BEACHHEAD

Technical Whitepaper

BeachheadSecure™ Architecture & Security

Specifications, compliance and certification considerations for the IT Professional

February 2018

Foreward

First-in-class web-managed mobile device security platform

Ten years ago, Beachhead was the first vendor to utilize the cloud to enforce encryption and security for Windows PCs. Today, BeachheadSecure is the only web-managed security platform that can enforce encryption and security policy – including remote access control and elimination of at-risk data – on Windows and Mac PCs, iOS and Android Phones & Tablets and USB Storage devices from one unified management console.

BeachheadSecure's innovative cloud architecture is comprised of three primary components, an ***"Agent"*** (sometimes in combination with an application) that resides on the protected device to enforce encryption, security policy and initiate communications to the Beachhead-hosted ***"Server(s)."*** The Beachhead Server holds and delivers security policy to the devices and serves as a conduit between the protected device and the desires of the organization orchestrated through a web-based ***"Management Console."*** It is with this management console that the organization enjoys visibility, security change-control and comprehensive real-time protection for its inventory of mobile devices.

This whitepaper discusses the underpinnings of this architecture from a technical perspective with special emphasis on the security of these elements including Beachhead's server environment, encryption methodologies, and communication protocols.

Table of Contents

Understanding the Solution

When an organization evaluates any software solution, part of that evaluation includes determining if the solution meets local security laws and has all of appropriate certifications. The BeachheadSecure platform is different than many other security encryption solutions so it is important to understand the product architecture before applying laws and certification requirements. BeachheadSecure is a cloud-based solution which calls for end user devices running client agents to check-in with the BeachheadSecure server to determine if there are any new instructions to implement. These instructions can be new encryption locations or file types as well as new rule triggers and actions.

Each customer has an account on the BeachheadSecure server where their administrators can login and manage their organization's end user devices. These accounts contain the following information:

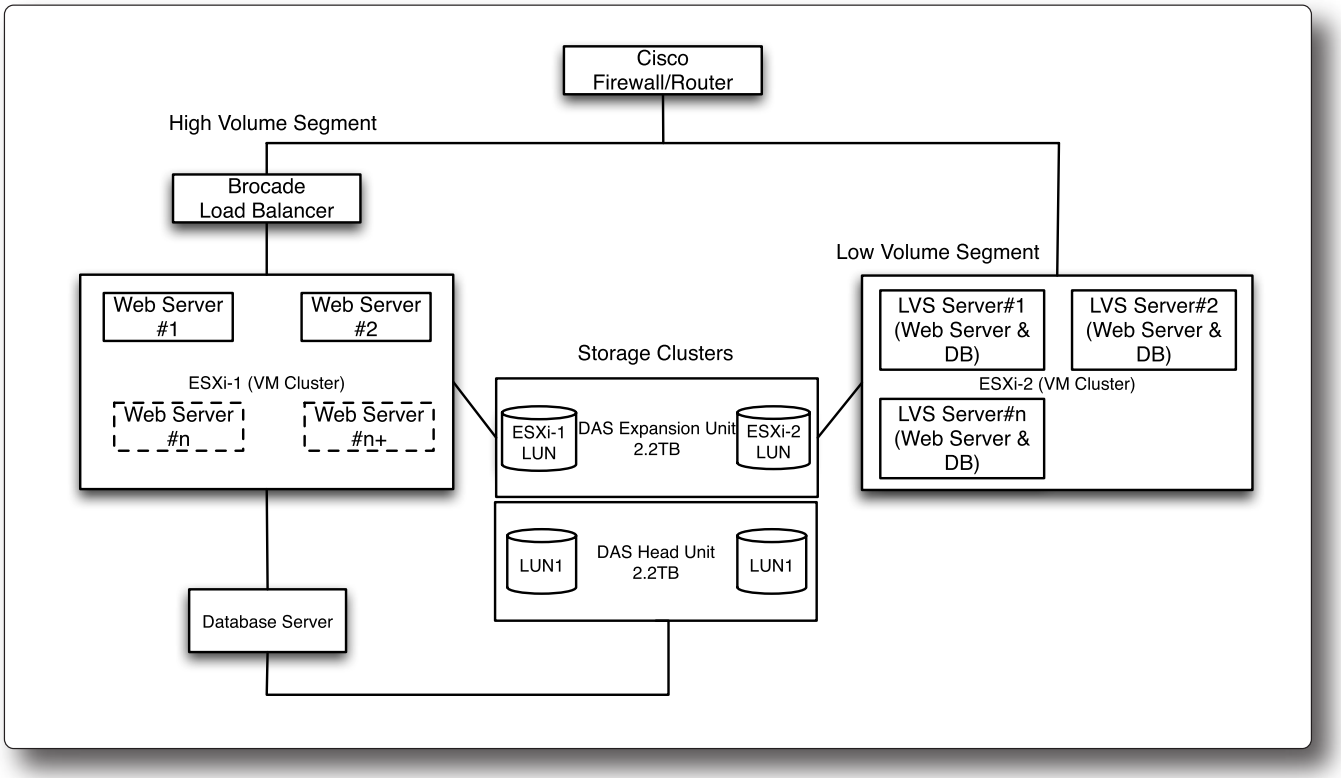
- Device names and specifications
- User names (logon)
- Encryption certificates
- File names (if using the file catalog function)
- Administrator names, email addresses, phone numbers, and mailing addresses

