Solution Brief

Entrust BoundaryControl

Policy-based control for virtual workloads

ENTRUST

SECURING A WORLD IN MOTION

Summary

Entrust®, through its technology collaboration with Intel, has introduced new capabilities to secure the most important elements in virtualized datacenters and the cloud — applications and data — against the loss of control in cloud environments.

Entrust BoundaryControl mitigates the risks that virtualization and the cloud create, simplifying regulatory compliance, preventing data theft or misuse, and ensuring the availability of enterprise applications and data.

"Customers need an assured root-of-trust and attested parameters, like location information, that can be relied upon to allow seamless movement of VMs in various cloud deployments. As enterprises become increasingly reliant on software-defined networks within virtualized and cloud infrastructures, Entrust BoundaryControl is exactly the kind of policy-driven control with an assured source of policy information needed to enhance security and ensure compliance."

Ravi Varanasi, General Manager, Cloud Security, Intel

Background

Virtualization and the cloud make data security more complicated. Virtual machines are by nature dynamic and highly portable. Because they are simply a set of files, they can be spun up, suspended, copied, or deleted with ease. Further, they contain everything needed to run an application or workload, largely independent of the underlying hardware. Historically, there has been no automated way to ensure these workloads can only be instantiated on a specific, designated, or trusted server in a trusted location.

There are three primary factors driving the need for BoundaryControl in the cloud.

1. **Geographical mandates:** There are a burgeoning number of privacy and data sovereignty laws — such as those in Australia, Canada, and Europe — that require residents' personal data to stay within country borders. As organizations expand their cloud deployments, they are increasingly concerned about how easily virtualized data sets can be moved across geographies, national boundaries, or legal jurisdictions.

2. **Zoning:** Organizations have traditionally kept data of different risk classifications physically separate by "air gapping" servers and applications. As companies adopt virtualization and cloud computing for mission-critical or regulated applications, they seek ways to create secure zones and enclaves within this consolidated infrastructure.

3. **Availability and uptime:** Human error accounts for a significant percentage of datacenter downtime. Virtualization makes it easier for simple errors to have far-reaching impact. For example, a virtual machine can be suspended or deleted in a mouse click. If that VM is running your credit card processing system, the implications and costs can be enormous. IT organizations consistently seek to ensure availability — and for cloud service providers, uptime is also mission critical.

Entrust BoundaryControl

With Entrust BoundaryControl, customers can now set policies so that virtualized applications can only run on proven, trusted hosts that are physically located within the defined parameters. This can significantly reduce the potential for theft or misuse of sensitive data, or violation of regulatory compliance laws.

The foundation for BoundaryControl is rooted in Intel® Trusted Execution Technology (Intel TXT): Intel TXT provides processor-level attestation of the hardware, BIOS, and hypervisor, allowing sensitive workloads to run on a trusted platform. Entrust, leveraging jointly developed tools and solution components built on this root of trust, now has capabilities to securely store and propagate an asset/location descriptor that gives administrators control over where workloads can be executed.

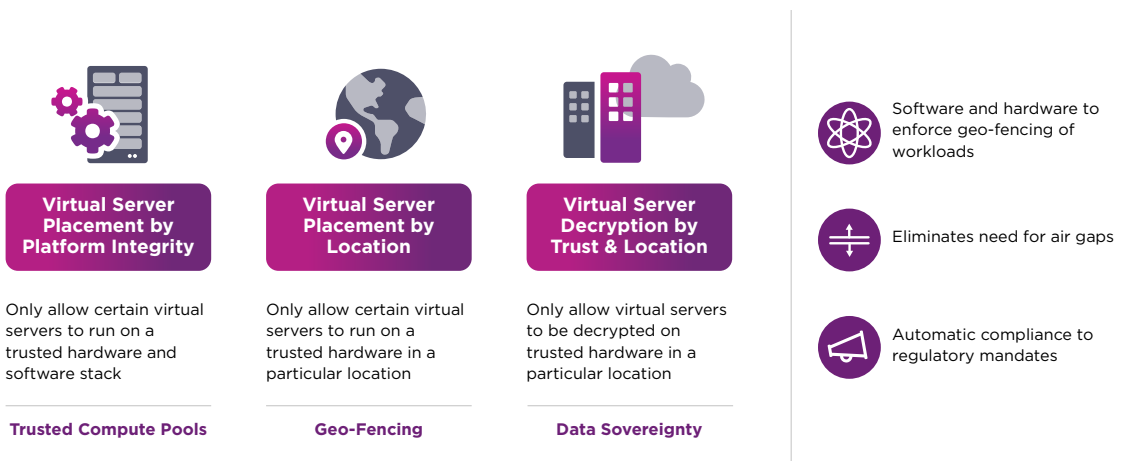
With Entrust CloudControl 6.x customers can assign labels that bind a virtual machine to a predefined location — such as a specific datacenter or within a country boundary. If the virtual machine is copied or moved outside of this location, it simply will not run.

With Entrust DataControl 5.x, an additional policy around encryption is added. Customers are ensured that data cannot be decrypted in the event the VM is moved outside of defined parameters. This reduces the possibility of theft or accidental exposure of sensitive or regulated data.

Leveraging tags enables security admins to set policies so virtual workloads only run on proven, trusted hosts or infrastructure. This boundary can be either physically or logically within Software Defined Data Center.

With BoundaryControl, encryption policies can be applied to ensure data is never decrypted outside the defend boundary or parameters set for where a virtual workload is allowed to run.

Entrust BoundaryControl



How BoundaryControl Works

To implement BoundaryControl, administrators set policies using Entrust's Tag and Label-Based Access Controls, which bind to the desired controls, such as:

- **Geography:** Companies can specify location control by country, state, county, or province. This is an ideal configuration for organizations that need to satisfy mandates to keep data within physical borders.
- **Security level:** Many organizations segment data (and datacenters) based on risk classifications or levels of confidentiality. For example, security levels allow IT to ensure PCI data only runs on virtual infrastructure classified for Payment Card Industry (PCI) data, thereby, reducing PCI audit scope or, in the case of the government, ensuring mission A's data is kept separate from mission B's.
- **Availability level:** Availability levels let IT classify and automatically validate that hardware meets the appropriate availability requirements for a given workload. This ensures, for example, that mission-critical applications cannot accidentally be moved to less available configurations.

Entrust BoundaryControl supports the European Union's upcoming new General Data Protection Regulation (GDPR), including its requirement to "implement data-protection principles in an effective manner and to integrate the necessary safeguards to protect the rights of data subjects.

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