BEACHHEAD

Whitepaper

Data Data Everywhere

IT considerations for ***Endpoint Data Access Control:***
Is encryption alone, sufficient?

Cam Roberson

February 2018

Introduction

Firsthand experience from other IT organizations

Organizations large and small spanning every sector are responsible for maintaining vast quantities of information across their networks. It is essential for these organizations to control who can access data, who can proliferate sensitive data, and under what circumstances. IT professionals have traditionally relied upon controls such as Microsoft Active Directory and other LAN security tools, which control data access through permissions (such as authentication) and/or lockouts based on misuse (such as invalid login attempts).

While effective within the electronic confines of a domain or LAN, these solutions are proving ineffective in extending their protection to data located beyond the boundaries of domains and LAN security controls. The unregulated proliferation of data by employees has placed more and more information outside the safety and security of the domain, beyond the locked doors. Data is being duplicated on PCs, tablets, smartphones and backed up and transferred to tiny flash drives—all outside the controls of LAN protection. And because employees are more productive, more efficient when data is available at hand, replication and decentralization of data has intensified – even for organizations that believe data should only stored in the cloud.

As computing and communication matures, the challenge of controlling access to data only becomes more complicated. Employees access and manipulate corporate data on their chosen smartphone and tablets which they've purchased themsevles. This "Bring Your Own Device" (BYOD) world has compounded the the duplication, proliferation and access of (and to) sensitive company data. Meanwhile, in a trend which will predictably continue, laptops are become smaller and even more mobile, blurring the distinction between a phone a tablet and a personal computer. Those responsible for securing an organization's data must face the very real prospect that the same sensitive data could be stored on multiple devices under different file types and names.

Challenges to IT Security Professionals

This new and evolving reality creates three significant challenges for security professionals. The first challenge is to ensure that data outside the domain can only be viewed by authorized personnel and only for as long as is appropriate. Authorization is never forever. Access should be limited to a finite period of time because while the need to access and the relevancy of this data will diminish over time, the damage caused by misuse rarely does. A former customer's credit card information may no longer be of value to the organization, for example, but the potential risk, and financial impact, of losing that data remains.

The second challenge is to protect this external data across a broad and growing range of computing, communicating and storage devices. Technological advancements and shorter product lifecycles bring faster obsolescence resulting in higher hardware turnover. Data often remains on these retired devices and is not properly "cleansed." In addition, smaller device footprints can increase the likelihood of theft or loss with potentially sensitive data left intact and unsecured. Finally, an increasing variety of productivity tools download data to multiple employee devices, adding to the proliferation of sensitive data. Organizations may feel secure believing that only one copy of backed-up data exists in the cloud, when in reality many copies may exist on many different endpoints.

The third challenge is ensuring that the organization meets compliance with regulatory and industry requirements governing data. These include the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), disclosure laws in 46 states, as well as the Fair and Accurate Credit Transaction Act (FACTA), Gramm-Leach-Bliley Act (GLBA), and Sarbanes-Oxley (SOX)—collectively affecting just about every organization in every sector. Most of these compliance mandates specify data encryption

as a means of protection. Encryption, however, does not always provide the organization with access control. Any individual with authentication or credentials has access to encrypted data. This includes not only those who are authorized, but those who are not authorized, as well as those whose authorization has expired, such as an employee or contractor who has quit or been terminated but still has the device with authentication in their possession. Clearly, something more than encryption is needed to enforce and control access to data.

