What is Cryptix?

Innovative Data Assurance Platform

Cryptix makes implementing a trusted data sharing framework, easy and provides organisations with the ability to manage data that is shared beyond the enterprise securely.

The Cryptix framework maintains work flows, data storage and enterprise application investments, while protecting data across all communication channels including untrusted networks and devices.

Sensitive and confidential data is often shared inside and outside an organisation. When shared internally, majority of the data is secure based on enterprise related policies, but once data leaves the secure environment, data security and traceability is generally lost.

Data leakage risk exists for authorised and unauthorised recipients. Beyond the constant threat of hackers and malware, data containing proprietary and regulated information are often exposed to inadvertent emails, lost portable storage devices, unsanctioned application use and undocumented transfers of data.

The Cryptix framework provides organisations the ability to apply internal business rules to all data beyond the enterprise using strong encryption, broad usage of access controls, multifactor authentication, recipient activity audit tracking and even the ability to remotely delete distributed data.

More so, the Cryptix framework is so intuitive that it does not impact any existing business processes as it works with any line of business applications and multi-function devices.

Cryptix Functionality Set

Next Generation Data Sharing Platform

### **Overarching Security**

Cryptix provides industry standard AES-256 encryption, standards-based key management, secure key server, authentication modelling and object orientated storage. Importantly, by separating the access control keys at data level means that Cryptix doesn’t provide a data “honeypot” for hackers like other file sharing solutions like Dropbox, Box etc.

### **No More Passwords**

Most file sharing systems still rely on traditional User name and Password to access data stores. This approach to “secure” data management is not reliable and provides hackers and unauthorised parties easy access to data.

The Cyrptix framework is purpose built for assurance using a variety of authentication methods including, one time passwords delivered by email or SMS, voice comparators, location based access and virtual tokens.

Cryptix’s tokenised authentication provides organisations with the strongest two factor authentication access control solution on the planet.

### **Data Mapping**

From the framework, users have the ability to be able to map data based on location, data sensitivity and user authentication methods. This unique functionality gives organisations greater control outside the enterprise and ensures non-repudiation and assurance.

### **Data Level Security Controls and Classification**

Every organisation marks their data in a specific way based on importance. The Crytpix framework allows users to be able to use existing internal naming conventions such as Top Secret, Protected, Classified and Unclassified to ensure continuity and data integrity beyond the organisational enterprise.

### **Data Geo-fencing**

Data can be geo-fenced to a specific location based on importance. This feature provides organisations with the ability to lock down data so that it can only be viewed at a specific location. This functionality is designed to support mobile and work from home employees.

### **Data Lifecycle**

Organisations generally have business rules associated with regard data lifecycle, Cryptix continues the lifecycle beyond the domain by providing organisations with automated disposition and destruction options. Cryptix never persists data.

### **Flexibility**

Cryptix works with any browser, popular devices, file storage and enterprise based content management systems like MS SharePoint, HP RM8 across all communication channels whether they are trusted, untrusted, private or public.

### **Intelligent**

Comprehensive auditing, delivery notifications and governance across the data usage lifecycle with the ability for organisations to be able to modify business rules associated with distributed data instantly.

### **Multi-Tier Architecture**

The Cryptix architecture is distributed across three servers and can be multi-tenanted across different locations if required for additional security or segmented to suit organisational requirements.

### **Easy Deployment**

Recipients do not have to have to download any software and can access related data via any browser or device. Cryptix has four different interfaces that can be deployed and include a Desktop Client, Dropzone, Batch Processor and Web Portal.

### **APIs**

Cryptix has developed a series of published APIs to allow developers and system integrators the ability to be able to interact with any enterprise line of business application, multi-function device or mobile application. Currently Crytpix supports MS SharePoint, Office365, HP RM8 and Windows out of the box.

