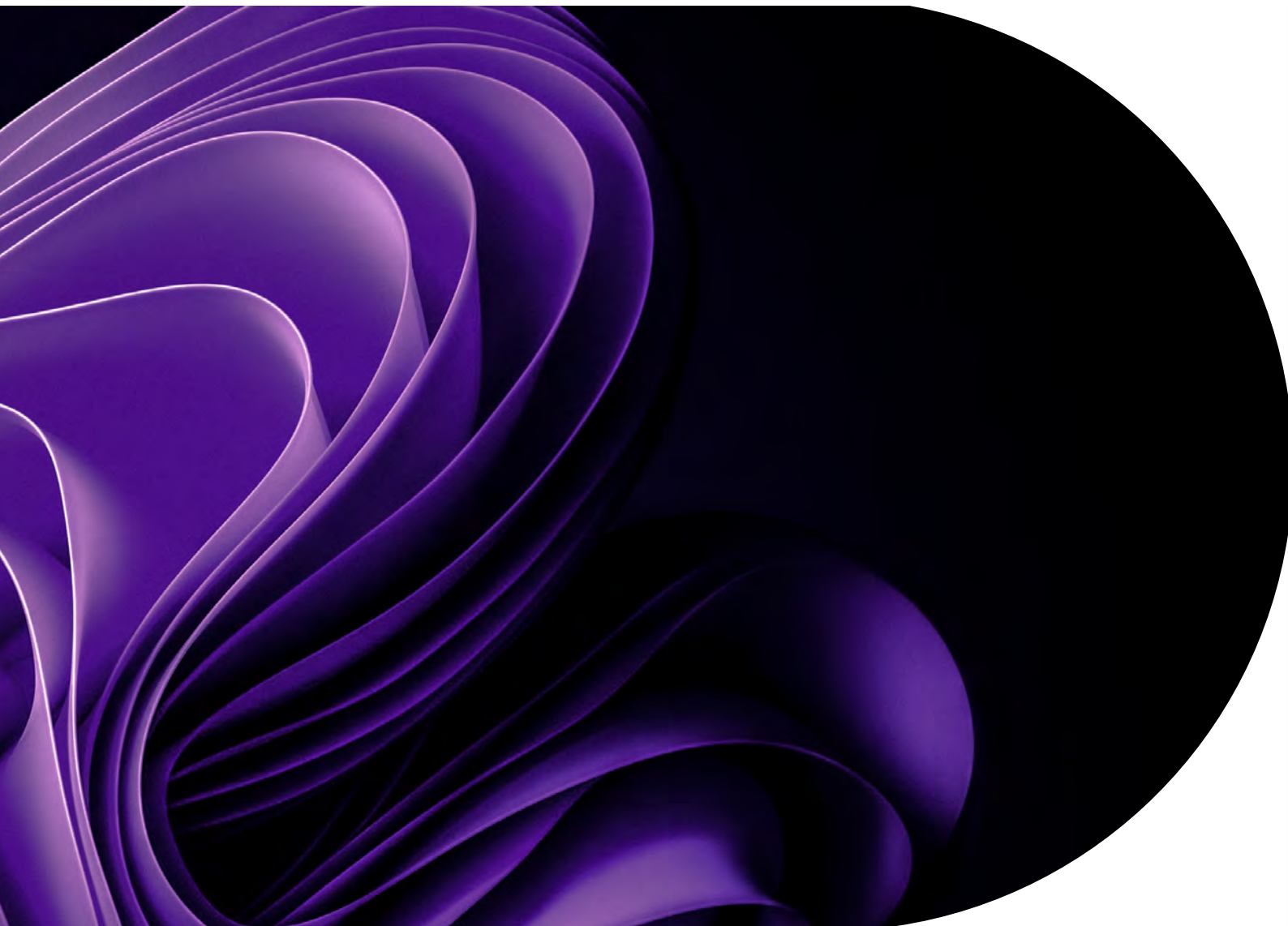




ENTERPRISE | COCOONCUSTOMCLOUD

Cyber-safe,
compliant
collaboration.



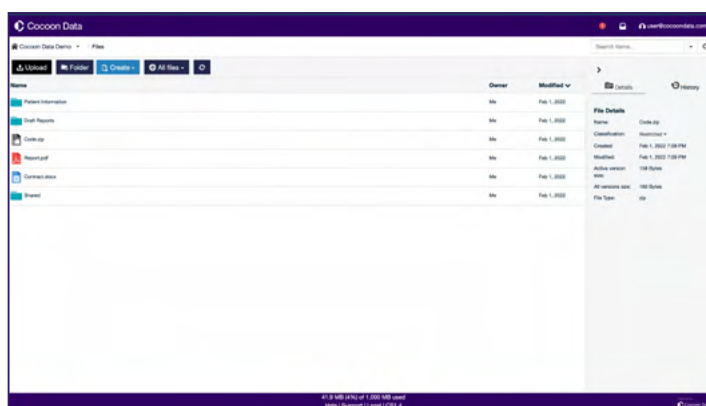
The explosion of Cloud software and organizational digitization has provided pathways for connectivity and engagement never seen.