It is important to understand that actual data files are not stored within the cloud-based accounts. BeachheadSecure is not a backup service and does not store any data files, encrypted or not, on its servers. No company data other than what is described above can be found on the BeachheadSecure servers.

Understanding the Architecture

Beachhead Solutions has partnered with Rackspace as a trusted facility to provide hosting for its servers. Rackspace is the leading managed cloud company in the world. Rackspace has over 200,000 customers worldwide and is a Gartner Magic Quadrant Leader. The partnership between Beachhead Solutions and Rackspace spans more than a decade and we attribute that to Rackspace's ability to quickly adjust to changing business needs.

Client devices which have internet connectivity and are running the BeachheadSecure agent software will periodically check-in with BeachheadSecure servers at Rackspace. The following diagram shows the current infrastructure that Beachhead Solutions has deployed within Rackspace's primary United States location:



Location of Systems: Rackspace Data Center IAD3 (Northern Virginia)

Services Provided: Fully Managed Dedicated Servers

Catastrophic Hardware Failure Replacement Commitment: 1 hour

Network Availability Guarantee: 100%

Beachhead Solutions' US based systems consist of two primary segments which are the Low Volume Segment (LVS) and the High Volume Segment (HVS). Customers in the low volume segment are primarily those with a small number of client devices (typically 200 or less). Customers in the high volume segment are primarily those with a larger number of client devices (typically in the several hundred or more).

The LVS consists of a large primary physical server which hosts a VMWare ESXi cluster. Currently this cluster contains two deployed virtual machines (VM's). Servers in this segment are designed to house customers that have lower numbers of client devices and do not expect sizable growth in their deployments. Servers in this segment utilize Beachhead Solutions' single-server deployment approach which houses the web services application server and the database server in a single [virtual] machine.

The use of virtual machines provides Beachhead Solutions with a great degree of flexibility and recoverability. In the event of a hardware failure [of the host machine], the VM's can easily be moved to a replacement box and operations restored in relatively short order. Similarly, if additional performance is required, the VM can be allocated with more computing cores, memory and/or disk using a simple reconfiguration which can be done very quickly. Both VM cluster hosts have been sized to accommodate the migration or movement of VM's from any failed cluster to the remaining operational one in the event of a failure. This provides Beachhead Solutions with a cost efficient way of creating redundancy as well as high recoverability.

