Ohanae®

Trust No One… Encrypt Everything!

Business Primer

March 2014

This white paper explores cloud users' requirements for data access and sharing, especially in relation to trends in BYOD and personal cloud storage in the workplace. Next, it key threats that attempt to compromise either user login or data and different approaches to solving these challenges in a corporate environment are discussed. The drawbacks of alternatives are discussed in the context of the Ohanae offering for businesses.

Trust No One…Encrypt Everything!

Today's business environment is dynamic and ever changing. The concurrent, twin trends towards widespread use of cloud based file synchronization and sharing (FSS) solutions, and bring-your-own-device (BYOD) have created new opportunities for those who would steal data and access, and new challenges for protection against this theft.

The Rise of Cloud Data

Ostermann Research indicates that cloud based file synchronization and storage had a significant use footprint of over 591 million seats in 2012[i]. Although growth has been tremendous over the last few years, continued uptake will occur through 2017, leading to adoption by over 781 million seats over the five year period.

As the moniker FSS suggests, the primary drivers for the use of cloud based storage has been synchronization (sharing between multiple devices of the same user) and sharing (sharing between the user and other individuals, either inside or outside of the company). The other users could include friends, collaborators, or any extended team.

The characteristics of data protection between these two types of sharing are fundamentally similar. Confirmation of identity is required as a first step. Once identity has been established, it provides the basis for authorization to access data. Finally, acceptable uses may limit the types of manipulation of the data that are permitted.

Bring Your Own Device

The proliferation of smart devices – smartphones and tablets, and the preference for laptop configurability according to user specifications has led to a sea change in the standard, centralized control over computing assets within an organization. In today's modern world, recent studies have shown over 80% of employees access some level of corporate data through their non-work mobile devices.

This trend for wider use of devices in conjunction with typical professional activities combines with the availability of data shared between multiple devices to allow employees using cloud data synchronization to easily access sensitive company data on all their devices and systems. Of those using BYOD devices, a Forrester research study found more than 70% were using IT "unsupported" software packages such as Dropbox.

With employee exposure to consumer targeted file synchronization and sharing products, these employees have been quick to adopt the same technologies to allow sharing in the business perspective. However, this adoption has run counter to typical corporate IT objectives around data security, which mandate control of data movements – especially outside the corporate networks, protection of data at all times, auditing of data sharing, and tracking of people who have access to sensitive data.

Sealing the Leak

The uptake and adoption of both the cloud data and the BYOD trend are inevitable, with "exponential" increases by 2018 according to a 2013 Forrester report. Corporate initiatives focused on strictly controlling devices, and turning personal assets into managed corporate assets are unlikely to succeed in all but the most secure environments. In order to succeed, companies must focus on "sealing the leak". By sealing the leak, companies can ensure that employees are able to productively synchronize data between their devices, and share with authorized collaborators while maintaining strict data protection practices.

Costs of Leaking Data

The costs of data compromise are multi-fold. First, there is the direct cost of property compromised through data loss. This includes money directly lost through compromised financial information as well as the direct value of data itself, either intellectual property, proprietary research and development, or competitive information.

Second, there are public perception costs to data loss, in terms of organizational reputation damage. Known data losses can cause customers to change to competing products, partners to disengage, and potential investors to look at other alternatives.

Finally, there are productivity loss costs associated with data loss. These may be either direct costs, where information for projects that are in progress is lost and must be recreated, or indirect costs where loss of data results in security reactions that, in turn, cause productivity loss due to the inability to share between multiple parties.

The costs of data loss are staggeringly high with individual costs of data breaches of customer information at almost $200/record [ii], costs of data loss related to laptops at almost $50,000/laptop [iii], and aggregate worldwide costs estimated in the hundreds of billions worldwide [iv].

Costs of Login Compromises

Login compromises also have several costs. First, compromised logins can directly lead to compromised data in the cases where the logins are securing data stored in the cloud.

Additionally, logins are a primary target for identity theft, and one of the primary means of accessing financial information or accounts, including cash accounts and credit accounts for individuals or businesses.

Finally, the threat of login compromise prevents efficient business processes around multi-party use of credentials. Businesses attempt to mitigate the risk of compromise by lowering the exposure of multiple parties using the same credential.

Together, the costs of data compromise and the costs of login compromise push individuals and business entities to establish tighter and tighter controls around data and logins. These stricter control regiments inevitably prevent easily and securely sharing data across either multiple devices of a single user, or between multiple users.

Market Needs vs. Product Reality

Individuals and businesses within the market need a product that secures both data and logins, facilitating and encouraging cloud data storage while encouraging sharing between devices and users in a secure, easy-to-use fashion.

In addition, for businesses that don't have large, dedicated IT staff, solutions are desired which don't require building on-premises infrastructure (servers, secured networks, VPNs, etc.).

Current products addressing the market space include individual offerings for password management and data protection.

Password Managers

Password management offerings in the market include single device offerings that use a centralized store to hold login credentials (typically passwords). The centralized store is often stored on a single device, although many implementations provide a cloud-based store where multiple devices can use the password store. In most implementations, the password store is protected through encryption, and the user must provide an encryption key, password, or passphrase to unencrypt the store prior to use.

