BEACHHEAD

Whitepaper

3 Endpoint Encryption Myths Revealed

Lessons from those who learned the hard way

February 2018

Introduction

Firsthand experience from other IT organizations

Once upon a time, IT managers could view data encryption as an option, something they could spend their limited resources on—or not. In recent times, however, encryption has become a necessity, either as a means to protect data or, increasingly, as a way to meet regulatory or industry compliance standards, such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), as well as various state-specific statutory mandates. IT groups in any sectors these days must contend with compliance auditors looking over their shoulder. Encryption cannot be ignored.

If you are one of those who is addressing data encryption within your organization for the first time, or someone who has already implemented encryption, but having second thoughts about your selection, there are some things you should consider before making a choice or a change in solutions. This whitepaper will illustrate some of the real-world experiences of Beachhead customers with firsthand knowledge of both standard disk encryption software and Beachhead's centrally-managed PC and endpoint encryption and security offerings. These customers provide a compelling illustration of the "3 PC Endpoint Encryption Myths Revealed"…and how they can lead to regret.

One of the customers you will meet is the Bank of Georgia. They chose Beachhead Solutions several years ago, but were wooed away by another encryption provider who promised encryption compliance and endpoint data security at a lower cost. After 18 tumultuous months, the Bank of Georgia came back to Beachhead.

Myth #1: License Price Equals Total Cost of Ownership (TCO)

IT must consider all tangible and those less-visible costs

When choosing between two or more suppliers of data encryption solutions, the most obvious comparison factor is the price of the software license. "Naturally, cost has to be considered with any IT purchase and we frankly made a decision that, based on the license cost, we'd be getting a less expensive solution than we had with Beachhead," admits Eric Martz of The Bank of Georgia. What Eric and the Bank failed to recognize was that the price of the license was only part of the overall cost (i.e., total cost of ownership), as many organizations have discovered from firsthand experience.

In addition to the license cost many vendors also require server-side software to run in your environment to manage the PC encryption. Clearly this cost must be considered when choosing a solution. Today, many vendors with seemingly near-equal offerings will reduce, or in some cases, waive this cost altogether in an effort to win business. This is certainly good news, however the software must run on hardware. Frequently the hardware must be dedicated to this lone task and/or it may run on an OS that you're not comfortable with - like Linux for example.

Other costs are not quite so easily measured but absolutely necessary to consider. First the IT resources required to install, configure and support both the server-side hardware/software *and* the encryption on your endpoints. For many of these solutions this task is formidable, time-consuming and costly. Second, there are end-user/employee productivity concerns. Most disk encryption solutions require all sectors of the drive to be encrypted, even sectors containing no data. Predictably, the larger the drive, the longer the time requirement to encrypt. As disk drives continue to grow in capacity, so too will the time necessary to encrypt. A 500 GB hard drive (pretty common these days) can easily take the computer out of commission (and employee use) not for hours, but in some cases, days. In addition to the time necessary to encrypt a drive, other factors affecting employee productivity can be excessive boot

times, performance degradation on data-intensive applications and data recovery from encrypted hard-drive failure. These hidden costs are highlighted in a previous Beachhead whitepaper entitled, "PC Encryption: Eyes Wide Open" which can be downloaded here.

In summary, while license costs will vary from one solution to another, there are many other factors that must be considered. Some of these costs are apparent and others are all too often, unanticipated. When evaluating solutions you must consider ***all*** hardware and software costs, the IT resources necessary to manage the solution, lost productivity, upgrades and maintenance. A purchase decision should never be made soley on license cost alone.

Myth #2: All Data Encryption Solutions Are Created Equal

Encryption alone does not protect data against all threats

There is a widely held belief among IT professionals that data encryption solutions have become a commodity, they're all the same, they all provide an equivalent level of protection. Yes, most encryption products utilize a good quality 256K Advanced Encryption Standard (AES), which offers great data protection when the protected computer is turned off and the password is unknown—but is encryption alone enough? What differentiates offerings, and what organizations should take into consideration in their selection process, are the security features and capabilities in addition to encryption.