# How Does Cryptix Work?

## Innovative, Seamless, Scalable

Through its robust architecture, Cryptix provides comprehensive data security that works throughout the data lifecycle and within an organisations existing data sharing infrastructure and enterprise applications. The framework not only employs strong encryption and multi-factor authentication functionality, but leverages Cryptix’s data mapping engine. Additionally, Cryptix makes data security easy to use and readily adoptable by employees, suppliers, partners and customers with limited change management.

Create + Business Rules

Information workers can set business rules based on the data type and sensitivity manually by the data owner or automatically in accordance with internal organisational policies. Interaction with the desktop and line of business applications makes creating secure wrappers seamless to the end user.

Encrypt + Send + Notify

Cryptix encrypts the secure wrapper locally, with the associated business rules encapsulated as a secure object. The Cryptix notification server generates a link to the intended recipient/s and is delivered to the recipient via email or SMS.

The creator receives an email notification that the secure wrapper was created and distributed. This notification can be added to a workflow or business process as confirmation that information has been sent.

Store + Control

Cryptix stores the created secure objects as individual encapsulated files and controls access to the objects through the associated business rules and pre-set access control permissions. All file access and usage is logged and available to the creator owner and the enterprise through the desktop client or web based administration interface.

Access + Assurance

Only valid recipients can access a secure object based on the pre-set assurance levels associated with the secure object.

If an unauthorised recipient tries to open the object, Cryptix will deny decryption and log the illicit attempt details. The creator can also dynamically modify recipients and permissions, and can do so directly.

A creator at any stage may change or revoke all permissions and block any decryption attempts.

**Need to design a diagram**

# Why Use Cryptix?

## Data Security Beyond the Firewall

Organisations face the ongoing challenge of protecting sensitive data outside the corporate enterprise. Even with significant capital investments in enterprise security applications, organisations still lose sensitive data regularly. Unfortunately, data leakage is amplified due to the proliferation of mobile devices, personal e-mail usage in the workplace and unsanctioned file sharing services that are outside an organisation’s IT management.

Cryptix delivers the next generation data security framework that provides organisations with an easy, comprehensive rules based engine and assurance controls to protect sensitive data outside the corporate network. Cryptix is the “next generation” data drop box that not only assists to mitigate risk for data in transit and at rest, but incorporates assurance levels through human interaction and location based boundaries.

### **Staff Need the Ability to Share Data Securely**

Cryptix’s strong file encryption, business rules engine and assurance controls is set locally prior to sending. These actions allow data security to be enforced after the file leaves the users enterprise and in accordance with corporate policy relating to information sharing. Importantly, this protection persists beyond the domain while closing data leakage gaps.

### **Easy Deployment**

To ensure limited change management, recipients do not have to have to download any software and can access related data via any browser or device.

Cryptix has four different interfaces that can be deployed and include a Desktop Client, Dropzone, Batch Processor and Web Portal file within the corporate perimeter.

### **Extend the Value of Existing Enterprise Applications**

External cloud-based data storage and collaboration services like Dropbox, are presumed to offer strong file security and tracking since the data is managed within cloud and application folders. This low-level security approach creates a “honeypot” of data for unauthorised access by whoever controls the access keys, in most cases these products use User Name and Password as the entry pass-phrase.

