CYBERCRYPT D1

CYBERCRYPT.

Seamless Data Protection in the Application Layer

It can start with a **zero-day exploit**, an **unpatched system**, a **human configuration error**, or a malicious insider. The next step is often a data breach or even a double/triple extortion ransomware attack.

To cope with today's threat picture, on top of encryption at rest and in transit, it is necessary to introduce additional protection of data at the application layer.

CYBERCRYPT D1 is an **application-layer encryption** microservice for cloud workloads. Its uniqueness is rooted in the seamless combination of:

(1) **explicit authorization** of each data point access using OAuth2.0,

(2) **individual key management** for each individual data point, and

(3) **cryptographic enforcement** of every access to a data point.

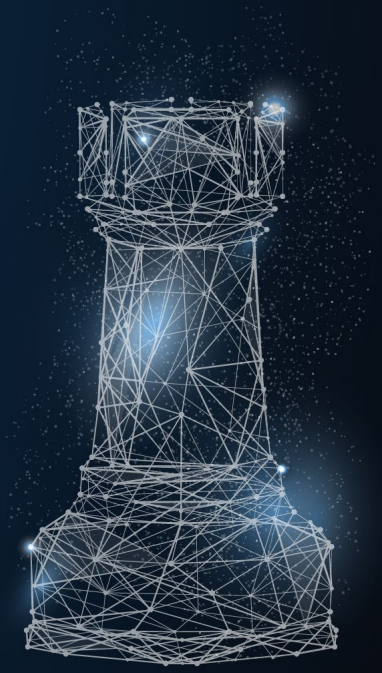
Databases: Integrations with SQL Server, MySQL, PostgreSQL, Cosmos DB, Azure Blob Storage, AWS S3, Google Cloud Storage, etc, as well as specialized SDK in various languages such as Go and C#.

IAM: Integrations with Auth2.0/OIDC, incl. Azure AD, AWS IAM, GCP IAM, Keycloak, and others, as well as claim-based authorization flows.

Automation: Available as a distroless-based Docker container that is easy to deploy into Kubernetes clusters or similar configurations. R eady-made Helm charts and deployment scripts.

Encryption: FIPS-compliant cryptography, quantum-resistant cryptography, and searchable encryption.

Key management: Integrations with AWS KMS, Azure KMS, GCP KMS, HashiCorp, HSMs, KMIP, etc.



D1

Zero Trust Data (ZTD)

Following **Chase Cunningham** of **Forrester**, we call our data- and identity-centric security framework Zero Trust Data (ZTD), which is the foremost part of the broader Zero Trust eXtended paradigm (ZTX). Here, one assumes a **"never trust, always verify"** mindset.

The controls of ZTD need to be tightly integrated with data in workloads and applications, with users' identities, with automation and orchestration, as well as with visibility and analytics tools.

CYBERCRYPT D1 packages the ZTD controls and makes them easy to use.

Three tenets of ZTD

1. Explicitly verify: Make the decision to grant access to data as late as possible.

2. Limit access and scope: Only grant access to data that is needed for the particular request within the particular access scope.

3. Assume breach: Minimize the "blast radius" in case of a breach.