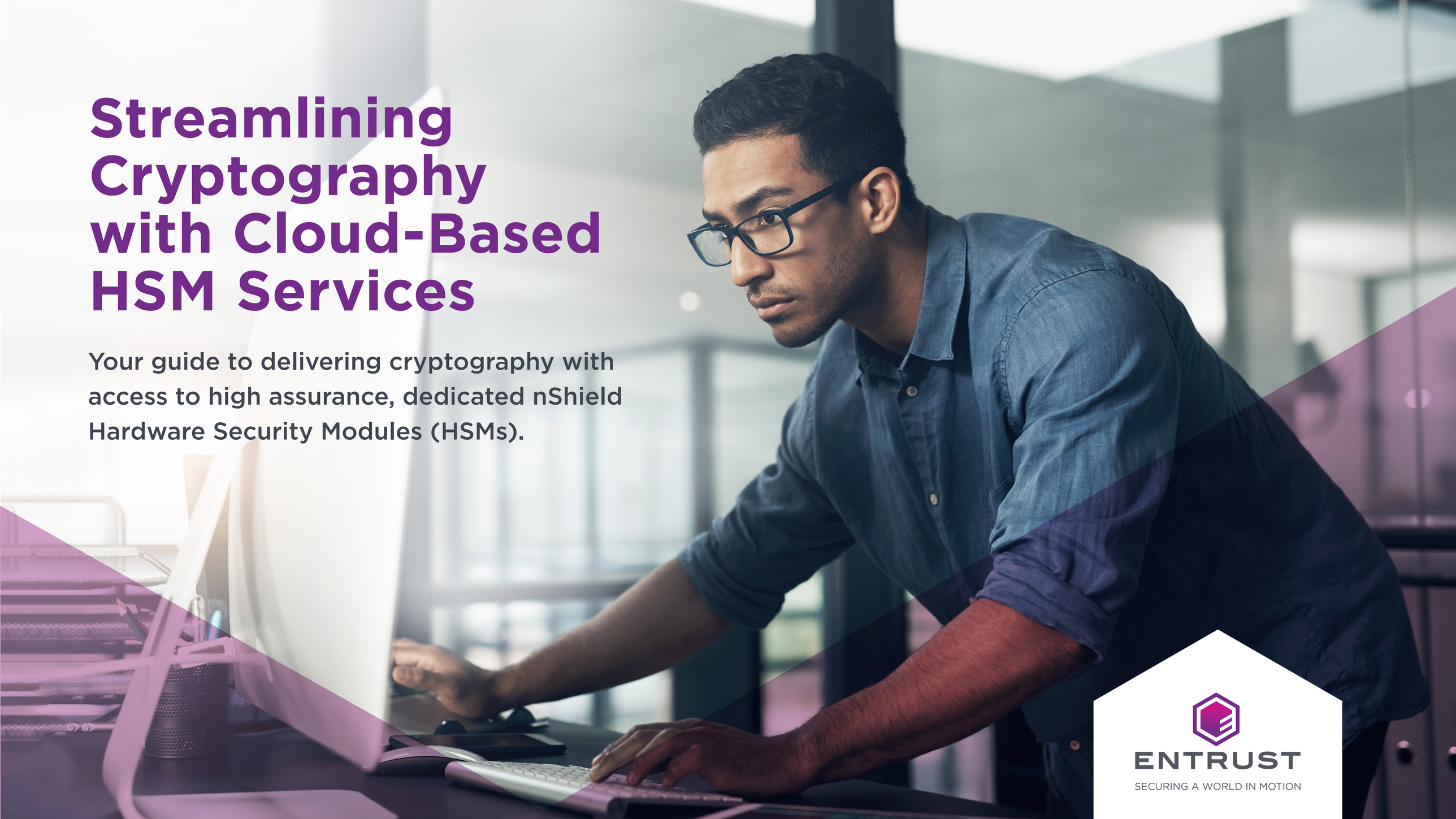
Streamlining Cryptography with Cloud-Based HSM Services

Your guide to delivering cryptography with access to high assurance, dedicated nShield Hardware Security Modules (HSMs).



ENTRUST

SECURING A WORLD IN MOTION

Introduction

Cryptographic keys stored in software can easily be found by attackers trying to hack your systems. A single stolen or misallocated key could lead to a data breach. The proven answer to securing the cryptographic keys and applications that use them is to protect those keys with a hardware security module (HSM).

