SOLUTION BRIEF

MACHINA™ TOOLS FOR CLOUD STORAGE

Organizations are embracing the complete freedom and control that a multi-cloud approach for storing their data offers them. You can now easily run any application, workload, or store data in any cloud of your choice. Or can you? The reality is that technical and operational limitations around cross-cloud portability are still restricting freedom of choice across modern enterprises.

But adopting and operating in a multi-cloud environment doesn't need to be complex or inefficient, and it definitely doesn't have to come with a high security risk and cost of ownership.

Choosing your multi-cloud strategy based on ideal business and technical requirements is possible today, along with having the ability to adjust and align your data security needs to your business goals or impending regulatory requirements, at any given moment in time.

SOLUTION OVERVIEW

Machina Tools for cloud storage provides a multi-cloud data security solution that extends policies and standards across all three of the major public cloud storage providers, as well as on-premises, to meet business and financial needs while helping organizations fully comply with current and future regulatory requirements.

Ionic provides a single interface to consistently secure and enforce access control standards to data in and across multiple public clouds, on-premises data stores, and hybrid infrastructures.

The solution leverages standard features of Machina to easily support enterprises seeking to gain cross- and multi-cloud data security capabilities via a single platform that provides:

- Data encryption
- Key management at scale
- Consistent policy management and enforcement
- Audit visibility into data access/transactions

By using Machina Tools for cloud storage, developers can easily create new or modify existing applications to apply cryptographic protection to data, abstracting key management, policy enforcement, and audit logging from their application code.

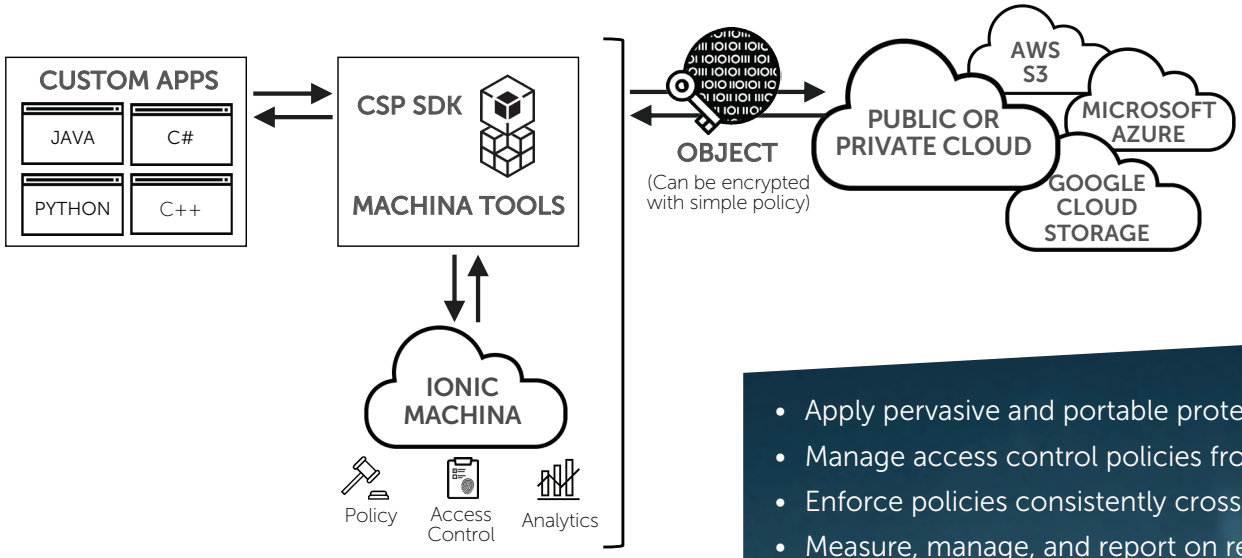
These capabilities can be applied to data stored in any of the three major public cloud storage providers or to data traversing cross-cloud and cross-storage boundaries. Application developers can now simplify management of data security and the complex access rules for each cloud provider, significantly reducing application development time and maintenance costs.

KEY SOLUTION CAPABILITIES

- Gain essential cross-cloud data security capabilities via a single platform (that extends to on-premises and hybrid storage), including policy management, data encryption, key management, and audit visibility
- Eliminate data security blind spots in your multi-cloud environment, due to lack of resources, expertise, or consistent vendor capabilities
- Automate incident response by applying data protection that's pervasive and portable
- Measure, manage and report on regulatory requirements and ensure compliant use of public cloud
- Optimize your existing public-cloud investments and reduce data exposure, vendor lock-in, or blind subpoena risks

TECHNICAL SPECIFICATIONS

- **Solution Requirements**
  - Cloud Storage Provider Account
  - AWS SDK for Java;
    Google Cloud Java Client for Storage;
    Microsoft Azure Storage SDK for Java
  - Ionic Machina license
  - Machina Tools for Amazon S3;
    Google Cloud Platform;
    Azure Blob Storage



- Apply pervasive and portable protection to data
- Manage access control policies from a single platform
- Enforce policies consistently cross-cloud
- Measure, manage, and report on regulatory requirements

CONSISTENT SECURITY ACROSS CLOUD STORAGE

CROSS-CLOUD DATA ENCRYPTION AT SCALE

- Add transparent encryption to the data stored in any of the top three public cloud storage providers (Amazon S3, Google Cloud Platform, and Azure Blob Storage)
- Apply fine-grained control and protection across documents, data objects, workloads, and more; One data element = One unique 256-bit key
- Hold complete control over the encryption keys in accordance with your enterprise policies
- Gain autonomous management of trillions of keys via owned, managed or hosted key servers, in any combination, at machine scale

CONSISTENT POLICY ENFORCEMENT ACROSS YOUR APPLICATIONS AND CLOUDS

- Easily integrate Ionic into your applications with minimal impact on existing code
- Reduce application development time to build and manage data security and complex access rules for each cloud provider
- Delegate data access logic to a central service that functions consistently across all three major cloud storage providers
- Gain audit-ready visibility into every data access attempt

IONIC

Ionic Machina secures sensitive data in today's borderless enterprise by providing:

- Advanced visibility, control, protection, & analytics
- Complete customer control of keys: autonomous management of trillions of keys via owned, managed, or hosted key servers, in any combination
- Fine-grained control & protection: entire documents, data objects, & individual database fields
- Audit-ready results: high-fidelity & high confidence, behavior tracking, reporting, & analytics
- Internet-scale: Globally available. Globally distributed. Globally resilient.
- One data element = One unique 256-bit key (no users or device keys)
- Templates: Ionic uses real-time policy vs. static policy templates used by others

MEASURE, MANAGE, AND REPORT ON COMPLIANCE REQUIREMENTS

- Eliminate data security blind spots in your multi-cloud environment by incorporating compliance requirements into just-in-time policies as you build varied applications
- Enforce those policies on data by applying data protection that is pervasive and portable
- Simplify authorized data access and manage unauthorized access in real time
- Confidently migrate data to public clouds with complete control and protection
- Reduce data exposure, vendor lock-in, and blind subpoena risks

ionic.com