Securing Data across the Dynamic Enterprise

By Topia Technology

Challenge 2014: Ensuring enterprise data security and accessibility

Enterprise data must be both secure and accessible—tough challenges, each, and today's enterprise must ensure that their information sharing environments both protect data and allow collaborative access to a rapidly evolving range of users, devices, and services. Specifically, secure, reliable data sharing must perform for global user bases, across computing environments with different security levels, support mobile and BYO (bring your own) devices, and integrate cloud and local services. Current coverage of massively damaging security breaches at Target, Snapchat, and Starbucks prove that data encryption alone is inadequate to these challenges.

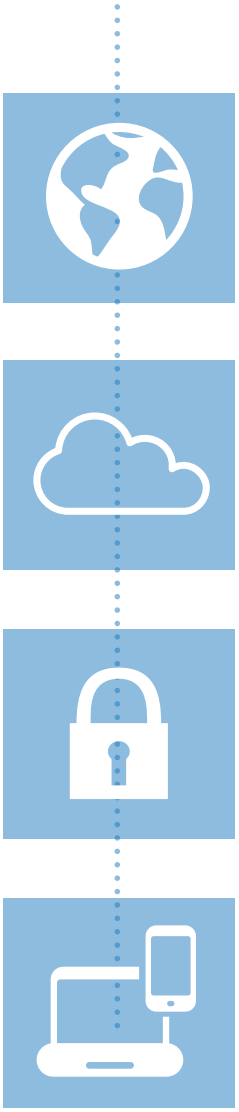
Encryption is not enough

Data encryption is essential to securing enterprise information, but it does not provide a comprehensive solution. Recent reports that the NSA can not only break industry standard encryption algorithms but has paid cyber security firms to weaken those algorithms (NY Times, 17 Jan 2014) underscore the need for additional security methods when data are in transit or at rest.

McAfee Labs (Dec 2013) predicts a substantial increase in attacks aimed at shared resources in the cloud, and organizations will face additional threats due to vendor security and the unintended—and unsecured—comingling of personal and corporate data on home and mobile devices and in the cloud

(InfoSecurity Magazine, Jan 2014).

Secure, reliable data sharing must perform for global user bases, across computing environments with different security levels, support mobile and BYO (bring your own) devices, and integrate cloud and local services.



secrata

Encryption, even properly used, can fall prey to threats including sniffing, brute force attacks, and malware, and is not proof against environments where encryption keys are stored locally or co-located with data, and where third-party applications integrate with cloud services. All of these threats resonate in today's enterprise computing--they cannot be merely avoided, they must be solved for and secured.

Additional challenges include a huge growth in the use of mobile devices and BYOD users. Administrators must attempt to secure these devices, the data they store and access, and both the cloud services they access and the connections across which they access them. Each represents a new security threat, and none are rendered secure by encryption alone.

Finally, security professionals must address a variety and range of security policies for applications and services and ensure that enterprise employees adhere to these policies and practice secure computing. Encryption doesn't apply here, at all.

Encryption, even properly used, can fall prey to threats including sniffing, brute force attacks, and malware, and is not proof against environments where encryption keys are stored locally or co-located with data, and where third-party applications integrate with cloud services.