HSMs are hardened, tamper-resistant devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates. HSMs are tested, validated, and certified to the highest security standards including FIPS 140-2 and Common Criteria, and they underpin the security of many enterprises around the globe today.

As organizations shift to cloud-based services, HSMs need to be accessible in the cloud too, delivering cryptography as a service to protect cryptographic keys with the flexibility needed to support workloads wherever they run. In an ever-changing digital world, enterprises need cloud-based HSMs to ensure full control over their keys, retaining the same assurance levels achieved with on-premises HSMs, while decreasing time spent on configuration, management, and maintenance.

Table of contents

4 Common Security Infrastructure Challenges

Many organizations are seeking a cryptography as a service model to support their cloud or multi-cloud strategy. Using a cryptography as a service solution helps address the following challenges:

Lack Of Resources

Finding experienced staff to deploy, manage, and maintain your security infrastructure can be a challenge. With a cryptography as a service model, the experts come to you.

Retaining Control

In seeking cloud-based HSMs for either single, hybrid, or multi-cloud workloads, retaining control of keys within the enterprise is critical to meeting compliance and regulatory requirements.

Reducing Total Cost Of Ownership

Business pressure to spread costs by moving to an OpEx model, from traditional capital expenditure (CapEx), and reducing reliance on enterprise-owned infrastructure is increasing.

Cloud-First Development

Development teams want access to cloud-based cryptographic services to align with their DevOps and DevSecOps development and deployment processes.

Considerations When Using Cloud Service Providers

Most companies' cloud strategy includes running their full suite of applications and workloads from cloud or hybrid deployments, while many are required, due to data sovereignty or compliance regulations, to keep cryptographic assets on-premises and retain control over when and where a key is used. Furthermore, some organizations determine that the risks of sharing infrastructure and HSMs in the cloud are inconsistent with their security posture and prefer dedicated services. As you evaluate cloud service providers (CSPs) that offer a one-stop shop for applications and cryptographic services for your organization's unique needs, be sure to consider the following:

- Supporting a multi-cloud strategy using cryptographic services embedded in the provider's infrastructure means solving problems such as moving your cryptographic resources from one platform to another and thus having to deal with the associated friction and possible security risks.
- When you give ownership and control of your cryptographic assets to a CSP, you have no guarantees provided on where they reside, making it very difficult to comply with data sovereignty mandates.
- With CSP services you might be sharing HSMs with other organizations.

Consider using cryptography services independent of the CSPs that:

- Support your workloads, wherever they are deployed, without the need to migrate keys between platforms
- Ensure the enterprise remains in full control of when a key can be used by your workloads and can guarantee the location of where keys are stored
- Ensure the HSMs are available for your use only

In choosing a service provider it's important to understand the roles and responsibilities for use of the HSMs and how a provider and the services they offer fit within your security posture.

HSM: A Root of Trust in the Cloud

An HSM is the root of trust in a hybrid, cloud-based, or multi-cloud environment. Its protection against cyberattacks provides:

- The highest level of protection for encryption or signing keys
- A way to implement and enforce customer-defined policy
- A recognized best practice that meets compliance mandates
- A source of high-quality key generation

A hardware security module (HSM) is a certified, trusted platform for performing cryptographic operations and protecting keys.

nShield as a Service

Entrust's nShield as a Service provides easy, efficient access to high assurance cryptography as a service. The subscription-based service gives dedicated access to FIPS 140-2 Level 3 certified nShield HSMs, enabling you to maintain full control over your key material, extend cloud-based cryptography and key management over multiple clouds, decrease time spent on configuration, management, and maintenance tasks, and meet requirements for data sovereignty mandates around the world.

Whatever your organization's use cases – from blockchain to payment security and more – with 100+ integrations with leading technology and security solution providers, nShield as a Service enhances your security posture by hardening partner solutions with certified, hardware-based cryptography.

Dedicated HSM service with fixed costs covering maintenance, software updates, and troubleshooting – avoiding metered pricing used by competitors.

CSP agnostic – retain full control of cryptographic keys within the enterprise while meeting compliance and regulatory requirements.

Facilitates geo-fencing to meet data sovereignty regulations with data centers hosted in multiple global sites. Choose where you deploy your cryptographic services.

Free up skilled cryptographic resources to work on other activities.