Encryption by itself is useless when the password is compromised, regardless of the data encryption solution, as illustrated in the following three scenarios:

- An employee quits or is terminated on a Friday afternoon, but has the computer in his or her possession with full access to company data.
- An encrypted USB Flash device with sensitive client data is found in a parking lot with the password written on it with a sharpie.
- A computer is stolen in an airport terminal powered on after its user "temporarily" went to the counter to check on the status of a delayed flight.

And there are any number of similar scenarios where the password is either known or can be learned. Protection under these circumstances is critical if true data security is desired. Due to these fairly common vulnerabilities which are not addressed by encryption, ***an encryption solution does not necessarily equate to a security solution***.

"Let's face it, users don't always follow security best practices and they are going to introduce vulnerabilities not covered by encryption that will surely compromise data security," admits Amy Eisenhower of the National Bank of Ohio, another Beachhead customer. "But let me tell you the peace of mind I get when I know that with Beachhead Solutions, I can remotely wipe at-risk data. I sleep very well at night."

"Let's face it, users don't always follow security best practices..."

Amy Eisenhour,
National Bank of Ohio

While protection beyond encryption alone is certainly compelling, Beachhead offers enhanced security management capabilities through the cloud that provided silent, two-way communication, giving the Administrator visibility, behavioral metrics, and evidence of data control. In addition, it allowed the Administrator to change use policy on the PC based on the data provided or the report of a user advising the Administrator that a PC or USB

flash has been lost or stolen. "If a computer is lost, I can quarantine the data," says Martz. "If it's stolen, I can eliminate it. If a USB Flash device goes missing I can revoke authentication. These tools give us the ability to control access to our data, wherever it might be."

"If a computer is lost, I can quarantine the data...If it's stolen, I can eliminate it."

In addition, Beachhead tool can also react independently to security risks in a pre-determined manner. Consecutive invalid logon attempts and time-based rules can be responded to automatically (without administrator action or Internet connection) in a manner commensurate with the risk. All these tools available with Beachhead offer a backstop or second-order of protection not available in ordinary, software-based, encryption products.

Beachhead can also protect highly vulnerable data stored on devices such as USB Flash drives, optical drives, and external hard drives. A Cloud-based authentication can be enforced before access is granted, even if a user has the correct username and password.

Finally, Beachhead tools for enforcing encryption and securing organizational data are centrally managed leveraging the cloud for real-time visibility and control.

To sum up, data encryption by itself is largely a non-differentiable commodity. It is the other security tools that an offering includes that differentiate the overall solution. One cannot equate encryption with security given the myriad employee-introduced vulnerabilities where encryption is incapable of protecting data. Organizations must be aware of these critical differences when they are implementing a data encryption product for the first time or changing vendors.

Myth #3: "One Size Fits All" Organizations

Organizations large and small, from Small Office/Home Office (SOHO) to Global, must contend with data security, and specifically with encryption. To remain effective and to combat unanticipated data threats, however, a comprehensive endpoint data security solution cannot be installed and forgotten—it must be managed.

Most already recognize that security management cannot rely on users to manage security—it simply won't get done, they will find a workaround. If there is a tradeoff between individual productivity and managing security, productivity will win out every time. Security must be transparently enforced at the user level. Instead, responsibility for security management must be placed on those stakeholders who stand to lose from a data breach because they are accountable for compliance and the consequences of not meeting regulations. It is, after all, the organization itself that has the most to lose in the event of a data breach. This same ownership of responsibility is rarely shared by the individual employees who are instead driven by productivity concerns.

Endpoint security must be managed for two additional reasons. First, it mustn't compound or create other PC support and maintenance problems. If, for example, the encryption or security tool can't be "turned off" or adjusted in some fashion, it very well may interfere with the ability to recover data from a hardware problem (e.g., a failed hard drive). This is the case with ordinary software encryption but not with Beachhead encryption. Second, the tools must also be managed—more specifically, remotely managed—to adapt and respond to changing conditions and data threats on a compromised computer or external storage device (e.g. USB Flash). By definition, a threatened PC or storage device is physically inaccessible to the organization. However, remote communications and remote policy change offers a mechanism to ensure that the data on that compromised hardware is as secure as possible.