The HVS consists of an identical large primary physical server just like the LVS. The primary difference is that the HVS VM cluster houses only Web Application Servers which are front-ended by a load balancer to balance incoming requests to the deployed number of Web Application Servers. Currently there are two active

web application servers in the VM cluster with the ability to deploy more as demand increases. This approach allows us to quickly respond to planned, unplanned, and sustained increases in demand should they occur. The database for the Web Application Servers in the HVS cluster is housed in a separate, non-virtualized database server capable of handling several hundred thousand client devices. This multi-server deployment is designed to address both scaling and redundancy requirements in a cost-effective manner.

All VM's and databases of the database Server are housed in separate storage clusters configured in RAID 10 which provide the best redundancy and performance.

If a customer experiences latency issues, Beachhead Solutions will work with Rackspace to determine the cause. It may be decided that the best course of action is to create a new instance of BeachheadSecure at a closer Rackspace facility. This can be done quite quickly, but the costs of bringing up the new server instance must be weighed.

Hosting Certifications

SSAE16 / SAS 70

The Statement on Auditing Standards No. 70, commonly abbreviated as SAS 70, is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 provides guidance to service auditors when assessing the internal control of a service organization and issuing a service auditor's report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. Service organizations are typically entities that provide outsourcing services that impact the control environment of their customers. Examples of service organizations are insurance and medical claims processors, trust companies, hosted data centers, application service providers (ASPs), managed security providers, credit processing organizations and clearinghouses.

As of June 2011, the Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, abbreviated as SSAE16, replaces SAS 70.

Rackspace provides SSAE16 certification to its customers including Beachhead Solutions. If a BeachheadSecure customer would like a copy of the certification, Beachhead Solutions will initiate the request with Rackspace and the customer will be sent credentials with which they can retrieve the information.

ISO27001

ISO27001 is an information security standard that was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee on September 25, 2013. It cancels and replaces ISO/IEC 27001:2005. It is a specification for an information security management system (ISMS). Organizations which meet the standard may be accredited by an independent accreditor.

The Rackspace datacenter where the Beachhead Solutions' servers are located has been certified under ISO 27001:2005. The certification was performed by Ernst and Young using CertifyPoint. It is the intention of Rackspace to complete the ISO 27001:2013 certification when their current certification expires.

If a BeachheadSecure customer needs proof of Rackspace's ISO27001 certification, Beachhead Solutions will provide the customer with a copy of Rackspace's current certificate upon request.

Hosting Maintenance and Security at Beachhead Solutions

Only the Beachhead Solutions Administrator and his/her designated backup have OS level access to the server. These individuals have full access rights to the server for purposes of configuration, management and control. They also have full access to the SQL Server, the database, and all its components.

Web portal access at Beachhead Solutions is secured with a private password. The password is changed on a regular basis and distribution is limited to those with administrative need. More importantly, web portal access is restricted to Beachhead Solutions IP addresses which provides an additional safeguard.

BeachheadSecure server maintenance is performed by the Beachhead Solutions Administrator or his/her designated backup. This includes application of updates and service packs and routine reviews of the system logs and system utilization. This data is gathered using Microsoft performance monitoring tools.

Monitoring of the BeachheadSecure application is done through a tool called the "Heartbeat" monitor. This is a custom application developed by Beachhead Solutions to test all application functionality. The application employs phantom devices to create and update records in a monitoring account on the database. These tests are performed every 30 minutes.

Further monitoring of the system is done using Active Xperts tools to test for availability of the web server, web site, and outbound mail services. These components are tested every five minutes.

Backups are performed in two stages. Stage one consists of two on-line backups to disk (on the local server) of the SQL Server database. Stage two backs up the changed files in the entire system via a third party backup solution onto a Rackspace Backup Server as part of the Managed Backup process Beachhead Solutions has put in place with Rackspace. This is a fully automated process that does not involve any intervention by Rackspace personnel.

Any changes to the BeachheadSecure production server environment must go through a Change Control process. This includes patching of the operating system, installation of components and applications, and Beachhead Solutions specific application enhancements or fixes.