Deploy a Cloud-Only or Hybrid Cryptography Strategy

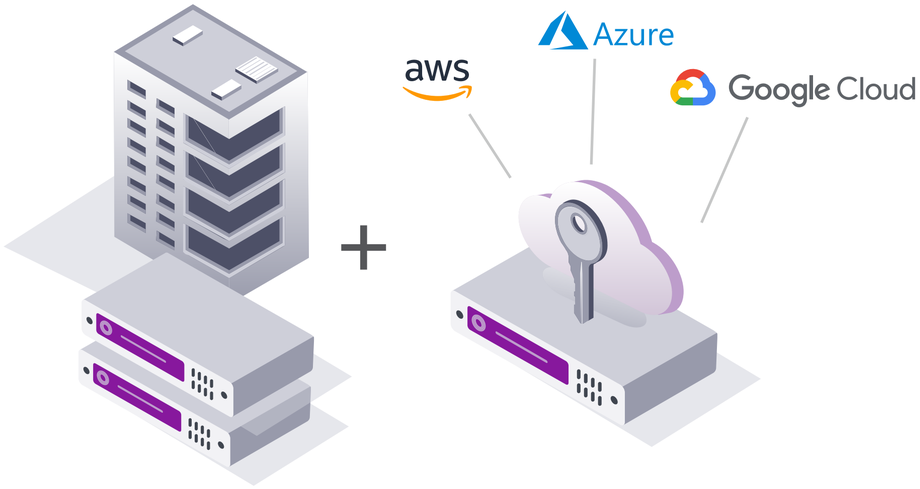
Choose a single cloud, hybrid, or multi-cloud deployment model with seamless integration via Entrust's unique Security World architecture.

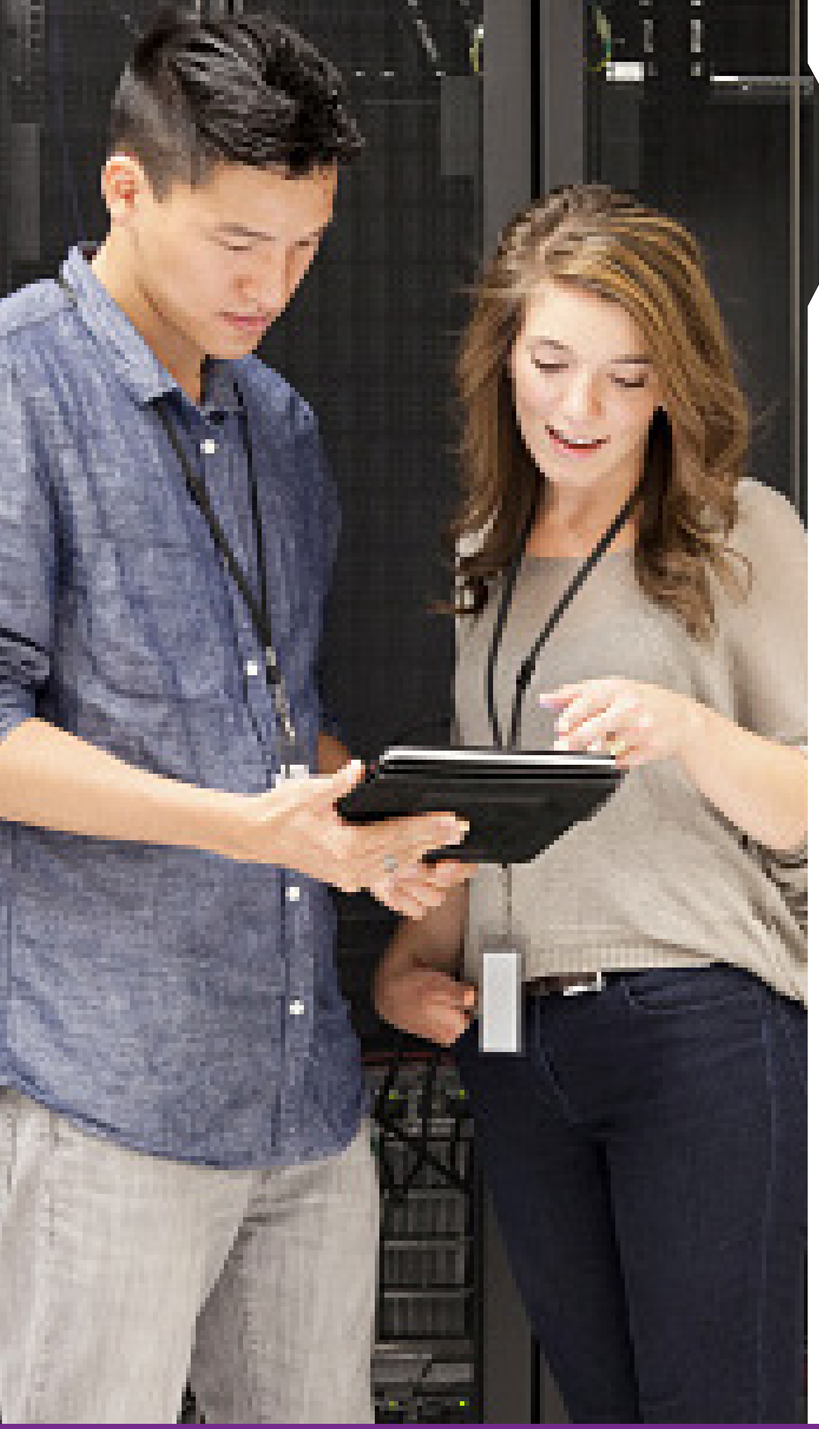
Are you an existing nShield HSM on-premises customer?

