Ohanae®

Cloud Privacy Protection

Protect Your Cloud Privacy

Ohanae uses patent-pending algorithms that generate cryptographic keys that never leave a user's desktop or mobile device. The private keys are used to protect confidential information stored by cloud services. They are also used to secure files before transfer to others by common applications including email, Skype, iMessage, and cloud sharing. Ohanae also easily generates complex passwords for application and web service access with the same patent-pending protection.

The Problem

Three independent forces have converged to create a perfect storm for security professionals. These three trends together have resulted in user data being widely available in the cloud, across numerous user devices, ultimately secured with easily compromised passwords.

First, cloud storage use for file sharing has increased dramatically as consumers have embraced remote storage and brought it with them into the workplace.

Second, employees use email or cloud sharing services to send company confidential information to other employees, customers, and partners. This information is unprotected and easily compromised in today's privacy threatened world.

Finally, the proliferation of Internet sites has created a situation where users access numerous sites, including cloud storage using a small number of easy-to-remember passwords.

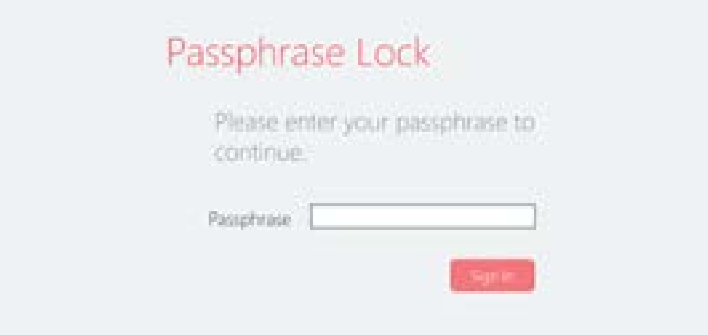
Cloud Security Challenges for Business

Without full-time IT departments and substantial budgets, enterprise mobile device management applications are not a good solution for Small and Midsize Businesses. Smaller companies need cloud security with smaller IT footprints and Software as a Service (SaaS) based pay-as-you-use costing.

A comprehensive solution for Cloud Privacy Protection addresses the challenges in a manner that complements smaller companies' IT priorities and constraints.

The Ohanae Solution

The Ohanae solution addresses all three trends, providing complete Cloud Privacy Protection.



Passphrase Lock

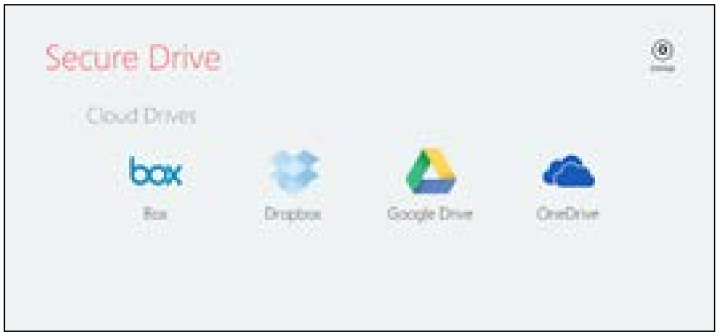
Please enter your passphrase to continue.

Passphrase

First, data at rest (either on the local machine or in a cloud storage provider) is encrypted. This prevents compromise from unauthorized users that are simply able to access the raw data. This includes attackers as well as cloud storage provider administrators, network providers, and government agencies.