Enterprise data security challenges

Threats to encryption

Mobile and BYOD users

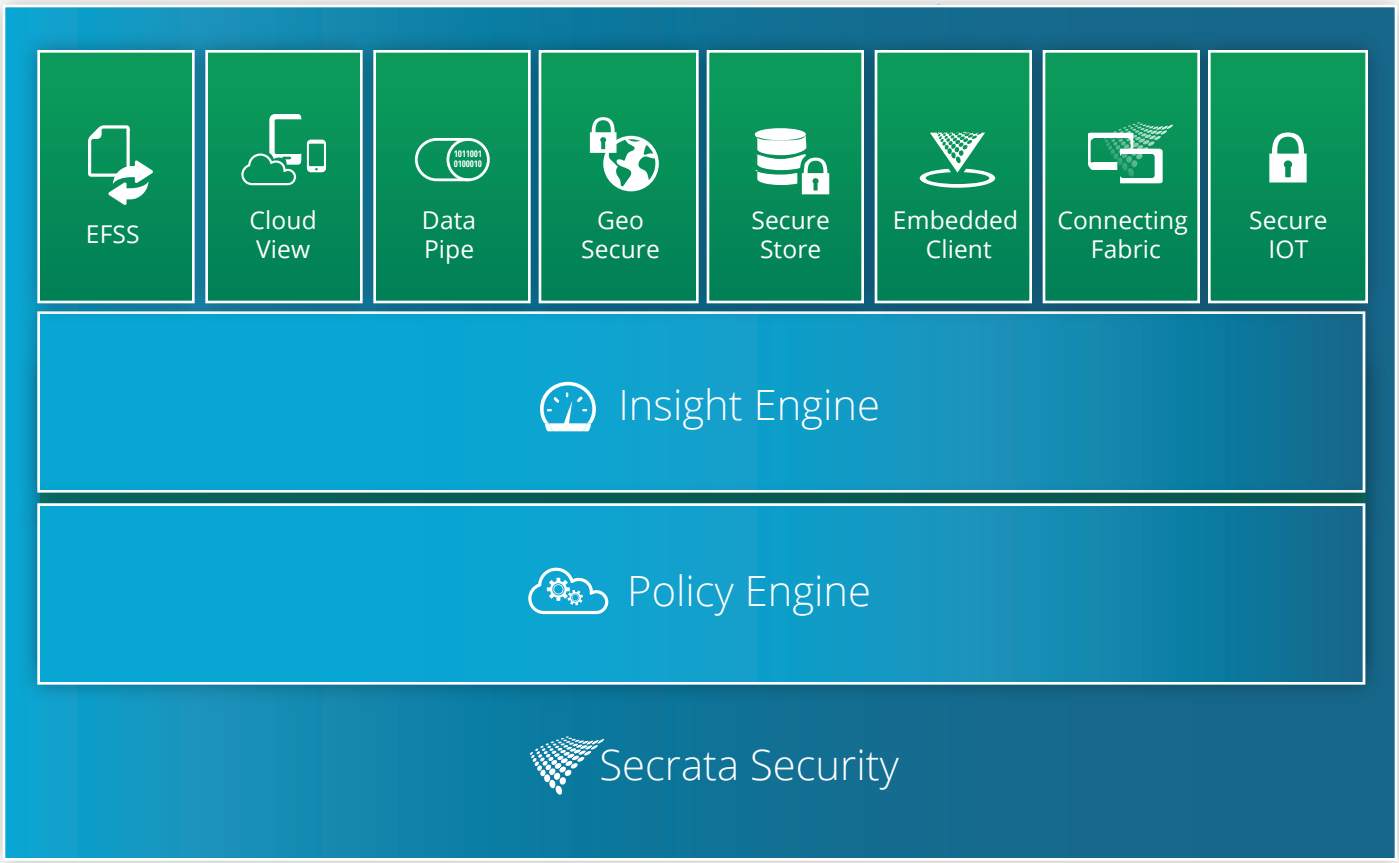
Security policies for enterprise employees

Secrata:
Infrastructure for moving data and files

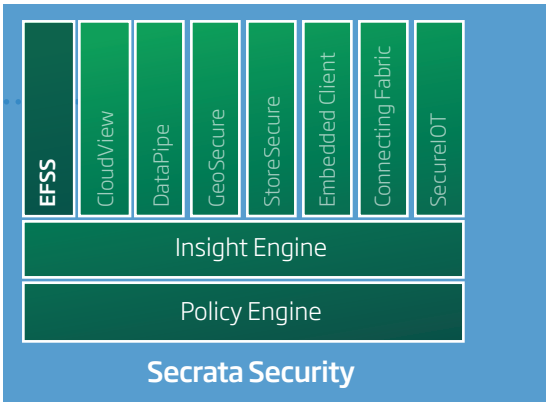
The answer to these challenges must address each aspect of today's evolving enterprise environment. Cloud services like Box, Egnyte, and Syncplicity that originally targeted a consumer market have attempted to retrofit their security implementations to meet enterprise requirements, slapping on a veneer of encryption that fails under fire.

