Solution Brief

Entrust Multi-Cloud Security and Automated Compliance

For Microsoft Azure

ENTRUST

SECURING A WORLD IN MOTION

Over the past few years, the cloud environment has changed radically while security has struggled to keep up. As software-defined data centers (SDDCs), hyper-converged infrastructures, and multi-cloud environments become the building blocks for data centers, organizations must implement security solutions that allow for seamless deployment on premises and in complex public and hybrid cloud environments. By providing support for leading virtualization, public cloud, and hyper-converged infrastructure, Entrust assures organizations they can deploy SDDC security controls and encryption with flexible key management across leading cloud and virtualization platforms like Microsoft Azure.

> “The key value proposition of a CMP is enabling multi-cloud management to apply policy, orchestrate, and automate across public and private cloud services in a uniform way.”
>
> — Gartner, Market Guide for Cloud Management Platforms

Top multi-cloud security challenges

A multi-cloud strategy is critical to today's organizations, because it offers speed, scalability, cost savings, and options to mix and match cloud providers; however, it comes with its own unique issues. Some of the key challenges facing today's CIOs as they look to implement multi-cloud strategies include:

- Increased operational burden and security risk, while migrating and dealing with workloads across multiple clouds
- Insider threat magnification and an increased risk of data breach due to virtualization across different business units
- Increased cost and complexity to meet auditing and compliance requirements across multiple clouds
- Increased need to avoid downtime, which is compounded by regulations that require periodic encryption rekeying

KEY FEATURES

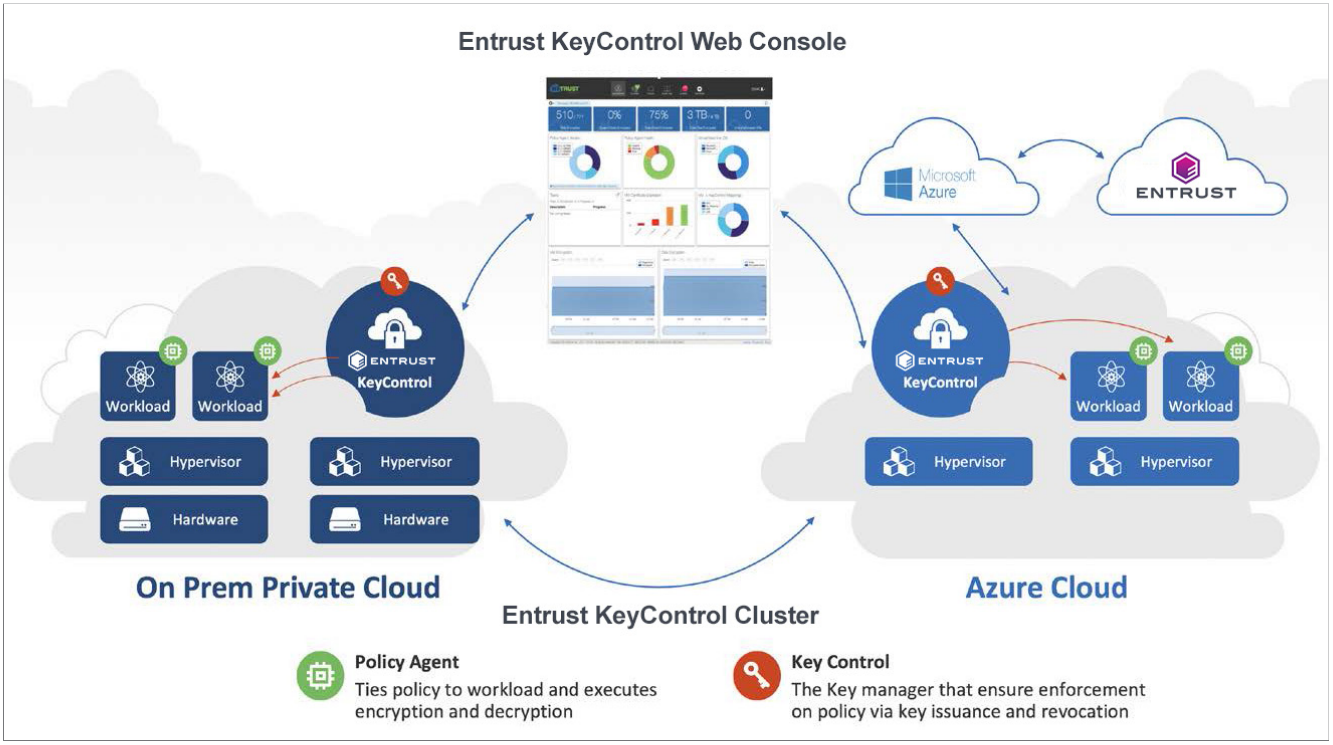
- Flexible key control – manage keys on premises and on clouds
- Microsoft-certified in the Azure marketplace
- Portable encryption travels with workloads on any on-premises or cloud platform for constant protection
- Always on – no downtime and no touch encryption
- Secure boot protection against unauthorized virtual machines or users
- Compliance with in-house security rules, as well as with industry and government regulations
- Stronger security with auto-provisioned, trusted virtualized environments
- Centralized key management provides a single pane of glass across leading cloud and virtualization platforms like Microsoft Azure

Entrust multi-cloud workload security solution for Microsoft Azure

The Entrust workload security platform allows organizations to take full advantage of SDDC and multi-cloud environments, like Microsoft Azure, without jeopardizing security. Entrust offers powerful encryption with easy-to-use, scalable key management to secure data as it traverses the computer, network, and storage stack and throughout its lifecycle – from creation to sanctioned decommission. It's the only encryption and key management solution that allows for initial encryption and rekeying of data with zero downtime. In addition, with schedule-based rekeying, administrators can "set and forget it," which eases the process for operations. This solution accelerates workload encryption by using technologies like Intel AES-NI to make encryption a transparent operation that doesn't impede performance and availability.

KEY BENEFITS

- Eliminates privileged account misuse
- Halts data breaches on all clouds
- Ends audit and compliance suffering
- Removes costly infrastructure air gaps
- Avoids data sovereignty landmines
- Prevents accidental downtimes



Key solution highlights

- **Multi-cloud key management:** Manages keys on premises and across all leading cloud and virtualization platforms, including Microsoft Azure.
- **Portable military-grade data encryption:** Delivers FIPS-140-2 Level 1 Certified and FIPS-140-2 Level 3 Capable encryption with built-in HSM support, giving organizations confidence that their data is safe in the cloud. Portable encryption controls enable workloads to check on when and where workload decryption is permitted.
- **Zero-downtime, zero-touch encryption:** Empowers IT organizations to consistently meet system-level agreements by never requiring applications to go offline and by using policy-based intelligence to ensure rekeying of workloads happens automatically.
- **Trusted platform:** Helps ensure workloads only run on trusted platforms, enabled with a hardware root-of-trust.
- **Secure boot protection:** Protects organizational data by not allowing any system to boot or access data disks for unauthorized virtual machines or users.
- **Real-time forensics:** Provides analytics ensuring data risk exposures are highlighted quickly and easily for operator override actions or automatic scheduling.
- **Complete stack protection:** Ensures the entire workload, including the O/S, applications, and data, are encrypted. Using block-level technology, the entire system can be protected, without worrying about skipping boot or operating systems files that are always in use.
- **Automated compliance:** Automates many trust- and security-related tasks for faster compliance with in-house security regulations, as well as with industry and government regulations.

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust is dedicated to securing a world in motion by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 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**