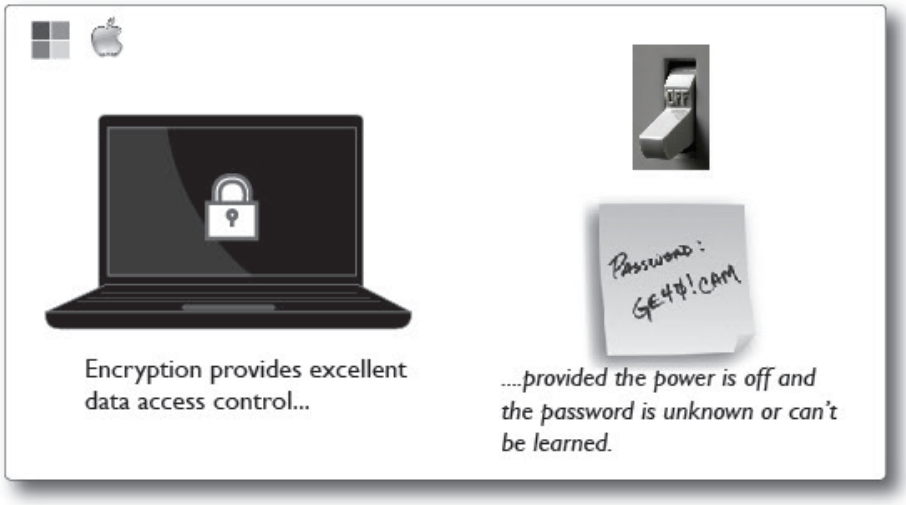
The BeachheadSecure™ Answer

Leveraging web-based communications and automated tools to control data access

To deal with these challenges, organizations need a comprehensive strategy that includes access control of data, coverage over a broad spectrum of endpoint data repositories, and encryption enforcement (i.e., compliance). Beachhead has the answer, leveraging the "cloud" and automated tools to promote communications and extend real-time access controls to endpoint devices where the data is. From one easy-to-use cloud-managed console, Beachhead delivers enforced encryption and data access control across a wide range of endpoint computing and storage devices. Following are four examples of how Beachhead meets the challenge of maintaining control of who, where, and when users have access to data under each of the conditions described in the previous section.

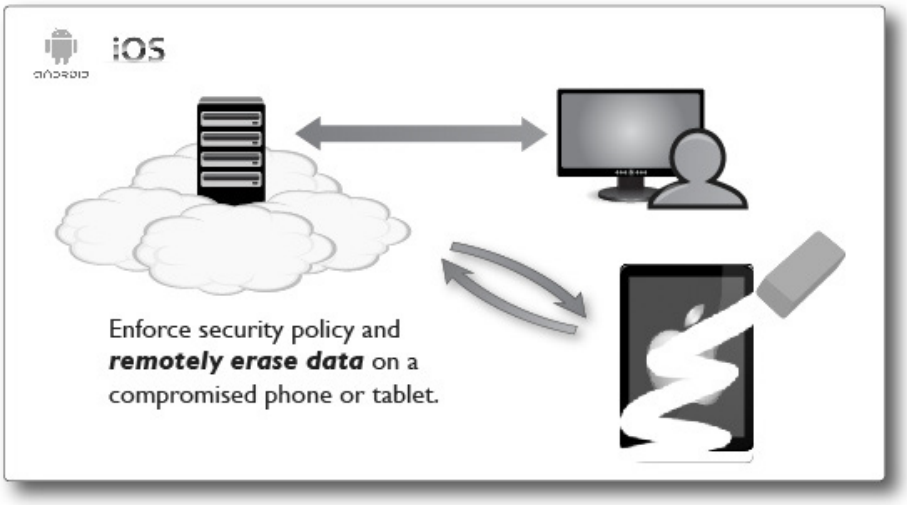
Example 1: Access control begins with encryption

Sensitive corporate data residing on a lost or stolen computing device presents a tempting target for anyone with malicious intent. An access control mechanism is needed. Encryption, while not a comprehensive solution to data security by itself, does offer access control. If the computer is off, has not been authenticated, and the password is unknown or cannot be learned, encryption will prevent access to the data. And if the person possessing the lost or stolen computer attempts to remove the disk drive and boot from a different computer or operating system, the organization will be effectively enforcing access control as the encrypted data is totally unreadable. The BeachheadSecure Protection Modules begin with encryption enforcement as is necessary to meet a growing list of legislative and industry mandates and provides organizations a safe harbor from costs and unwanted publicity associated with an unprotected loss of private or confidential data.



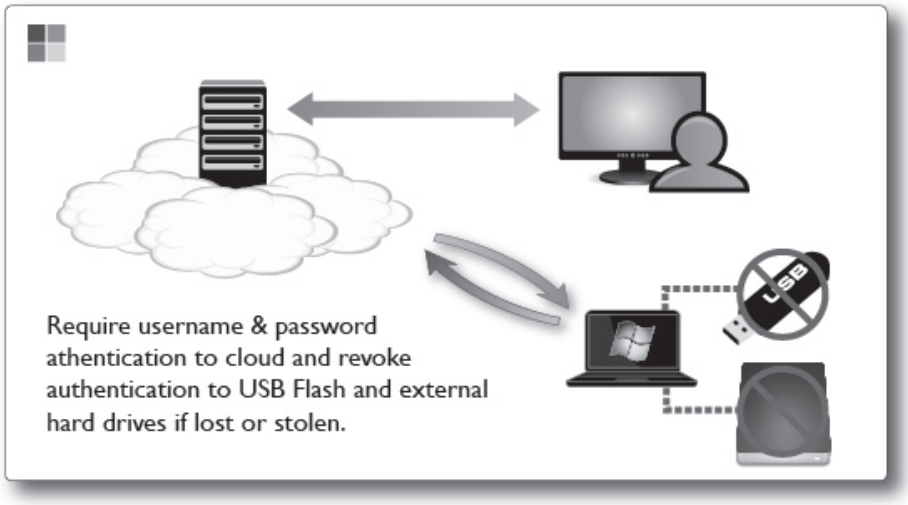
Example 2: Smartphone data quarantine or elimination

The adoption of smartphones and tablets with Apple's iOS and Google's Android operating systems – have exploded on the enterprise business market. In many cases these devices are chosen and purchased by employees of the firm.