Approved changes are then scheduled to go into one of the regularly scheduled maintenance windows. Except in the case of unplanned service interruptions or maintenance durations that exceed the normally scheduled maintenance, no special customer notification is required for this.

Customer notification will always be provided for changes that can visibly affect the BeachheadSecure user interface or have potential impact to the performance of the system. These notifications are provided by the production team via email from the Beachhead Solutions Customer Center (NetSuite) and announcements posted on the BeachheadSecure administrator home page.

Beachhead Solutions have created an Operations Guide to act as a reference tool for existing operations staff, a teaching tool for new operations hires, and a scoping tool for staff outside of operations. The operations team is responsible for ongoing maintenance, monitoring, and software and hardware upgrades. The guide details the steps that must be done for each of these events and the order in which they must be done. In addition, a 'top 10' list of events that can lead to server issues has been included to help educate staff to all the moving parts that must be monitored.

Understanding the Encryption Security on Devices

On Windows PCs

The encryption BeachheadSecure deploys on Windows PCs is EFS (Encrypting File System), BitLocker, or both. The choice is largely dependent on the operating system a device is running. The Federal Information Processing Standard (FIPS) Publication 140-2, is a U.S. government computer security standard used to accredit cryptographic modules. FIPS compliance as it applies to both EFS and BitLocker is described below.

The Encrypting File System (EFS) on Microsoft Windows provides filesystem-level encryption. The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer. EFS encryption has been deemed FIPS 140-2 compliant and by default, it uses the AES-256 symmetric encryption algorithm.

EFS works by encrypting a file with a bulk symmetric key, also known as the File Encryption Key, or FEK. It uses a symmetric encryption algorithm because it takes less time to encrypt and decrypt large amounts of data than if an asymmetric key cipher is used. The symmetric encryption algorithm used will vary depending on the version and configuration of the operating system. The FEK (the symmetric key that is used to encrypt the file) is then encrypted with a public key that is associated with the user who encrypted the file, and this encrypted FEK is stored in the $EFS alternate data stream of the encrypted file. To decrypt the file, the EFS component driver uses the private key that matches the EFS digital certificate (used to encrypt the file) to decrypt the symmetric key that is stored in the $EFS stream. The EFS component driver then uses the symmetric key to decrypt the file. The encryption and decryption operations are transparent to the user and all their applications.

Folders whose contents are to be encrypted by the file system are marked with an encryption attribute. The EFS component driver treats this encryption attribute in a way that is analogous to the inheritance of file permissions. If a folder is marked for encryption, then by default all files and subfolders that are created under the folder are also encrypted. When encrypted files are moved within a volume, the files remain encrypted.

BitLocker is a full disk encryption feature included with the Ultimate and Enterprise editions of Windows Vista and Windows 7, the Pro and Enterprise editions of Windows 8 and Windows 8.1. It is designed to protect data by providing encryption for entire volumes. BitLocker encryption has been deemed FIPS 140-2 compliant and by default, it uses the AES encryption algorithm in cipher block chaining (CBC) mode with a 128-bit or 256-bit key.

In order for BitLocker to operate, at least two NTFS-formatted volumes are required: one for the operating system (usually C:) and another with a minimum size of 100 MB from which the operating system boots. BitLocker requires the boot volume to remain unencrypted. Windows 7 creates the secondary boot volume by default, even if BitLocker is not used initially.

Once an alternate boot partition has been created, the Trusted Platform Module (TPM) needs to be initialized (assuming that this feature is being used), after which the required disk encryption key protection mechanisms such as TPM, PIN or USB key are configured. The volume is then encrypted as a background task, something that may take a considerable amount of time with a large disk as every logical sector is read, encrypted and rewritten back to disk. The keys are only protected after the whole volume has been encrypted, when the volume is considered secure. BitLocker uses a low-level device driver to encrypt and decrypt all file operations, making interaction with the encrypted volume transparent to applications running on the platform.