By shifting to a hybrid or cloud deployment model, you can grow your nShield HSM environment without the need to invest in additional hardware or factor in delivery, installation, and setup time. Our subscription models result in faster implementation. Because of our low-friction migration, you can continue to use your familiar business applications with cloud-based HSMs.

Cloud Deployment

Hybrid Deployment





Protecting Sensitive Business Logic in the Cloud

Running workloads in the cloud can add risk of exposure of sensitive code, exposing application logic, processes, and intermediate results. Using nShield as a Service CodeSafe protects your proprietary code and safeguards sensitive processes by running applications in a secure environment inside nShield HSMs. By being functionally isolated from external uses of the HSM, nShield as a Service CodeSafe provides an extra layer of integrity, confidentiality, and authentication to your security applications.

Without nShield as a Service CodeSafe, applications running in the cloud rely on the operating environment's security to protect their applications.

You're left wondering:

- Is process memory protected?
- Can my application be patched to alter its behavior?
- Can application logic or intermediate results be exposed to adversaries?

With nShield as a Service CodeSafe, your critical code can be moved inside the HSM, providing an extra shield of protection to your applications.

You're confident that:

- Your application is running within the FIPS certified physical boundary of the HSM.
- Your code and memory are being protected in the same manner as keys.
- The integrity of your application code is maintained throughout its life and cannot be amended or patched by an adversary.

nShield as a Service – The Entrust Difference

Easy, efficient access to cryptography as a service.

nShield as a Service offers several key advantages:

- Delivers high assurance FIPS 140-2 Level 3 certified security for cloud workloads
- Offers customers a dedicated HSM service
- Offers customers full control over when and where their cryptographic keys can be used to meet data sovereignty and residency regulations
- Ensures customers own their cryptographic resources and can securely manage their keys across workloads wherever they are deployed
- Enables customers to enhance their security posture or expand their on-premises deployment with secure code execution within the HSM FIPS boundary
- Enables customers to continue using the same business applications with their cloud-based nShield HSMs without modification
- Enables seamless extension of on-premises nShield environments, enhancing HSM capacity to handle occasional workload spikes or to implement disaster recovery strategies without the need for risky key migrations or cloning
- Enables customers to adopt a multi-cloud strategy, deploying workloads across cloud service providers, as well as supporting hybrid cloud deployment and data repatriation from a cloud service provider to on-prem as required

KEY BENEFITS:

Enables full, hybrid, and multi-cloud cryptography on-demand

Scalable, efficient, and flexible service – no additional hardware needed

Allows you to run code inside the FIPS-certified boundary of an nShield HSM

Gives you full control of your cryptographic keys at all times

Additional Resources

To learn more about nShield as a Service, view the resources below.

Watch our 2 minute whiteboard video to see how nSaaS could work for you
nShield as a Service Explainer Video

Learn about the differences between using an HSM on-premises, in the cloud, or adopting a hybrid approach
HSM Options: On-Premises vs. Cloud

View our infographic to see how a subscription-based hardware security module solution could help you
Top 5 reasons to Use nShield as a Service

Ready to talk to an HSM expert? Use the contact form on this webpage
Learn More About nShield as a Service

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments, and data. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

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