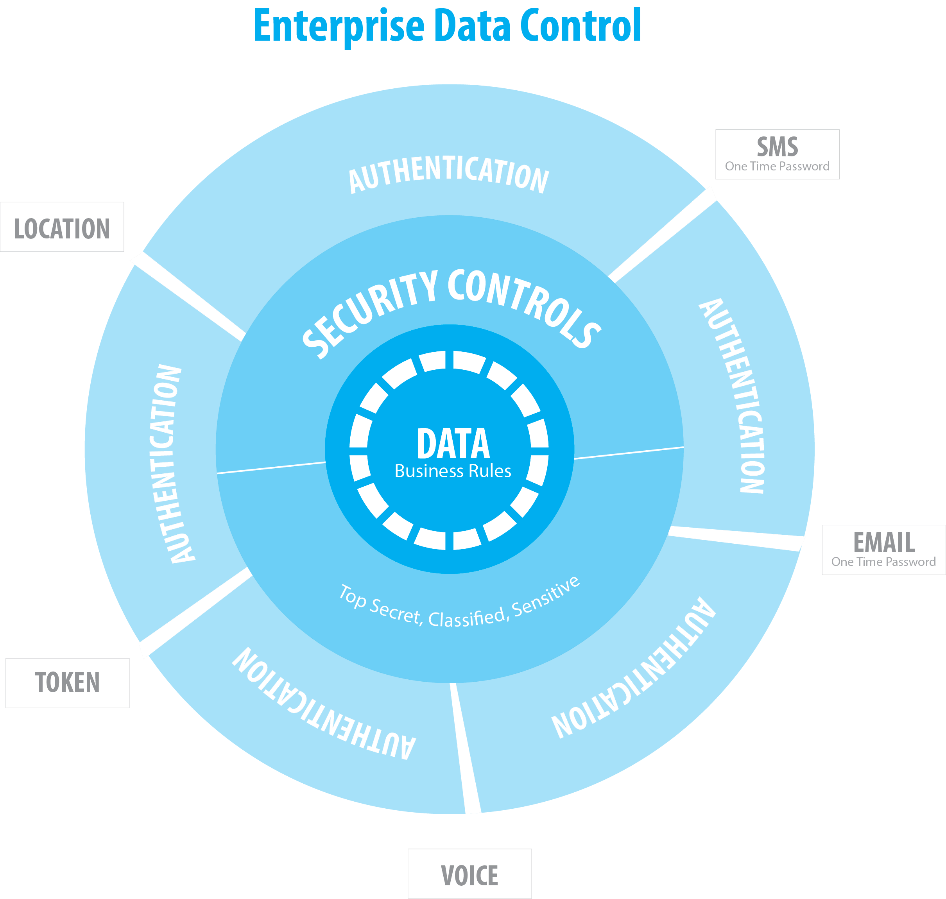
Cryptix’s Dropzone extends the value in existing IT investments in enterprise applications like information management systems, ERP, HR and others by simply interacting at the desktop using drag and drop functionality. This approach also limits the amount of change management required to train staff as most users are already familiar with these core systems.

### **Simplified Data Security to Reduce Risk**

Most employees understand and want to protect sensitive information. The key is to make data security easy, intuitive and aligned to corporate policy – and Cryptix does just that.

The Cryptix framework makes it easy for data owners to encrypt, specify data access and assurance permissions directly or in accordance with pre-set corporate policy. It provides strong protection without requiring the user to remember multiple passwords or for IT Departments to be burdened with the ongoing task of managing a multitude of keys.

Cryptix’s strict business rules and assurance approach maintains users work flows and processes while protecting data across untrusted networks and devices.



# Cryptix Deployment Flexibility

Cryptix has been designed with security in mind and it’s three tier server architecture allows organisations the choice to select what deployment option best suits the needs of their organisation. Cryptix can even be segmented across three locations if so desired for additional security if so desired.

Cryptix offers three types of deployments including;

* on premise private cloud – three server tiers are deployed internal to the organisation
* a hybrid cloud architecture – key management server deployed internally and one or two other server tiers are hosted external to the organisation
* a hosted/ managed cloud service – fully outsourced deployment where all three server tiers are managed outside the organisation

### **On-Premise**

On-premise deployment of Cryptix creates a private cloud environment and allows organisations to have full control and oversight of security, privacy and compliance.

The Cryptix on premise private cloud provides organisations;

* all the productivity benefits of the cloud
* greater security as Cryptix sits behind the organisations firewall
* the ability to be able to manage the access control keys – leaving the organisation in control of its own data
* simpler administrative management and no need for third parties to be engaged

Cryptix server software is currently available for Windows Operating Systems.

