BEACHHEAD

Whitepaper

Rights Management & Access Control Beyond the Network

SaaS data encryption and security enforced through the "cloud"

(read what ties LAX, Lady Gaga & Alphagraphics together)

Cam Roberson

March 2011

The State of Data Access Control

Healthcare organizations, financial institutions, enterprises of nearly every size in every industry sector maintain vast stores of information across their networks. It is vital for these organizations to control who gets data access privileges, who can proliferate sensitive data, under which circumstances these rights *are* available - and when they're *not*.

One of the most widely implemented tools to provide data access control is Microsoft's Active Directory, an integral part of the Microsoft Windows Server architecture. Similar to other directory services, such as Novell Directory Services, Active Directory is a centralized, standardized system that automates network management of user data, security, and distributed resources and enables interoperation with other directories. It is designed especially for networking environments.

Through Active Directory, organizations can provide effective, highly efficient data access control features such as auto lockouts based on invalid logon attempts, file folder shares that can block data from being moved to local storage, and network administrator mandates to revoke user access privileges.

But data is increasingly stored beyond the reach of the domain or physical network—and also beyond Active Directory. The computer is a roaming productivity tool. It is simply not practical, for example, for remote workers—particularly those who are traveling—to be on the domain. Not only can data be stored on highly mobile laptops. It can also be stored quickly and cheaply on optical media (CDs and DVDs), flash drives (sticks), and removable disk drives that are capable of storing gigabytes to terabytes of potentially sensitive corporate data. These devices can easily be lost or stolen. How can organizations extend Active Directory-like centralized access and rights management and control to these devices?

Leveraging "The Cloud"

The network, and the way we define it, is expanding. It has become ubiquitous, dependable, and readily available through a variety of disparate access points, including Wi-Fi, broadband, cellular, and WiMAX. While this has contributed to wide distribution of data (and to inevitable data breaches), the network controls and security of this data have not kept pace. This data is beyond the reach of access control, rights management, and security of network management tools like Active Directory.

We contend that these controls should extend to where the data is and we must utilize the cloud and automated tools to exercise that control and security. One way to provide data access control of devices that may not be physically connected to a local network is by turning to "The Cloud." Cloud-based security tools can offer reporting, use and security information and allow an administrator to manually act upon the information when a cloud connection is available, and automatically when a connection is not. Those who hold data security responsibility for an organization will use these tools to define and control who has access to data, and when, in much the same way as a Active Directory administrator does in a well-planned domain.

Following are three case studies based on real events. Each illustrates a potentially risky and costly situation in which passive security was insufficient and where dynamic access and rights management control could have ameliorated the risk.

Case # 1: Los Angeles International Airport

A business traveler sits uncomfortably in the gate area of American Airlines terminal checking emails on a laptop. A sudden commotion around the arrival/departure board produces an involuntary sigh by the Traveler. Could there be yet another flight delay? A previous nod and exchange of "Hellos" with another waiting passenger convinces the Traveler to trust the stranger. "Would you mind keeping an eye on my stuff for just a moment while I see what the hubbub is all about," asks the Traveler. "Sure, no problem," replies the fellow passenger. Returning moments later, after learning of another 45-minute delay, the Traveler finds the friendly passenger, and his laptop, gone.

This trusting behavior is not uncommon. The reader may have experienced a similar situation at the airport—or their neighborhood Starbucks. A survey conducted by Ponemon Institute for Dell Computer found that up to 12,000 laptops are lost in US airports each week (1200 a week at LAX alone). Nearly 70 percent of lost PCs were never reclaimed. Most disturbing, 65 percent of those surveyed admitted not taking steps to protect data when traveling.

Like the airport scenario, the hassle of shutting down the PC and carrying it, the sensible and secure choice, usually takes second place to productivity and convenience. What about encryption? Encryption might be considered a form of "passive access control," but in the all-too-typical scenario described above, encryption would have been ineffective. Once a computer is authenticated, as it was in this scenario, data is decrypted (or in a decryptable state) and encryption is useless.

It is worth noting that encryption is a necessary baseline data protection tool that is required for compliance with a rapidly growing array of legislative and industry-specific mandates. These include Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), disclosure laws in 44 states, as well as the Fair and Accurate Credit Transaction Act (FACTA), Gramm-Leach-Bliley Act (GLBA), and Sarbanes-Oxley (SOX).

