DATABASE SECURITY PLATFORM

Enterprise-grade data security platform helps organizations control users and protect critical data at rest, in transit, and in use while facilitating regulatory compliance.

Overview

Entrust addresses the increasing threats and complex challenges related to protecting sensitive data. As a trusted advisor with leading expertise in data protection, key management, identity, and certificate solutions, Entrust offers an enterprise-grade database security platform to ensure data is always protected and readily available to only users, devices, and applications with authorized access.

Rendering data unusable to anyone or anything else, even if perimeter defenses fail, the platform enables encryption through scalable cryptographic key management to facilitate compliance with increasingly stringent government and industry security regulations.

Entrust is securing a world in motion – one where data is increasingly fueling competitiveness. No matter the use case, the Entrust Database Security Platform keeps sensitive data safe and organizations moving forward and compliant.

The Challenge

The rapid enterprise adoption of distributed and cloud-based deployments introduces new threat vectors that put sensitive data at risk. Unlike other cybersecurity areas, database security is unique, because a breach can often result in significant fines, not to mention bad press, and impact on reputation. Regulations including GDPR, PCI DSS, HIPAA and others are driving the need to encrypt all databases.

Protecting sensitive data is critical for maintaining competitiveness. Organizations need to safeguard intellectual property (IP) and commercially sensitive data, as well as customer personable identifiable information (PII) and financial data. The challenges organizations face as they deploy growing numbers of databases across distributed environments include:

- Maintaining consistent policies governing how data is protected across on-premises and cloud-based deployments
- Managing the high volume of encryption keys that secures the data
- Providing hardened protection for all critical cryptographic keys throughout their lifecycle
- Ensuring that employee errors do not lead to security misconfigurations that may expose sensitive information

Learn more at entrust.com

Entrust Database Security Platform

The Entrust Difference

Entrust combines strong human and machine identity management capabilities with robust protection of underpinning signing and encryption keys to prevent the unauthorized access to, and loss of, sensitive data. Entrust database security products interoperate with leading database vendors to centrally manage encryption keys, reduce complexity, and facilitate compliance with security regulations.Our solutions address enterprise database security requirements, from managing who and what has access to the data, to protecting the data at rest, in motion, and in use. The platform encompasses a range of encryption approaches that allow the customer to choose the point where cryptography is introduced (i.e., at the image, the full database (TDE), the field, or the enterprise boundary level). Unlike competing solutions that only focus on access controls, encryption, or key management, Entrust provides customers a range of security capabilities paired with professional services to help customers through their data protection journey, simplify the implementation and maintenance strategy, and ease procurement.

The Solution

Entrust offers a comprehensive and unified database security platform that ensures critical data is always secured from external and internal threats, and available for uninterrupted business. Backed by a certified root of trust protecting the underpinning cryptographic keys, the platform provides the flexibility organizations need to speed up processes, helping them mitigate risks and facilitate compliance. The Entrust database security platform delivers:

- High assurance, integrated protection of the keys underpinning the transparent data encryption capability from popular database vendors (IBM, Microsoft, MongoDB, Oracle)
- A FIPS 140-2 Level 3 root of trust using certified nShield on premises or as a service hardware security modules (HSMs)
- Lifecycle management and protection of database encryption keys from a growing list of database vendors that support the Key Management Interoperability Protocol (KMIP), whether cloud-based or on-premises (Bloombase, Cohesity, IBM, Microsoft, MongoDB, NetApp, Nutanix, Oracle Quantum, Red Hat, Rubrik, VMware)
- A cloud key management server that supports bring your own key (BYOK) to protect databases housed by major cloud service providers
- Full encryption of the virtual machines running sensitive databases
- Cloud-based identity and access management with multi-factor authentication, credential-based password-less access, and single sign-on
- Certificate solutions that control and automate the management of user and device certificates in a single portal
- Credential issuance with a public key infrastructure (PKI) capability that helps limit database access to only authorized users and devices
- A tokenization server that pseudonymizes sensitive data and preserves its format for seamless use by applications

Benefits

- Address range of database security requirements and approaches all from a single vendor
- Deliver certified encryption and key management to enforce best practices/standards of due care
- Enforce separation of duties isolating master keys from encrypted data, reducing insider attacks
- Keep encryption keys readily available to ensure optimum database and application performance
- Ensure that users and devices have necessary authentication credentials to access databases
- Streamline the management of user and device certificates
- Simplify authentication, authorization, risk policy decisions
- Align with data protection regulations and industry mandates
- Facilitate auditing and reporting for compliance obligations

Learn more at entrust.com

Entrust Database Security Platform

Entrust Products Supporting the Database Security Platform

KeyControl integrates with leading database vendors to deliver enhanced database protection with centralized, automated cryptographic key management. Using KMIP, KeyControl establishes and enforces key use policies, and maintains keys separately from the database environment, providing stronger security and aligning with both data protection mandates and industry best practices.

KeyControl BYOK capability allows enterprises to generate, manage, and use their own encryption keys across cloud service providers, including AWS, Google Cloud Platform, and Microsoft Azure.

Tokenization Server enables protection of sensitive data while preserving format for easy deployment across restrictive database schemas.

DataControl delivers data encryption, multi-cloud key management, and workload security while enabling compliance with data privacy regulations.

nShield HSM and **nShield as a Service** integrate with leading database vendors, providing a secure solution for generating and protecting TDE data encryption keys, within a FIPS 140-2 Level 3 certified environment.

Entrust Identity Enterprise and **Identity as a Service** delivers cloud-based identity and access management with multi-factor authentication, credential-based password-less access, and single sign-on.

Entrust PKI establishes and maintains a trustworthy networking environment by providing key and certificate management services (on-premises or managed as a service) that enable encryption and digital signature capabilities across a wide set of applications.

Certificate Hub enables customers to find, control, and automate the management of the device and user digital certificates that help ensure only authorized access to databases.

Professional Services help customers operate and maintain Entrust database security solutions effectively over time, enhance operational efficiency and meet compliance goals.

Entrust Database Security Solutions Integrate with Leading Database Providers

Google Microsoft IBM aws ORACLE mongoDB.

Learn more at entrust.com

Entrust Database Security Platform

Key Features

- Unified platform protects sensitive data
- Universal key management for KMIP-compatible databases
- Range of robust encryption approaches
- Strong user and device/application access controls
- Simplified implementation and deployment
- Entrust database security products interoperate with leading database vendors to centrally manage encryption keys to reduce complexity and facilitate compliance with security regulations
- Certified HSM root of trust can generate and protect underpinning keys used to sign and encrypt critical organizational data
- Entrust PKI establishes/maintains trustworthy environments with certificate management services for encryption and digital signing

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com **entrust.com/contact**