**Need to design a diagram**

**Hybrid Cloud Model**

The Cryptix Hybrid Cloud deployment is a mixture of both a private cloud and public cloud infrastructure. This approach allows an organisation to manage the access control keys, whilst taking advantage of lower cost external storage options.

The Cryptix Hybrid Cloud infrastructure;

* is fully compatible with any public cloud service
* provides multi-tier deployment options
* allows for systems to be easily scaled

**Need to design a diagram**

### **Hosted Cloud, Managed Service**

Cryptix offers organisations a fully hosted cloud based managed service. It is aimed at small businesses that do not have the IT infrastructure or staff to be able to manage and support Cryptix, but wish to take advantage of all the benefits that Cryptix has to offer.

Deployment can take as little as four hours to commission and the access portal and notification infrastructure can be personalised to an organisations brand without the need to deploy any software.

This flexible and low cost deployment option provides small business with a secure collaboration framework, whilst ensuring data security and compliance with all Australian legislative and regulatory laws.

**Need to design a diagram**

# Case Studies

# Financial Services

## Innovation for a Highly Regulated Environment

As hackers become more sophisticated and online fraud increases, financial services institutions are increasingly challenged to keep customer data safe. As consumers and remote staff increasingly use personal mobile and storage devices, they also introduce unauthorised disclosure risks.

Evolving Australian and International regulated data protection specifications, such as The Privacy Amendments Act, PCI-DSS, APRA regulations and others require due care with the handling of personal identifiable information (PII) and financial information.

Consumers more than ever now play an active role in managing their own finances, they also need the assurance that their privacy and sensitive information is protected.

How can you guarantee only authorised users access shared data and at the same time, ensure that access to the data is assured?

### **Cryptix Solution**

Cryptix provides financial services organisations with added security for data shared with credit and payment processing partners, parties conducting sensitive business transactions, and documents shared with customers. Whether accessing customer credit reports, personal finance reports and authorisations, corporate loan information or profit and loss statements, data security controls remain active and can be easily updated as organisational policies change.

* Share sensitive information with third parties with confidence.
* Keep sensitive data secure at all times with pre-defined usage assurance settings.
* Reduce the risk of data theft with embedded strong file encryption and multifactor authentication.
* Supports industry and government regulations
* Reduce security breaches and negate public breach notification by ensuring data is secure at an object based level
* Low total cost of ownership as the Cryptix seamlessly interacts with the enterprise and is easily implemented.

Object level data security can be simple and seamless when you have complete and flexible control. Cryptix makes it all possible so you can keep your customers’ hard-earned trust and preserve your reputation.

# Government – Federal, State and Local

## Compliance for a Highly Legislative Environment

Federal, state and local governments are now under pressure to be more efficient and to collaborate more than ever. From citizen, defence and intelligence departments to state and local agencies, government institutions strive to provide cost-effective and efficient public services. This often means sharing sensitive information between agencies and law enforcement authorities quickly and securely – all while complying with standards and legislation.

State and local government agencies often need to protect bids, projects and other sensitive information they collaborate on, to deliver their essential services to constituents, critical data must be shared securely with suppliers and subcontractors and remain protected even after they’ve reached their intended destination.

In a world where these agencies face daily attacks and experience data breaches, how can local, state and Federal government agencies protect and share sensitive data quickly and reliably without compromising intelligence and privacy?

### **Cryptix Solution**

Cryptix protects data containing classified, restricted and confidential information by providing secure access and usage control that remains active no matter where the data is stored and delivered. The Cryptix technology simplifies data collaboration, by setting assurance permissions based on internal policy when a secure wrapper is created whilst maintaining protection through the entire lifecycle. Only appropriate users can access, download, print data based on agency security requirements.

As a leader in assurance and location based data sharing, our framework offers enterprise-class security and performance required by federal, state and local agencies and their contractors. From transferring data inter-agency to sharing data across untrusted private and public networks, Cryptix offers persistent security and comprehensive auditing across the data lifecycle and in accordance with statutory obligations.