Data Protectors

Data protectors come in a few flavors. One system of data protection monitors exit points from the device and prevents information flow from the system. This approach solves data compromise problems by simply not allowing data off the device – however, this prevents any use of cloud data storage, and precludes sharing between devices or users.

The second type of data protection is encryption. Encryption generally uses a key to encrypt data prior to storage. In some implementations, the user specifies the key during access; in others, the user specifies a key that unlocks stored encryption and decryption keys.

Encryption solutions also differ in the methodologies of the implementation. Some implementations encrypt on the local system, and allow cloud services to synchronize the encrypted data. Some encrypt the data prior to transmission to a cloud system, and some rely on the cloud storage provider to encrypt the data.

Beyond the timing of the encryption operation, the keys used to do encryption vary. In general, approaches that use longer key lengths, or stronger algorithms (AES vs. RSA for instance) provide solutions where data is harder to hack through brute force attacks. Approaches which rely on a strictly PKI based approach (with certificates issued and used) often have significant challenges around certificate and key management.

Finally, encryption approaches also vary on the requirement for a proxy server between the user and the cloud data provider. In some implementations, there is no proxy required. In others, a proxy server sits between the two and takes unencrypted transmissions from the client and turns them into encrypted transmissions prior to connecting to the cloud data storage. In others, the proxy server becomes a dedicated cloud data storage provider of its own, with all the data remaining within the user or enterprises control.

One or the Other: Both Incomplete

Both password management and data protection as stand-alone solutions suffer from weaknesses in the total solution.

Only password management ignores the problems around data protection. It assumes all data access is controlled via user credentials and keeping these credentials safe is sufficient to secure the data. However, this is not the case – cloud data providers are susceptible to direct compromise – by physical or network breaches, data snooping, or by unauthorized access by internal personnel of the cloud data provider.

Conversely, only protecting the data ignores the fundamental problem that login access is typically the predominant method for a legitimate user to validate identity and gain access to the data. An attacker who is able to compromise logins can use this to impersonate the valid, allowed user and access data directly.

Finally, the additional complexity of file sharing often brings compromises in security. For instance, cloud data providers typically have simple mechanisms for sharing files that allow access to anyone with the correct URL. Direct sharing of data (via email, instant messaging or other peer-to-peer protocols) also tends to have very limited management and controls – files transferred in this way can typically be intercepted by or forwarded to other parties that will also be able to access them.

The Ohanae Solution

Ohanae provides a device-centric combined solution for both login and cloud data protection. Both services are based on patent pending technology that prevents storage of keys anywhere (on local devices, with cloud data providers, or on Ohanae cloud servers). Instead, keys are generated on the device at time of use, used, and then disposed of.

Ohanae provides integrated sharing capabilities based on public key infrastructure (PKI) standards when sharing between multiple users. Sharing between devices of the same user is accomplished using Ohanae's proprietary algorithms.

This combination allows decryption keys to be totally controlled by the data owner. These keys are used only at the point of encryption/decryption and never shipped off device. These keys are used to protect data (files "at rest" on the local filesystem, "in motion" between the local device and a cloud data provider, and then "at rest" again in the cloud data provider. The cloud data provider does not have access to decryption keys, and cannot access the unencrypted file content. Additionally, any compromise of the cloud storage provider (for instance by accessing the user's account) also only provides access to the encrypted data.

Ohanae uses cloud based servers to store public user information, and as a transmission point between multiple devices. There is no requirement for an on-premises server (and the IT costs associated with such an infrastructure). The Ohanae cloud servers do not hold any encryption keys, simply configuration files, so a breach of the server does not allow access to any sensitive information. Additionally, allowed devices authenticate to the server using the SRP protocol which precludes impersonation attacks by non-authorized devices.

Finally, the device specific real-time generated keys are used to secure login credential information (typically passwords) for all sites used by a user. This allows the user to have arbitrarily complex and individual passwords on each site – preventing a large number of account attacks (dictionary, brute force, etc.).

Conclusion

Ohanae software allows users to protect their data and their logins through industry standard, high strength encryption. Everything is encrypted, and accessible only to the user from authorized devices. This two-factor security allows users to tame the inherently untrustworthy environment of the cloud, and operate as though they trust everyone – secure in the protection of their data and login information through the Ohanae system.

Trust No One, Encrypt Everything.
Ohanae is your Armor Shield for the Cloud.

(Endnotes)

[1] File Synchronization and Sharing Market Forecast, 2012-2017, Osterman Research http://www.ostermanresearch.com/whitepapers/orwp_0189.pdf

[2] 2013 Cost of Data Breach Study, Ponemon Institute, https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

[3] The Billion Dollar Lost Laptop Problem, Ponemon Institute, http://www.intelligenceinsoftware.com/featur/feature/it_software_strategy/lost_laptop/index.html

[4] Forbes, http://www.forbes.com/sites/andygreenberg/2012/08/03/mcafee-explains-the-dubious-math-behind-its-unscientific-1-trillion-data-loss-claim/