Unfortunately for security professionals, the business use and personal use of these devices frequently blend together. Small and highly mobile, these devices can be easily misplaced and are a high-value commodity to a thief. Organizations must ensure that sensitive corporate data stored on phones and tablets – company- or employee-owned – are not compromised. BeachheadSecure™ modules for both Android and iOS provides organizationally managed access control in the form password policy, encryption, and the ability to quarantine or destroy sensitive data if an attempt is made to access it by an unauthorized party. These controls, like those designed for many external computing and endpoint storage devices, are managed through The BeachheadSecure™ management console through nearly always available wifi or cellular connectivity.

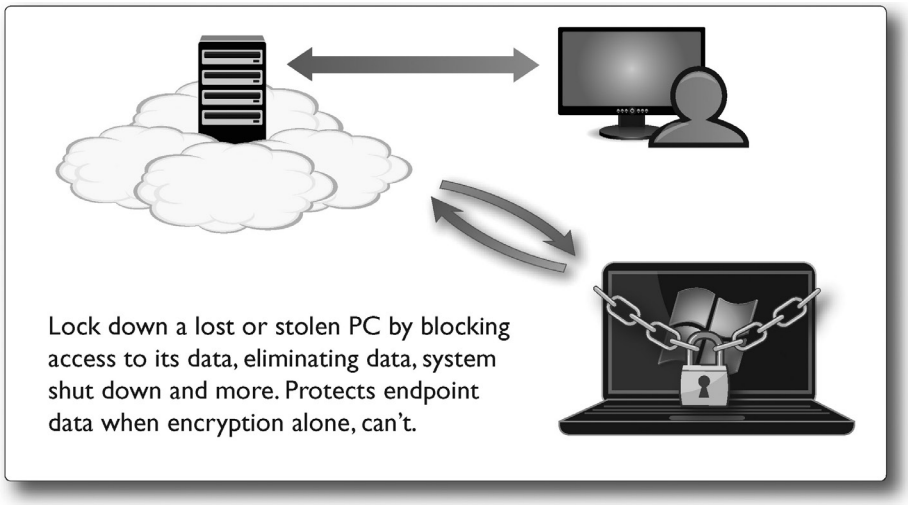
Example 3: USB authentication through the cloud



USB flash and USB attached hard drives are highly susceptible to loss or theft due to their small footprint, low cost, high density and transportability. Data stored on these devices typically has a limited shelf life. It is critical that, as time passes and these devices become lost, stolen, or simply misplaced, the data they contain will never be accessible to an unauthorized party. BeachheadSecure™ MEDIA offers encryption, rights management, and access control. The organization can enforce a policy which requires a username & password authentication that must come through the cloud for approval by policy before the data is decrypted and therefore, accessible for the holder of that device. If the device is determined to be at risk, the requester – even with the correct username & password – will be prohibited from accessing the

data. Instead, the data will remain encrypted and inaccessible until which time the BeachheadSecure™ administrator again permits access.

Example 4: Data quarantine



Encryption can provide access control and should be deployed by every organization. But as discussed, encryption is a passive solution that cannot prevent access to data once the computer is authenticated. The bullets below are just a partial listing of the circumstances when encryption alone provides no data protection:

- The computer is stolen with the power on
- The computer user becomes unauthorized (quits or is terminated) but still has the computer
- The password is stolen with the laptop (perhaps written in a notebook in the computer bag)

There must be a way to deny access to this data to preclude access to it under any of these conditions. The BeachheadSecure™ Management System allow an organization to effectively ensure that access to the data is removed – even if authentication, through whatever means, is successfully performed. And, if the lost or stolen device is ever again recovered, or if the user is reinstated and is again authorized to view the information, the BeachheadSecure™ administrator can bring the data back into readable condition, thus ending the quarantine.

BEACHHEAD
Beachhead Solutions Inc.
1955 The Alameda
San Jose, CA 95126
408.496.6936 x-6866

Question, comments? Write Cam Roberson
croberson@beachheadsolutions.com