At Cocoon Data, we help organizations store and transfer data outside their organizational firewalls safely and compliantly. Our technology is cloud-agnostic, to work across existing cloud infrastructure, people, and processes to help businesses store and transfer regulated and commercially sensitive data.

Conceived for the Military and the intelligence communities, this solution is a world-class ultra-secure file sharing and collaboration solution. Our cloud-based platform supports teams within Government, Healthcare, Finance and Defense who share data under the world's most stringent compliance environments.

Today, we are one of the preferred providers in the US for helping meet compliance solutions in the US Defense Supply Chain.



Cocoon Data's highly secure portal



Cocoon Custom Cloud

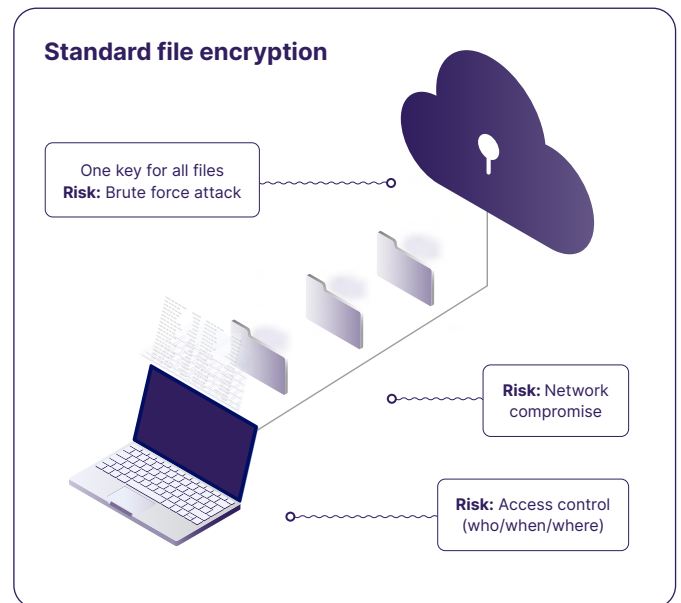
Our security and encryption applications are enabled across customer's private, on-premises data centers or IaaS providers:



What makes Cocoon Data unique?

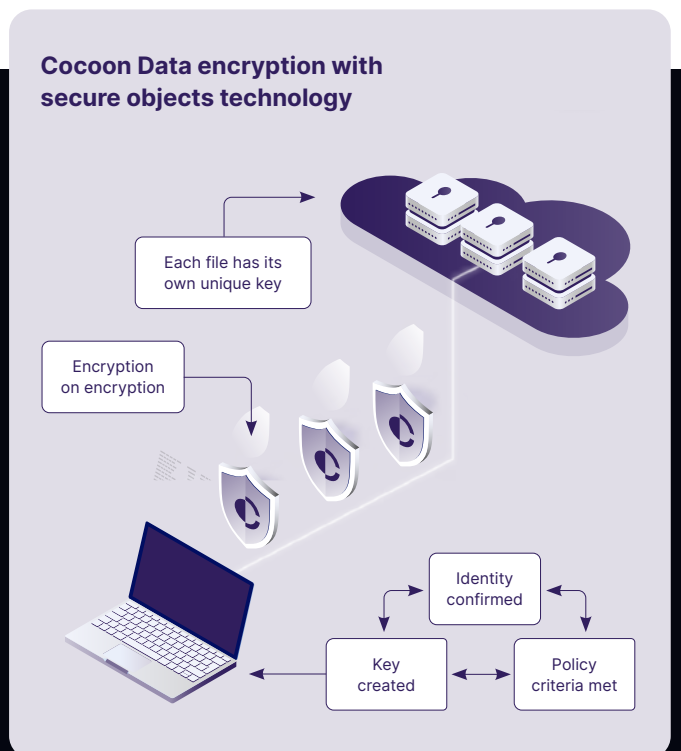
Cocoon Data's encryption is unmatched – where Microsoft O365, SharePoint and similar products stop at the firewall for policy, key management and identity based access to sensitive and encrypted content, Cocoon Data's offering takes over.

Our 'Secure Objects Technology' platform uses three key principles to afford unrivaled security and compliance – identity, policy, and unique encryption keys.



How Cocoon Data works:

- ① Encryption is initiated when we allocate a unique key to the user's file, encrypting files before they depart the device to the cloud.
- ② The encrypted file is then linked to an identity, including the creator and recipient, ensuring only those identified can access the file through the key service.
- ③ Finally, our application embeds a policy condition to each-individual file, determining what conditions the file can be accessed by way of the encryption key release. For example, geolocation, time, edit or view, classification and many more.