The Encrypting File System (EFS) may be used in conjunction with BitLocker to provide protection once the operating system kernel is running. Protection of the files from processes and users within the operating system can only be performed using encryption software that operates within Windows, such as EFS. BitLocker and EFS, therefore, offer protection against different classes of attacks.

On Macs

The encryption BeachheadSecure deploys on Macs running OS X Lion or later is FileVault 2. This encrypts the entire OS X startup volume and typically includes the home directory, abandoning the disk image approach. For this approach to disk encryption, authorized users' information is loaded from a separate non-encrypted boot volume. FileVault 2 encryption has been deemed FIPS 140-2 compliant and uses the AES-XTS mode of AES with 128 bit blocks and a 256 bit key to encrypt the disk, as recommended by NIST.

FileVault 2 uses the user's login password as the encryption pass phrase. Only unlock-enabled users can start or unlock the drive. Once unlocked, other users may also use the computer until it is shut down.

On iOS Devices

BeachheadSecure employs the Apple FIPS iOS Cryptographic Modules v4.0 to deploy encryption on iOS devices running iOS 6.0 or later. The iOS Cryptographic Modules, Apple iOS CoreCrypto Module v4.0 and Apple iOS CoreCrypto Kernel Module v4.0, require no setup or configuration to be in "FIPS Mode" for FIPS 140-2 compliance. This encrypts all data and programs accessible to the end user. iOS encryption uses the AES-XTS mode of AES with 128 bit blocks and a 256 bit key to encrypt the disk, as recommended by NIST.

iOS encryption uses the user's login passcode as the encryption pass phrase. A user passcode must be in place for encryption to operate.

On Android Devices

BeachheadSecure employs encryption upon Android devices running operating systems of 4.0 or greater. The FIPS compliance of the solution is dependent upon the hardware chosen. For example, most of the newer model Samsung Android devices provide FIPS 140-2 compliance. The encryption uses an AES 256 algorithm to encrypt the internal storage of the device, but will not encrypt any SD cards.

BeachheadSecure prompts Android users to accept encryption upon their devices. The user can accept or deny the encryption, but the BeachheadSecure administrator can verify whether or not encryption has taken place on any device via a review of the console.

On USB Flash Devices

BeachheadSecure employs a proprietary encryption method to protect data upon USB flash devices. This proprietary method is a secure vault for the information your applications create, process or archive. BeachheadSecure for USB Flash Devices offers a container with hierarchical structure, on-the-fly encryption and compression. Transparent strong encryption based on a 256-bit AES algorithm is applied to the whole storage container.

BeachheadSecure administrators control the behavior of USB devices created on BeachheadSecure PCs. The most common deployment is the 'Bring Your Own Device' (BYOD) model. A user's personal items are left unencrypted, but an encrypted container is created for all data copied from the protected PC. User credentials are required to unlock the container to allow access to the encrypted data. These credentials are created by the end user during the encryption process.

Understanding Security for the BeachheadSecure Client

On Windows PCs

After installation, the BeachheadSecure client software is visible to the end user in the Add / Remove Programs listing. However, if an end user attempts to uninstall the program, they will be denied. Every attempt to uninstall the software prompts a check-in with the BeachheadSecure server to determine if the device has administrative permission to remove the product. An 'uninstall' can only occur if the BeachheadSecure administrator who manages the device sets the device status to 'inactive' before the uninstallation process begins.

Even after a successful uninstall, the files on the device will still be encrypted. Only the software is removed. A decryption utility must be used to decrypt the files to complete remove the effect of the product.

The BeachheadSecure client software is a signed agent. Beachhead Solutions has chosen Startcom to sign the product because of their double signature technology. This technology gives Beachhead Solutions the additional capability to sign all drivers issued with the product.

The BeachheadSecure client software has been screened for exploits in the past, but no regular schedule is currently in place. Some customers and resellers have required the screening in the past and no issues have been found to date.