* Increase productivity with secure file sharing and collaboration with contractors and suppliers. that enforces policy in the applications they are accustomed to.
* Align information sharing compliance between teams, agencies and departments according to policy and need-to-know.
* Collaborate seamlessly between departments, outside agencies, private sector or international partners through expedited provisioning and dynamic controls.
* Get enterprise-class file security functionalities covering access, usage and audit; designate who can access and for how long.
* Stay in control: set and change file security parameters even after files are distributed. Delete files automatically based on duration, user, use and authorized access attempt.
* Reduce the available attack surface of files from hackers and malware.
* Prevent data leaks and sharing violations across users, networks and devices.

Collaborate seamlessly but securely on planning, inspections, public project bids, missions and initiatives, policy sharing, public safety, finance and taxation, welfare benefits, HHS and case management files. Cryptix allows your agency to leverage your existing storage, distribution, collaboration and end user applications, and with the option of an on premise or SaaS implementation, IT departments can readily implement Cryptix for internal and external use.

# Healthcare

## Treating Patient Data with Care

Technology is quickly changing the way patient, medical and clinical data is accessed in order to be responsive to patient needs. Currently, most healthcare providers use email or fax to distribute sensitive patient data, or patient files that are too large they use file sharing platforms like Dropbox, which are all insecure, as none can guarantee assurance. By using any of these methods healthcare providers are putting patient’s personal health data at risk.

### **Cryptix Solution**

Whether in an expansive healthcare institution, across a large hospital network, for use within a chain of labs or clinics, within a medical practice, or with patient claims and billing processing partners, patient data stays secure from the moment it leaves your environment. The Cryptix framework has been specifically designed to incorporate data level security and assurance level access, to protect patient data in transit and at rest.

* Improve patient and resident trust with robust data security.
* Keep sensitive data protected across multiple users and devices.
* Collaborate quickly between hospitals, specialists, GPs and labs while meeting strict compliance standards.
* Integrate persistent data security seamlessly into existing clinical workflows and processes.
* Support industry standards by assuring data access security and the privacy of healthcare and financial records internally and amongst third-party patient processing providers.
* Expand your data security coverage to include clinicians, researchers and other personnel outside your organisation.
* Supports legislative requirements for the handling and access of patient data (Australian Health Records Act, Privacy Act) to ensure data privacy.

# Professional Services

## Assured Data Access

Professional service providers work in a highly connected world where sharing data and collaborating online is the norm.

Consultants, recruiters, accountants, media, creative, IT and other service providers routinely access and share sensitive information to meet client needs.

Without proper data protection and auditing controls, business agreements, legal and financial documents, analytics, human resources, audits, employee information, personal identifiable information, health records, tax and other critical files are open to unauthorised access and misuse – putting sensitive and confidential information and the business relationship at risk.

### **Cryptix Solution**

Cryptix assists professional service providers protect company, client and third-party information at all times. It controls and monitors data access and usage activity from the moment sensitive data is shared.

Authorised recipients, outside the organisation, can access data containing sensitive, regulated or confidential information they way they are accustomed to, but with comprehensive business rules intact.

* Enhance information security with robust persistent file encryption and usage control.
* Securely share, review, edit, print, and forward business critical and privacy-sensitive files across public or private networks, collaboration platforms and popular devices.
* Secure client information to reduce liabilities associated with confidential data leakage.
* Protect use of files and respective collaboration with your organization and among clients.
* Track and audit file access and usage, as well as unauthorized access attempts across customers and partners.
* Protect your firm’s reputation with solid file encryption, persistent usage control and extensive audit log of file activity.

# Education - Governance

## Secure Data Sharing for Good Governance

As the governance body of a school, school councils deal with a variety of sensitive information and correspondence that contains policy based views, student and parent complaints, financial and budget matters, welfare management, teacher and administration management, building works and projects, departmental level communications, supplier liaisons and interactions to name a few.

Generally, email or unsecured file sharing applications like Dropbox are used as it is seen as the most convenient method of communication, but is open to interception, incorrect distribution, snooping and hacking.

