SOLUTION BROCHURE

Entrust Cryptographic Security Platform

Agentless File Encryption for Unstructured Data

ENTRUST

SECURING A WORLD IN MOTION

Overview

Ensuring data security is a critical necessity for modern-day businesses. In the past, organizations protected their data from unauthorized access with agent-based file encryption solutions. Unfortunately, traditional agent-based solutions tend to slow performance by 5% to 40%. They are also difficult to manage and scale and may be incompatible with newer workloads and cloud services.

The Entrust Cryptographic Security Platform (CSP), deployed on premises, offers an innovative, agentless alternative to agent-based file-level protection with "set and forget" management to protect data on file servers, Network Attached Storage (NAS), and Storage Area Network (SAN). The platform secures data from threats without the cost and complexity of agent-based solutions and provides strong data confidentiality.

The solution's low latency and fast throughput architecture has minimal to no performance impact. Data on end devices can be accessed without requiring changes to existing applications.

Our solution ensures unstructured data is well protected against outages, attacks, and other forms of data compromise. The Cryptographic Security Platform provides a singular dashboard view of keys across on-prem, public cloud, and hybrid cloud environments, including information about ownership, environment, purpose, and critical system.

In addition, the solution combines the benefits of agentless file-level encryption with the secure key protection of Entrust nShield® HSMs, our hardware security modules.

This platform addresses the growing need for comprehensive cryptographic asset management in an increasingly complex digital landscape. By integrating these critical components, the Cryptographic Security Platform, deployed on premises, offers unparalleled security, compliance, and operational efficiency for organizations dealing with securing an increasing number of machine identities, protecting sensitive data, and navigating complex cryptographic requirements.

Benefits

Meet Regulatory Requirements for Data Privacy
A growing number of jurisdictional data privacy regulations make it difficult for businesses to store data where they want. With strict cross-border data privacy laws like the EU's General Data Protection Regulation (GDPR), the Schrems II ruling, and the CCPA/CPRA in the U.S., it's becoming increasingly difficult for companies to protect their data, remain compliant, and take advantage of the cloud.

> With the Entrust Cryptographic Security Platform, businesses can use the cloud storage providers of their choice, in the geographic locations and jurisdictions of their choice, to mitigate data transfer risk and address data sovereignty and compliance concerns.

Data can be distributed across different regions of a single cloud provider, across multiple cloud providers, or across a hybrid mix of on-premises storage and one or more cloud providers. Cyber audit and assurance firm UHY Advisors states, "This solution has the potential to lower cyber risks and compliance costs while maintaining compliance with the spirit of European and U.S. data protection regulations."

Ransomware Mitigation
While encryption offers strong protection, it alone may not suffice against sophisticated ransomware threats.

Our solution enhances resilience through its self-healing data capabilities and RAID-like reconstruction, automatically restoring compromised data without manual intervention.

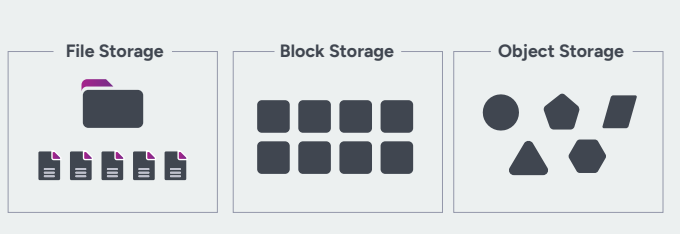
Continuous integrity checks detect unauthorized modifications – including cloud-based ransomware attacks – and promptly revert data to its secure state. This built-in data integrity ensures that critical data at rest remains protected and accessible at all times.

Prevent Unauthorized Access

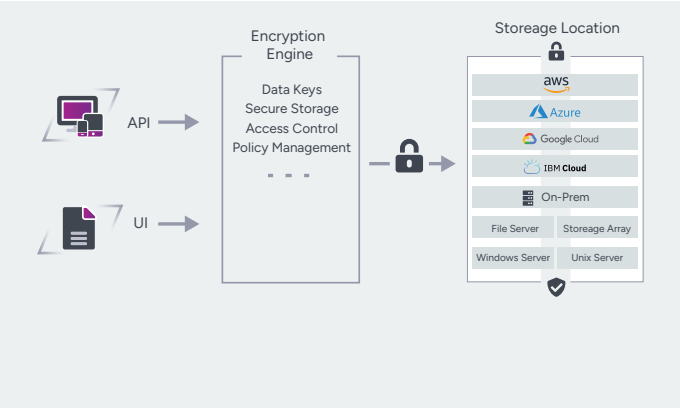
The solution offers advanced data protection – even when storage locations or file systems are misconfigured or are vulnerable to attack. The platform also separates storage admin and cloud provider access from data access to support privacy, confidentiality, and compliance.

In the unlikely scenario that a malicious actor gains access to every storage location for a given data set, that data still cannot be reconstructed, since the solution:

- Strips file content, filenames, file extensions, and all other metadata, meaning there is not enough identifying information for reassembly
- Allows organizations to add a configurable amount of poison data to their real data
- Makes the unauthorized reassembly of exfiltrated data impossible



The solution also requires multiple components to be used in concert for data reassembly, making it impossible for unauthorized users or attackers to reconstruct the data.