While these requirements apply to organizations of all sizes, the motivations, needs, and capacity to manage security can differ widely between small and Enterprise organizations. Many small businesses, for example, manage their datacenter and network infrastructure with one, two, or perhaps three IT staff. Large enterprises, in comparison, often have large groups of IT staff dedicated to the requirements of different organizational units broken down by function, geography, or both. It is unlikely that the security and management requirements of a small business would match those of a large enterprise. The challenge of installing an encryption solution can be taxing enough for a busy IT team, but managing the new software on a daily basis can easily stretch available resources beyond their breaking point, as the Bank of Georgia discovered when they migrated from Beachhead to what they thought was a cheaper, but equivalent solution. Martz was overwhelmed with the complexity of the solution he purchased, "The only thing I can liken it to was a 5000 piece Lego set with no instructions. If we had the head count of a much larger organization we may have learned that it was a good product, but we just don't have those kinds of resources. It was just too complex."

> *"It was like a 5000 piece Lego set"...*
>
> *"We just don't have those kinds of resources. It was just too complex."*
>
> Eric Martz, Bank of Georgia

The lesson learned here is to ensure that the management tools are not only intuitive and simple to use, but appropriate for the size of the organization. Remote recovery from hardware or software issues is also important, eliminating the time-consuming process of bringing in computers and issuing replacements.

In contrast, larger organizations may want or require a broader assortment of management tools and more granular control of their encryption solution. Their laundry list of wants may include extension of the domain and network tools, the ability to leverage Microsoft Active Directory to deploy security policies by groups, or have different policies in place based on business disciplines such as geographical location, computer, or storage type.

A global retailer and Beachhead customer with over 10,000 licenses explains, "We've got to have the flexibility to apply appropriate and diverse security policies to computers by department. We exercise very different rules depending on the mobility of the computer, the sensitivity of the data by department, tenure, and rank of our employees." The key point is that one size does not fit all. Beachhead offers three different management console tools with features and interface requirements appropriate for different organizations.

> *"We've got to have the flexibility to apply appropriate and diverse security policies to [our 10,000] computers by department"*
>
> BeachheadENTERPRISE customer

While we are discussing sophisticated security solutions, it is worth mentioning the distinction between data security and general security. Some vendors use a broad definition of security that includes anti-virus, anti-spyware, anti-malware, firewalls, anti-phishing, and even parental control. But data security (which includes encryption) and general security are not the same. The threat, the liability, and the party most affected (i.e., user versus organization) are usually different. Most importantly, the response and protections are always different.

These products (i.e., platforms) may allow the purchase of specific general security modules—mixed with data security modules—containing a wide variety of tools that have little to do with one another. Even if an organization chooses not to purchase or use all of these modules, the overhead/infrastructure needed to support these disparate tools can overly complicate the task of managing the secrecy and integrity of organizational data at the endpoint.

Beachhead addresses this issue with two management console interfaces: one designed to meet the needs of an

SMB, the other an enterprise. For very small organizations with little or no internal IT support, the solution can be provided as a monthly service from a Beachhead-authorized MSP. What could be easier? A monthly service where the management is performed by a team of service experts.

The Beachhead solution, delivered as a cloud-managed offering, covers all computing and storage endpoint devices under one console including Windows and Macintosh computers, USB Flash and external hard drives, iPhones and iPads, and Windows computers with self-encrypting hard drives (SEDs). Looking toward the future, Beachhead's roadmap will support a unified, optimized, cloud-managed endpoint security tool that will include other emerging computing and storage platforms.

In summary, while the need for encryption and security applies to organizations of all sizes—from the very small to the largest Enterprises—the requirements and capacity to manage security can differ widely. Therefore, the security solution must match the size of the organization.

Choose Wisely

Making the wrong choice can lead to regret

Data encryption is a must-have in today's insecure world. Organizations must choose wisely, however, when selecting an encryption solution. Just ask the Bank of Georgia. Assuming that the price of the software license equals the total cost of ownership can lead to many thousands of dollars of unexpected costs in related hardware and software, IT staff time, and lost productivity. Assuming that all data encryption and security solutions are created equal can put corporate data and security compliance at risk regardless of the encryption product used. And assuming that one size of encryption/security solution fits all can result in a solution this is either inadequate for the complex requirements of a large organization, or too complex for a small organization, preventing either of them from achieving the level of security they need.

Beachhead Solutions Inc.
1955 The Alameda
San Jose, CA 95126

408.496.6936

Question, comments? Write Cam Roberson

croberson@beachheadsolutions.com