Wouldn't it be nice to have the capability to control access to the data irrespective of whether an unauthorized user acquired data in a situation where encryption wasn't protecting that data? Tools such as these could extend network data protection and security to the farthest reaches of the new definition of a corporate network. ***Organizations need the ability to manage/change access to sensitive data on PCs***. This capability is essential since remote users can't be managed. Users may undermine security by writing down passwords or failing to exercise good sense (like the Traveler at the airport), or they may become unauthorized through termination or resignation.

Protection against these eventualities is available within the network domain. Organizations need similar controls beyond the domain. The Cloud can provide that protection. And while remote Internet communications may not always be available, protection most of the time is far better than no protection at all.

Case # 2: Lady Gaga

The now-infamous WikiLeaks organization released more than 250,000 documents last year containing confidential exchanges between the US and other countries worldwide. This information was allegedly passed on to WikiLeaks by US Army Private First Class Bradley Manning who was serving in Iraq. Private Manning simply copied (burned) the information onto a Lady Gaga CD and mailed it off. A 2008 directive by the Department of Defense prohibited the use of thumb drives and other storage devices on Pentagon and Armed Forces computers, but there was no such ban on CD drives, which are nearly always built into computers.

As with the Traveler in the last case, ***organizations need the ability to manage or change data right management and access control***. While malicious behavior is hard to prevent (short of completely disallowing access to data), care and planning must be taken with respect to allocate rights management only to those who absolutely require it. Similarly, the organization must be able to revoke access to data on compromised peripheral storage devices once they are known to be lost or stolen—even when that data resides beyond the visibility or control of a domain network. Controlling possible leaks requires planning, and organizations need tools that are able to change rights.

Circumstances can change rapidly. An individual can go from authorized to unauthorized instantly. Those changes need to be implemented outside of the domain. Therefore network control must extend beyond the confines of the traditional network.

Case # 3: AlphaGraphics

Inexpensive, practically disposable USB sticks can be found laying around in virtually every office on almost every desk—typically not plugged into a PC or on a lanyard, with no labeling or information as to the data stored on them. This was the case when Joe (not his real name) in Marketing was looking for a convenient way to deliver a file containing a brochure to AlphaGraphics, a nearby printing company. "Bob (also not his real name), have you got a spare stick I can borrow," Joe asked. "Sure," said Bob. "I suppose you can use this one. I can't remember where I got it."

Under a tight deadline, Joe quickly copied the file onto the stick and dropped it off at the print shop. Unclear instructions required the print shop to search for the files that needed to be printed. But there was more on the disk than Joe and Bob could have imagined. The printer alerted the organization that there was a file on the computer with customer names, credit card numbers, and social security numbers. Fortunately the printer notified Joe and the sensitive files were immediately deleted.

In this case, the USB stick was sent outside the company unencrypted. There was no reason for Joe or Bob to believe there was a risk. In fact, however, the USB stick did not even belong to Bob. It had been misplaced by Mary in finance. While she knew it was lost, she had no way of knowing where it was, whether it was vulnerable, or whether it was somehow compromised. Mary hoped that the missing stick was in a drawer and she simply couldn't find it. There was nothing she could do about it anyway.

Data lasts forever. Organizations need the ability to encrypt and control who gets access to the data and under what conditions. This control must be dynamic because circumstances change. Mary knew she'd lost the flash stick but there was nothing she could do about it. Its data was at the mercy of whoever discovered it. Fortunately, a Good Samaritan at AlphaGraphics found it. It could have ended much worse. But what if the organization could enforce encryption of the data and mandate that access to it required a user name/password authentication? Without sufficient credentials, an unauthorized individual would have no access to the encrypted data.

Centrally Managed Encryption, Access Control and Rights Management

Happier endings to the risky cases above

The definition of an organizational network is changing, growing both in scope and reach. One must now consider a network to include any location where its users are leveraging computing tools, resources, and data to perform their jobs. This work is being performed increasingly outside the walls of a corporate building and beyond the view of co-workers and management. The communications link fueling the new network is the Internet—the Cloud. Whether accessed though broadband, cellular or Wi-Fi, worker productivity has been enabled or enhanced in places not previously possible. Data – sensitive corporate data – is now at the borders of the new network.

All good, right? Well yes…and no. There are almost no boundaries to where workers can be productive. However, the centralized management tools of traditional networks services like Active Directory in Microsoft Server domains can't reach these boundaries. Much like the Old West, the new frontier is an almost lawless state.