Simple Integration and Access

Despite its powerful data security and privacy features, our agentless file-level encryption solution has minimal impact on existing applications and operations teams, delivering instant data access with just a few clicks.

Equipped with a vendor-agnostic tool that works in the background as a zero-downtime event, our platform appears and behaves like traditional storage to applications, requiring minimal code changes to get started.

Since CSP is also transparent, user workflows are not impacted. There are no visible changes to employee interfaces, and retraining employees or redesigning applications is unnecessary. This allows for seamless integration with existing operations.

High Performance

Introducing privacy and security almost always brings a performance cost. CSP is a notable exception. By reading and writing in parallel and compressing pointers, the platform achieves high throughput and low latency.

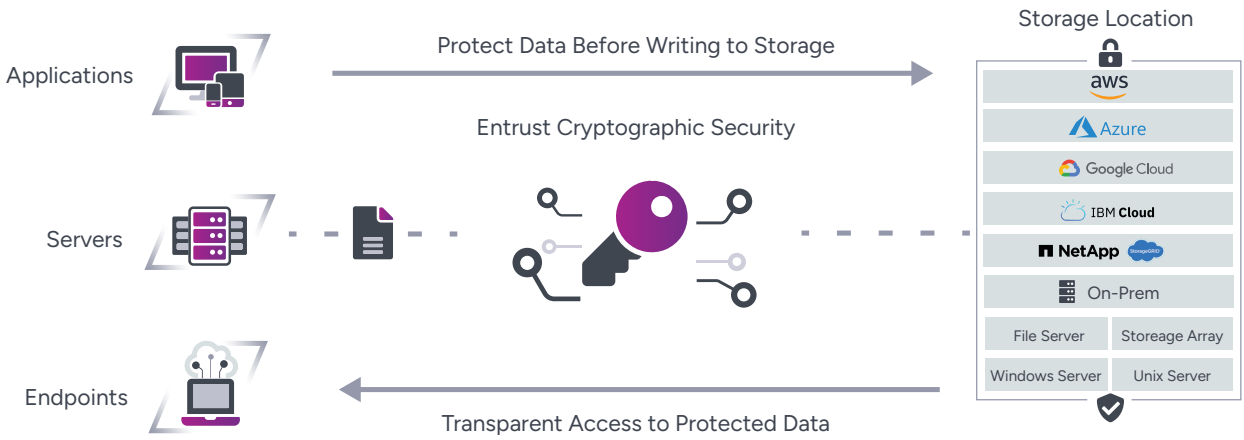
Additional Use Cases

Beyond the benefits listed above, the Cryptographic Security Platform:

- Protects sensitive files so teams can collaborate safely and without losing functionality
- Integrates with existing cloud backup solutions to further protect backup data
- Accelerates cloud migration initiatives
- Supports secure cold storage migration from on-prem to the cloud

How It Works

The platform's abstraction layer sits between applications and storage infrastructure, where it performs advanced file protection. This approach allows for a simple plug-and-play implementation without changes to data flows.



The Entrust Cryptographic Security Platform uses agentless end-to-end encryption to maintain the security and privacy of unstructured data on prem, in the cloud, and in hybrid- and multi-cloud environments. The platform keeps data safe from unauthorized users, separating infrastructure administrators and cloud service provider access from sensitive data.

Technical Specifications

On-premises storage	• Local disk • NFS (Network File System) • Microsoft SMB shares
Cloud storage platform	• Amazon EFS and S3 • Microsoft Azure Object Storage • Google Cloud Storage • Backblaze B2 • Wasabi • Alibaba Cloud Object Storage
Additional interfaces	• FUSE (Filesystem in Userspace) • S3-Compatible API • iSCSI Protocol
Supported hypervisors and cloud platforms	• VMware ESXi 7.0 (HW version 17) • AWS • Microsoft Azure • Google Cloud Platform (GCP)
Certifications	• FIPS 140-3 Level 1 certified • FIPS 140-3 Level 3 certified using Entrust nShield HSM
Management and monitoring	• Centralized management with Web UI and REST API • Syslog integration for centralized logging • Real-time alerts and notifications for data integrity events • Compatible with leading SIEM solutions for enhanced security monitoring

Key Features

Secure unstructured data wherever it resides: on prem, in the cloud, or in hybrid- and multi-cloud architectures

Strong data privacy and security in a unified, multi-protocol platform across multiple cloud providers

Separate data owner from infrastructure owner and cloud provider

Agentless file-level protection

Self-healing data and ransomware mitigation

Easy integration with existing applications and data workflows

Highly available and scalable architecture

Support for hybrid-and multi-cloud environments

FIPS 140-3 Level 1 compliant key protection

FIPS 140-3 Level 3 compliant key protection using Entrust nShield HSMs

Cryptographic Security Platform Components and Capabilities

Entrust's Cryptographic Security Platform is an innovative solution that unifies cryptographic management by combining the rich capabilities to operate PKI, Certificate Lifecycle Management, Key and Secrets Management, and HSMs all from a single, cohesive system.

This platform addresses the growing need for comprehensive cryptographic asset management in an increasingly complex digital landscape. By integrating these critical components, the Cryptographic Security Platform offers unparalleled security, compliance, and operational efficiency for organizations dealing with securing an increasing number of machine identities, protecting sensitive data and navigating complex cryptographic requirements.

For more details, download the Entrust CSP Solution Brochure

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION