security tool that has a back-up plan because inevitably, you will need it.

6. **There are more than just PCs holding company data.** Mobility is no longer the exclusive domain of the laptop. Proliferation of data on smartphones, tablets and USB storage as well as Windows and Mac PCs must be part of a comprehensive mobility security plan.

Publication SP800-111, "Guide to Storage Encryption Technologies for End User Devices" from the US Department of Commerce strongly recommends encryption and provides detailed description of encryption technologies: http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

[1]California's Breach Disclosure Law (SB 1386) was enacted in 2003 and required firms to provide written notification to any consumer whose personally identifiable information was potentially exposed. Similar legislation has since been adopted by 41 additional states.