Manager+Agents™

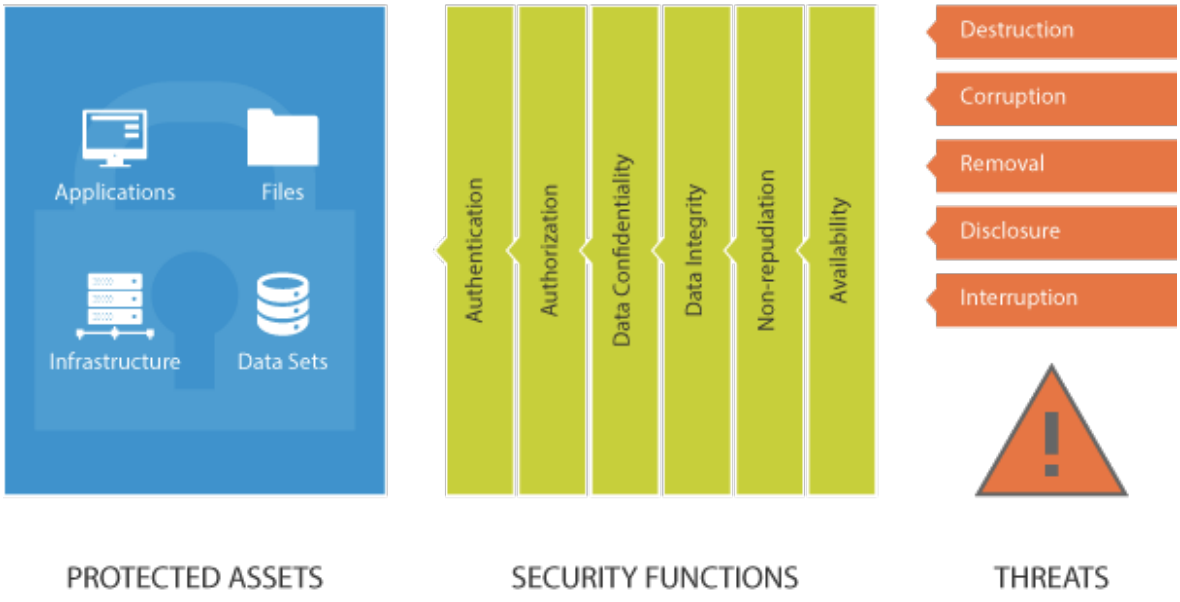
Signiant's Manager+Agents Content Security Strategy

Introduction

Effective security requires much more than encryption during transfer or storage. Even the strongest lock is only as effective as the protection of the key or combination used to unlock it.

Signiant's Manager+Agents software, in conjunction with appropriate organizational policies and procedures, protects assets from threats posed by individuals, hacker groups and criminal adversaries. Assets, including computing and network resources, intellectual property, business timelines, and reputation must be protected from threats including destruction, corruption, disclosure and interruption.

Manager+Agents implements security services including authentication, authorization, data integrity, data confidentiality and non-repudiation, to mitigate these threats.



91 Hartwell Ave. - Lexington, MA 02421
p: +1 781.221.4051 - www.signiant.com

SIGNIANT®

Authentication services confirm that someone or something is what they claim to be.

Signiant's Manager+Agents implements authentication services in the form of login and password credentials with the added certainty of certificate-based authentication. Whenever passwords are used for client side authentication, the server side is authenticated using SSL certificates from Comodo certificate authority (CA) to make sure that User IDs and passwords are sent to the intended target and not some rogue man in the middle trying to steal authentication credentials.

Signiant ensures that mutual certificate-based authentication keys are always employed for machine-to-machine connections and that the distribution of these keys is secure so that they can be reliably used in the authentication process.

Signiant also enforces password policy, including a configurable expiration cycle that requires users to change passwords periodically, and minimum password strength validation to require users to create formidable passwords.

Enterprise customers have the option to use Active Directory or LDAP, where authentication occurs behind the customer's firewalls. Through Active Directory and LDAP, customers can implement multi-factor authentication as well.

Authorization services implement and enforce access policies to data.