Some anti-virus applications have been known to the block the BeachheadSecure processes. Customers will be told which processes to whitelist within the anti-virus application in order to make sure BeachheadSecure continues to operate properly.

On Macs

Unlike the PC, it is possible for an end user to remove the BeachheadSecure product from a Mac without administrative permission. However, as with the PC, the Mac will still be encrypted with FileVault 2. If an end user is successful in attempting to remove the software, the BeachheadSecure administrator will still see the device in the computer listing on the console, but the device will no longer be able to check in.

On iOS Devices

Once BeachheadSecure is installed upon an iOS device, if the end user attempts to uninstall the app, it will be reinstalled upon next check-in.

If the iOS MDM profile is removed, then the device is no longer aware of BeachheadSecure and a reinstall will not occur. However, the BeachheadSecure administration will be alerted that the device is no longer checking in.

Without BeachheadSecure on the device, an end user could remove the need for a passcode which leaves the device without encryption.

On Android Devices

BeachheadSecure Android administrators can activate a setting within their accounts to lock Android devices which attempt to remove the BeachheadSecure application. With this setting in place, if an end user attempts to uninstall the app, the device will be locked and the password will be changed. The end user will need to contact their administrator in order to regain access to the device.

On USB Flash Devices

Once a USB Flash drive is protected with BeachheadSecure, the end user cannot bypass the encryption provided

for the data written to the container. When viewing the drive via the Windows File Manager, the encrypted container will appear as a file. A warning is placed at the root of the drive to tell end users not to delete the container file. If the container file is deleted, all of the data within the container will also be deleted. If the drive is then plugged back into a PC protected by BeachheadSecure, a new, empty container will be built and a new USB Flash drive will appear on the administration console.

Understanding the Security on the Administration Console

Access to the BeachheadSecure administration console is initiated via a Hypertext Transfer Protocol Secure (HTTPS) link. HTTPS provides authentication of the website and associated web server that one is communicating with, which protects against man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication. In practice, this provides a reasonable guarantee that one is communicating with precisely the website that one intended to communicate with (as opposed to an imposter), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

For each customer account, each account administrator has access only to their specific account. They are not able to identify or gain access to any other customer account for which they do not have credentials. Credentials for the BeachheadSecure administration console include a user ID and password. Upon account setup, a root level administrator is granted access to the console. The root level administrator of each account is the only administrator that can create other administrator accounts and only for their specific account.

Administrative password policies include expiration timing, enforcement of password history, minimum password length, complexity requirement, maximum invalid logon attempts, and lockout period length.

Any actions performed by BeachheadSecure administrators are logged, time-stamped, and available for review. That means any changes to policies, rules, devices, etc. can be traced back to the date and time the administrator in question performed them.

Each time a device executes a rule, misses an important check-in time, or experiences other important events, the BeachheadSecure administrators for the account which contains the device will be notified via email alert once. Each alert will be sent only once per trigger event. The alerts within the product are configurable by the root administrator. In addition, these events will be written to the device log and will appear on account site reports. Log information is kept for at least 35 days before it is pruned during server maintenance periods. If a customer requires that log information be kept longer, they should contact the Beachhead Solutions support staff.

Understanding the Security of Client / Server Communications

BeachheadSecure devices initiate check-in with the BeachheadSecure server at pre-defined intervals. This communication is encrypted using a 2048 bit RSA key via a Secure Sockets Layer (SSL). The encryption is Advanced Encryption Standard (AES) using 128 bit blocks.

BeachheadSecure customers should not have to make any firewall or network changes to allow for the communication between their clients and the server. All communications, including BeachheadSecure's use of

BEACHHEAD

the Background Intelligent Transfer Service (BITS), are done via secured port 443.

Beachhead Solutions Inc.

1955 The Alameda

San Jose, CA 95126

408.496.6936 x-1265

Question, comments? Write Beachhead

sales@beachheadsolutions.com