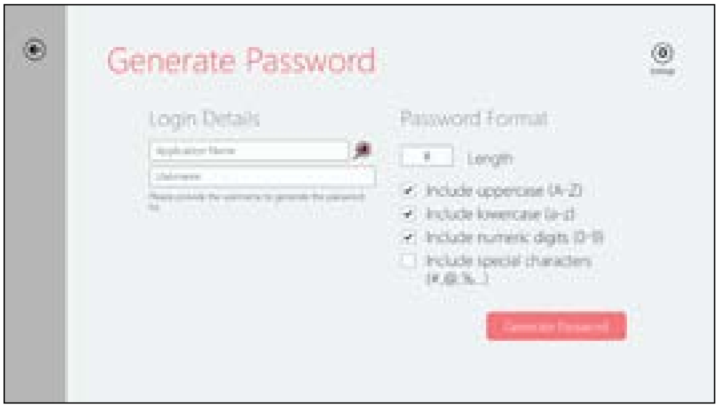
Second, Ohanae provides secure file synchronization and sharing. Secure file sync allows a user to move files between devices without risk of data compromise. Secure file sharing allows a user to share files with others using industrial grade encryption.

Third, Ohanae protects against compromise of logins that might expose web resources, including data stored in the cloud. This is done by providing secure password generation, management, and sharing between all user devices.



Secure Drive

Cloud Drives



Generate Password

Login Details

Application Name

Username

Password Format

8 Length

☑ Include uppercase (A-Z)

☑ Include lowercase (a-z)

☑ Include numeric digits (0-9)

☐ Include special characters (#,@,%,..)

Finally, the complete Ohanae solution achieves all three aims while protecting the cryptographic keys. Keys are dynamically generated only when needed. Multi-factor authentication is used to ensure that data and login access is only granted to the authorized user while using an authorized device.

Since the Ohanae solution is cloud based SaaS, no additional IT infrastructure or team is required to support Ohanae servers. Client packages are small, easily installed and updated automatically by individual users without IT intervention.

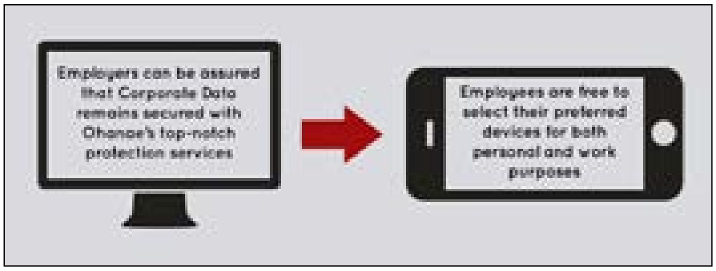
Account Options

Ohanae software supports the popular Windows and Macintosh operating systems on laptops and desktops. On mobile devices, Ohanae supports iOS, Android, and Windows.

Ohanae is available in three different capability tiers. The free version provides the complete Ohanae suite of functionality for a single device. This allows for a user to secure logins and data on devices and in the cloud. Also, the user may share securely with other Ohanae users.

In the premium version, all the capabilities of the Ohanae system are expanded to support up to eight devices for a single user. Ohanae transfers information required to regenerate passwords and unencrypt data across all devices. Secured data stored in the cloud storage by Ohanae on one device may seamlessly be accessed on all other Ohanae devices for the user.

The business version includes all the capabilities of the premium version across eight devices and also includes remote management capabilities for the business.



Employers can be assured that Corporate Data remains secured with Ohanae's top-notch protection services

Employees are free to select their preferred devices for both personal and work purposes

Secure Workplace

Secure workplace allows the business administrator to require that all data be stored in Ohanae secure locations. Data that is stored in an unprotected location is removed from the device on device or Ohanae shutdown. This feature ensures that privileged corporate data may only be accessed using Ohanae in protected locations at all times.

Remote Wipe

Remote wipe allows a business administrator to quickly remove access for a specific device. This feature is primarily of use when a trusted device is lost or stolen. It allows administrators to very quickly prevent any unauthorized access in this case – even if the user passphrase is compromised.

Device Enablement

Device enablement allows users or administrators to disassociate registered devices from a specific user. For users, this is useful when a device is sold or otherwise disposed. For businesses, this is useful when devices are reallocated to other users.

Make Ohanae a Part of Your Business Now – Protect Your Privacy in the Cloud

Visit http://www.ohanae.com to download Ohanae and get started today!