Manager+Agents is able to "box in" transfers to a particular directory on a particular host server, so that access policies can be enforced as designed. The software does this by connecting to the host using a local or domain userID, and thereby adhering to the access rights policy assigned to the user on that server.

Similarly, users can be enabled or restricted when running transfers, monitoring, and reporting according to the access rights given to their profile.

Data integrity services protect information assets from corruption.

Signiant employs hashing and digital signing of data during transit to prevent malicious tampering and errors between sending and receiving parties.

91 Hartwell Ave. - Lexington, MA 02421
p: +1 781.221.4051 - www.signiant.com

SIGNIANT®

Data confidentiality services protect information assets from disclosure.

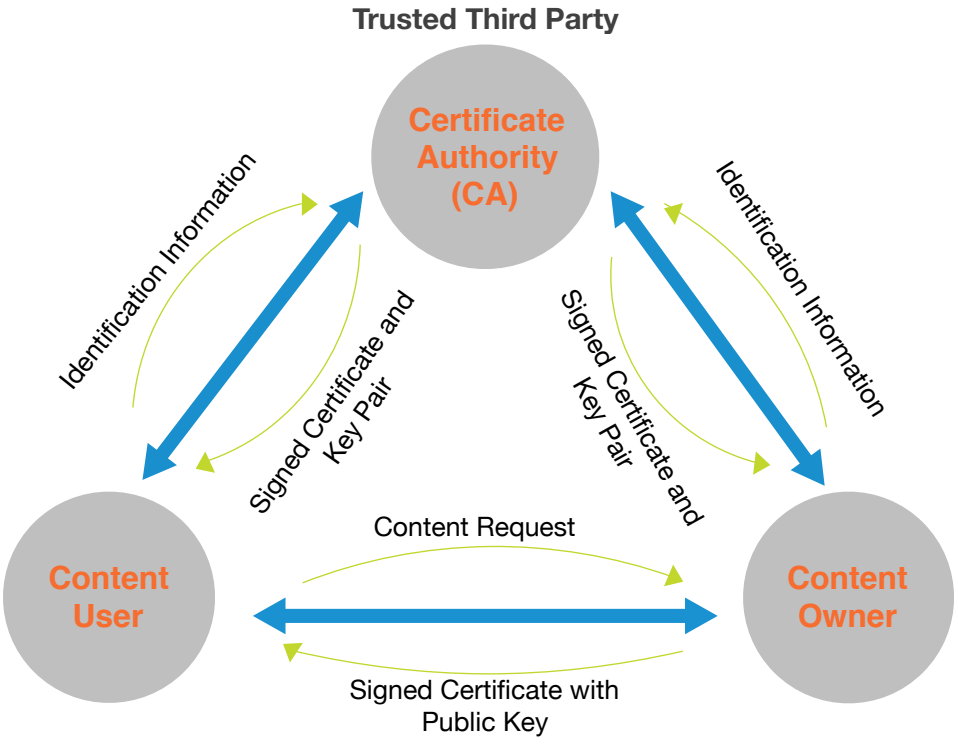
Manager+Agents employs 256-bit AES encryption to ensure data confidentiality during transfer of files and when the file is at rest. Though AES encryption is the 'state-of-the-art' for encryption, it is very important that the encryption key management scheme is 'state-of-the-art' as well. You can have big lock on the door, but if anyone can find the key under the mat, then the door is not secure.

Signiant encryption keys are managed with the same public key infrastructure that Signiant uses for authentication services, including the Comodo certificate authority. This key management scheme ensures that the encryption keys are secure in transit and at rest.

Non-repudiation services provide a trustworthy record of what has been done by whom and when.

The reporting and log files provided by Signiant products enable companies to determine the complete history of a file's movement. The data will allow a forensic analysis of who, where, and when file assets were moved. Signiant user interfaces an audit trail of both end-user and administrative activity.

The "certified delivery" function provided by Signiant software identifies each file that has moved from a source to a target, along with signed hashes of the file as computed by the source and target agents. These signed hashes are compared and if they match, it is guaranteed that the file has not been modified in transit.



91 Hartwell Ave. - Lexington, MA 02421
p: +1 781.221.4051 - www.signiant.com