Secrata™, a Topia Technology platform, ensures data security and accessibility by providing an infrastructure designed specifically for moving data and files within and across enterprises and the cloud, on network, home, and mobile devices.

Secrata is a modular platform, comprising a seamless infrastructure for controlled and flexible data movement.



EFSS: Secure enterprise file sync and share



Enterprise File Sync and Share (EFSS) is the most secure way to move and manage files across content locations (data stores). This Secrata module ensures full control and visibility for IT, and provides ease of use for employees. EFSS uses workspaces to help the user manage their files. An integrated messaging platform provides a way to securely collaborate and annotate documents. EFSS is easily integrated into existing workflows to drive adoption and extend corporate assets. IT can control where files can reside and be sent, using a powerful policy engine. EFSS is elegantly simple to use, and powerfully secure.

EFSS performs secure file sharing and syncing across devices and platforms. Using a simple and elegant interface, users can securely share files in three quick steps:

1. Create an invitation-only workspace
2. Invite others using their email address
3. Add content files

EFSS ease of use is fortified by a powerful security framework that far surpasses the use of simple encryption and SSL; EFSS with Secrata ensures that sensitive file and data assets are protected wherever they live. EFSS breaks individual file data into chunks; chunks are then encrypted, with each chunk given a separate key; chunks are stored and transferred in non-sequential order, and their location is listed, and the list is encrypted and stored on the client; thus, a file's individually encrypted chunks and that file's encrypted reassembly instructions are stored separately and cannot be re-assembled or decrypted without authentication. This triple-layer security implements encryption, separation, and authentication, and is proof against brute force attacks and more innovative security threats.

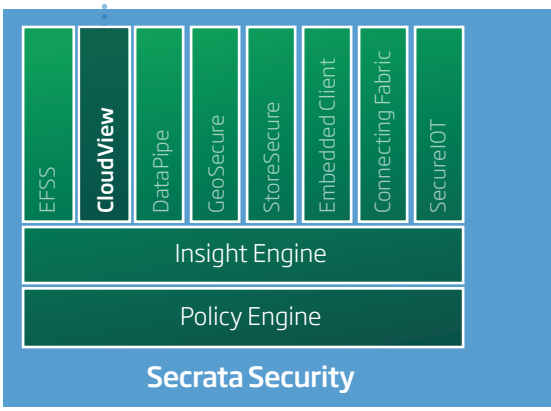
EFSS with Secrata also allows enterprise security specialists and system administrators to roll out, manage, and ensure compliance with enterprise data security policies. Policies may be adjusted by user, device, or service, and files may be coded with metadata that aligns with security policies covering access and sharing privileges.

EFSS ease of use is fortified by a powerful security frame that far surpasses the use of simple encryption and SSL

Secrata file transfers are also fully logged and auditing by service, device, user, workspace, and file is supported. Audit reporting data may be exported to other applications to mine system and service intelligence.

CloudView

CloudView creates a unified user experience across file locations. This Secrata module allows the enterprise to securely register content where it lives—no need to aggregate files into a single location or cloud vendor. CloudView extracts metadata to securely and easily find and manage files no matter where they reside. Files are not dumbly replicated but are securely made available to access or share from any data store. IT remains in control and the user remains productive.