Encryption has been singled out as a compliance requirement by a growing array of new laws and industry mandates. Encryption provides a kind of passive access control to the data that resides on laptops, and to a lesser extent on other storage devices. By itself, however, encryption is insufficient. Why? Because in the new frontier things change. Remote authorized users can quickly become unauthorized. PCs, optical media, and flash devices can fall into unauthorized hands. Malicious employees might seek to profit from an organization's sensitive data. Even well-intentioned but careless employees may inadvertently expose sensitive data to unauthorized eyes.

This whitepaper highlighted these all-too-common occurrences with three real-world events. In each of these, encryption by itself was either insufficient or ineffective due to a lack of central enforcement. Secondly, and especially because things can change quickly, an organization must be able to dynamically determine who can write data to what devices and under what conditions ("data rights management") and control access to who gets to read that data ("access control").

Cases revisited

Beachhead subscriptions and services provide for centrally managed encryption and can extend access and rights management control to the edges of the network utilizing the same communications channel (e.g., Wi-Fi, cellular, etc) that created this new network paradigm.

Let's revisit the three cases described above with the specific Beachhead data protection tools that would have prevented the threat.

Case #1: Laptop lost or stolen at LAX with power on while accessing email

On discovering his laptop gone the user would have immediately called his support desk where the status on that device would have likely been changed to "lost," or perhaps "stolen" On the next automated (and silent) Internet check-in to the Beachhead server, the laptop agent would have learned of its status change and executed the data protection response(s) accordingly. In this case of a lost status, the encryption keys would be immediately wiped, rendering access to the data impossible. If the status had been set to stolen, all data could be wiped to DOD standards, rendering the computer a brick.

Case #2: Rogue government employee copying sensitive data to Lady Gaga CD for nefarious reasons.

Several protections available through Beachhead*MEDIA* could have been utilized to mitigate or eliminate this event. First, the Beachhead*MEDIA* administrator may have identified what rights this user had. Can the user write data to optical media and, if so, under what circumstances? For example, can this user (or group of users) write data on CDs that can be read only within the organization? Or, perhaps, should this user be able to write only encrypted data to the media and require a cloud-based user name/password authentication? Authentication privileges are under the control of the administrator and can be revoked so that data cannot be authenticated and read. Additionally, if the degree of risk is high, the administrator can disable the disk the next time the unauthorized user attempts to authenticate.

Case #3: : "Found" USB flash device used to transport a print job to AlphaGraphics

Beachhead*MEDIA* provides similar rights management and access control for USB flash devices. The administrator would have determined that USB flash devices must be encrypted under any circumstance for all users within the organization. Furthermore, a user name/password authentication must be performed in order to decrypt that data. Neither Bob nor Joe would have had the credentials to unlock the encryption, nor would they have been given the chance. As soon as the flash device was plugged into Joe's computer, it would have made an immediate and silent connection to the Beachhead server where it would learn that Mary had called IT to report the disk lost. The contents of the flash device would have been immediately wiped to eliminate the risk of data exposure. The entire scenario would have been thwarted from the beginning.

Beachheads' SimplySecure™ Management System

Complete mobile data protection

SimplySecure™ enables organizations to enforce encryption of sensitive data on their inventory of mobile devices quickly, easily, and without significant IT burden or user impact. SimplySecure™ is deployed and managed through secure Internet communications (via the "Cloud") so compliance to a growing array of legislative mandates can be achieved in literally one day. There is no need to locally install encryption on each mobile device and there is no investment or support necessary for IT hardware/software infrastructure. Finally, users have no involvement in the operation of the tool, so they continue to operate their device – whether theirs or the company's – in exactly the same manner. This innovative approach to encryption and data security provides compliance without impacting the productivity of employees.

Some laws and industry requirements go beyond encryption of personal data. An unauthorized person in possession of the password who can authenticate a mobile device is immediately able to access the (previously encrypted) data. SimplySecure™ gives the organization the capability to wipe or control access to at-risk data on a device if an unauthorized individual gains access to that data.

Beachhead invites you to learn more about the comprehensive protection offered the SimplySecure™ Management System, delivering unprecedented control and security of personal data on your inventory of mobile computing and communication devices.

Beachhead Solutions Inc.

1955 The Alameda
San Jose, CA 95126

408.496.6936

Question, comments? Write Cam Roberson

croberson@beachheadsolutions.com