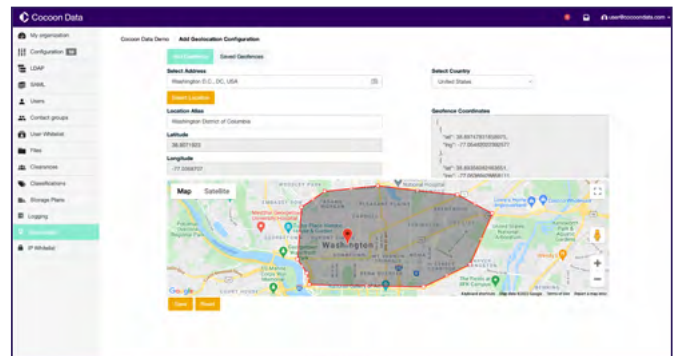


Choose between two Cocoon-configured applications:

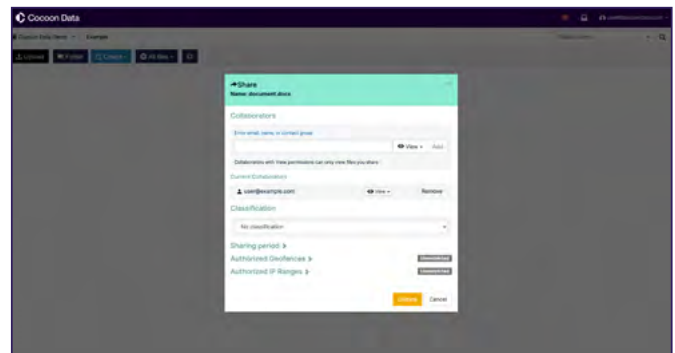
1 Cocoon Data file-sharing platform

Immediately deployable, ultra-secure, file-sharing and collaboration. This single-tenancy solution provides an expansive set of high-security features, including:

- Immediate SaaS provisioning in a country of choice for secure file-sharing and collaboration
- Geofencing functionality to protect and limit file access based on a user's latitude and longitude location
- Dynamic watermarking to discourage unauthorized downloads, sharing, screen capture and photography of a confidential file
- Two-factor authentication and reporting on usage and logging of all activities. Includes SAML or active directory integration.
- Time and location access for any device, with zero-trust facility
- Full audit trails down to the 'by file' level to track access and time
- 'Kill the key' to immediately switch access on and off to each unique key for each file
- Choice of data sovereignty control
- Integrated Microsoft Windows environment and secure data storage



Geofencing feature



Control how users access your files



2 Cocoon Custom Cloud application

Custom and configured to an organization's requirements, a Cocoon Custom Cloud enables our applications to be configured within a cloud-agnostic environment.

Designed for cyber-advanced enterprise and government departments, our security and encryption applications are enabled across clients' private, on-premises data centers or IaaS providers, including AWS, Microsoft, Google, IBM, and Oracle. If your cloud provider supports Kubernetes, we will most likely run on their infrastructure too.

We can tailor pricing for large deployments ranging from thousands of users to hundreds of thousands of users, exclusive of the IaaS cost base – a simple license within your cloud provider.

Furthermore, bespoke customization and functionality can be created to wrap-around organizational requirements, including corporate design, operating models, security protocols and tenancy demands.

Custom tenancies

Custom and unlimited tenant structures can be deployed to reflect and support specific organizational design, operating models, and security hierarchy and protocols. Each tenancy is configurable, allowing large organizations to delegate specific administration to departments or sections of the business for optimal governance and administration.

Key as a Service

Our Cocoon Custom Cloud is an API driven product. This means all the attributes of our secure-objects patented technology are available as an API Key as a Service (KaaS). This affords organizations access to our encryption technology and extensive API integration, enabling them to secure data in a way that's bespoke to infrastructure and security requirements. This is a revolution for IoT and edge computing. PKI/VPNs do not scale to the new paradigm of Web 3.0 or IoT landscapes – but our KaaS does.

Custom controls

Custom controls and policies can be determined to balance data governance with global and functional operating needs. Location-based access, classification structuring, intellectual property fences, and security configurations can be specified and enabled across multi-devices.

Compliance

Customized controls can also be aligned for industry-specific compliance, including CMMC, ITAR, ISO 27001, NAIC, FERPA and HIPAA.

Custom branding and support

Cocoon Custom Cloud allows businesses to create a company-branded platform with a custom URL. Dedicated account specialists are assigned to support the development and implementation of the Custom Cloud environment along with support on business updates and cyber hygiene reporting.

Find out more about Cocoon Data and how we can help your organization.



Book a consult now at info@cocoondata.com