School councils and councillors have a duty of care and fiduciary obligation to ensure that any communication internally or externally shared is secure in transit and at rest to protect the integrity of the school council.

How does Cryptix solve the problem?

### **Cryptix Solution**

Cryptix provides a better alternative to email or unsecure file sharing services. It is simple to use, doesn’t require software to be downloaded or registered, works on any web browser or device and importantly ensures that all communications between councillors and third parties is protected at all times. Additionally, Cryptix ensures that school councils comply with all State and Federal legislative requirements including Privacy and Records Acts.

* Easily deployed
* Share and collaborate safely with school council members and other 3rd parties
* Works on any computer or mobile device
* No password or email management required
* Extend the value of Cryptix to parents, teachers and students, bringing the classroom to the lounge room to provide better student outcomes
* Keep school community financial information safe with end-to-end file encryption

# Education

## Secure Portal for Information Sharing

How does Cryptix solve the problem?

### **Cryptix Solution**

Cryptix provides a better alternative

Privacy & Compliance

Cryptix allows recipients to be able to access sensitive data and meeting your regulatory obligations by applying assurance at object (data) level.

* Data is encrypted so that only the people that are authorised can access your data; not system administrators, service providers or cloud companies
* Store critical data securely on premise on your own server, giving you complete control and visibility over your data and who accesses it
* Easily set permissions to control who can access, view, download your data
* Share data using secure, multifactor-protected links and activity logging
* Enable productivity gains that come from accessing information on any device without compromising security, compliance and privacy obligations
* Ensure compliance with privacy and other regulations to meet PCI DSS, Legislation and ISO 27001 requirements

Encryption

Cryptix provides industry-grade, end-to-end encryption. Data is encrypted at rest on the server and in transit. Only you have the keys to your data, preventing unauthorised access - even to system administrators, IT service providers or other 3rd parties.

How do we do this?

* Data is secured at all stages using 256-bit AES encryption. By making your data almost theoretically impossible to read without the encryption keys in case of a data breach.
* All files stored on Cryptix servers are automatically encrypted at object level using ensuring sensitive data is protected when not in use
* Data is transferred using a hardened SSL/TLS secure tunnel to protect data in transit
* Set and manage your own encryption keys removing the need to leave the most important security element in the hands of another service provider or 3rd party

Data Sovereignty

When you upload your data to public cloud services, where is it actually stored? Your data could be on a server in Australia, or it could be hosted offshore. With Cryptix you know exactly where your data is - critical when storage of sensitive data needs to comply with local data sovereignty laws and other regulations

* Store your data exactly where you want to store it.
* Multi-server and multi-site friendly, deploy multiple servers, mix on premise and cloud storage and access your data from anywhere on any device
* Mix and match on premise storage with other solutions. Use on premise storage for your most sensitive data and leverage low-cost cloud storage for less critical information.
* Share your data directly from your own on premise or private cloud storage without ever touching the public cloud. Cryptix gives you the tools to share data directly from your own infrastructure without ever needing to trust third party providers

Full Visibility & Access Control

Through the Management Console, Cryptix gives you full control and visibility over who has accessed data.

* Gain clear visibility of who accessed and shared files, when and who files were shared with and from which devices they were accessed.
* Detailed user login history enables administrators to see when a user last logged in, their location and from what device. Detect patterns of unusual behaviour to stop potential breaches before they happen.
* Active Directory and SSO compatible through LDAP. Sync your users and groups from Active Directory and grant user permissions based on your existing corporate structure.
* Assign user access to drives and root-level folders either directly or using groups
* Grant administrator access to users in important roles to assist with managing the system
* Securely share files with external suppliers or contractors through authenticated links, ensuring that only the intended recipients can access your data
* Easily erase files from desktop clients and cached mobile app data with ‘one click’ remote wipe. Wipe every device a user has used and instantly lock their account to prevent future access or sharing.