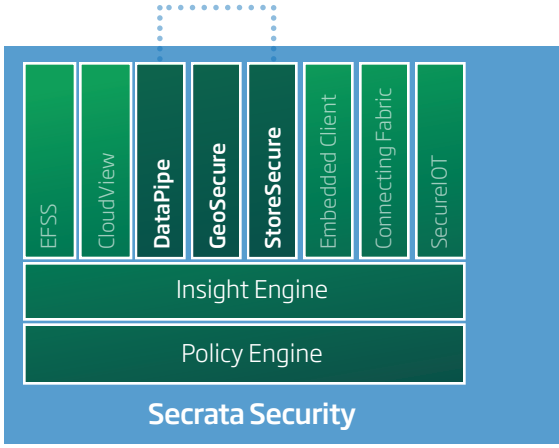


Using a single interface, CloudView with Secrata allows users to access and manage all of their data and file assets wherever that information is locationed, across devices, and cloud services.

Once a user registers a device (desktop, laptop, tablet, or smart phone) or a location (network attached storage, fileshare, or cloud services like Box.net or Google Docs), CloudView automatically creates a secure index of the data assets and files located on the device or stored by the service. Content indices are searchable using basic and advanced search functions through CloudView.

From any registered device, CloudView users can find, move, share, update, remove, and otherwise manage all of their data, regardless of where it is stored. Data and files are protected by Secrata's multi-faceted data shredding and layered encryption features.

By allowing this powerful single interface, CloudView with Secrata harnesses and secures the power of the cloud for enterprise use without losing the flexibility required by today's BYO device user.



DataPipe

DataPipe is the most secure way to move data between machine end-points. This Secrata module enables secure optimized transfer of any type of data to a remote location. Now, POS transactions, medical device data, or any point-to-point data transfer can have unmatched security that goes far beyond encryption.

GeoSecure

GeoSecure adds a new dimension to data security—*location*. This Secrata module uses GPS and IP geo-location to give you a powerful way to secure data based on a user's physical location. Administrators can restrict access to files and data in a Secrata Workspace when access is attempted from a restricted location. Now, you can ensure that sensitive assets cannot be downloaded, shared, or even viewed from dangerous locations such as foreign countries, unsecure WiFi networks, or outside a company location.

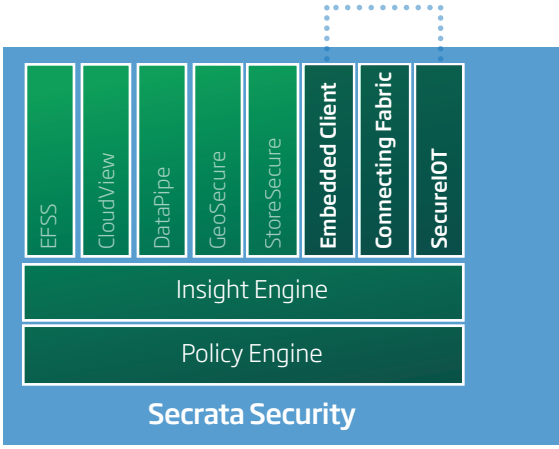
StoreSecure

StoreSecure allows the enterprise to shred and encrypt files at rest. This Secrata module goes beyond encryption and introduces shredding with unique encryption keys for each resulting shred. The enterprise now has a way to further mitigate the risks to its files assets.

Secrata protects sensitive data and file assets beyond the enterprise

Embedded Client

The Embedded Client allows Secrata to be integrated into devices and applications through the inclusion of a library containing a micro-client for Secrata. This micro-client provides all the secure access and transfer of data like a full client, but with a reduced footprint and entirely programmatic control.



Connecting Fabric

Integration with third-party applications is also secure using the Connecting Fabric integration module and software APIs. Connecting Fabric allows integration with Secrata, CloudView, or other Secrata modules, free from the threat of malware, both to the enterprise and to the external integration platform.

Secrata is seamless infrastructure for flexible and powerful data movement

SecureIOT

As connectivity expands with the introduction of IPV6, SecureIOT enables secure transfer from emerging categories of network enabled devices. By shredding and encrypting data between these devices, your Internet of Things can expand with unmatched security.