HyTrust® Boundary Controls: Policy-based Control for Virtual Workloads

Summary

HyTrust®, 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.

HyTrust Boundary Controls mitigate the risks that virtualization and the cloud create, simplifying regulatory compliance, preventing data theft or misuse, and ensuring availability of enterprise applications and data.

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.

> 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, HyTrust Boundary Controls are exactly the kind of policy-driven control with an assured source of such policy information needed to enhance security and ensure compliance."
>
> - Ravi Varanasi, General Manager, Cloud Security, Intel.

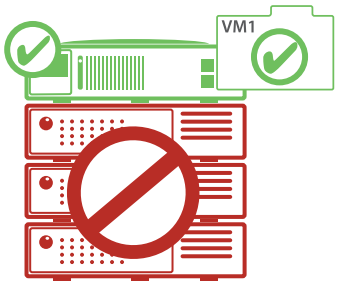
There are three primary factors driving the need for Boundary Controls in the cloud.

1. **Geographical Mandates**: There are a burgeoning number of privacy and data sovereignty laws – such as those in Australia, Canada and Europe - that require that data 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. **Availablity and Uptime**: Human error accounts for a significant percentage of datacenter downtime. Virtualization makes it easier for simple errors to have far-reaching impact — 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 cost can be enormous. IT organizations consistently seek to ensure availability; and for cloud service providers, uptime is also mission critical.

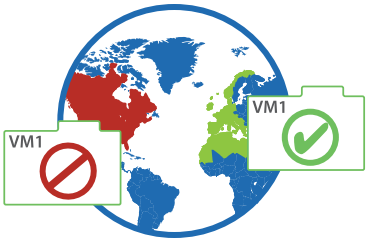
HyTrust® Boundary Controls

With HyTrust Boundary Controls, 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 Boundary Controls 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. HyTrust, 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.



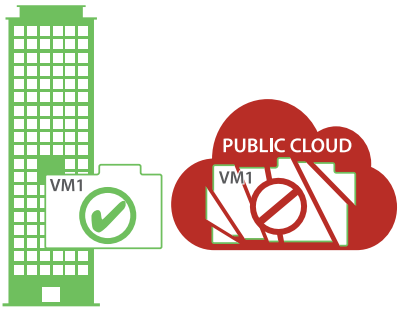
Intel TXT helps verify platform trust status. HyTrust policies can enforce that sensitive virtual workloads only run on trusted systems.



VM Geo-Fencing allows certain virtual servers to be run only on hardware in a specicific location

With HyTrust CloudControl™ 4.0, 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 HyTrust DataControl™ 2.5, 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.



Boundary Controls with ***Decryption by Location*** *allows virtual server data to be decrypted on a hardware in a particular location*

How Boundary Controls Work

To implement Boundary Controls, administrators set policies using HyTrust'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 upon risk classifications or levels of confidentiality. For example, security levels allow IT to ensure PCI data only runs on virtual infrastructure classified for PCI, thereby reducing PCI audit scope, or in the case of the government, that 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.

For More Information

To learn more about HyTrust Boundary Controls, visit www.hytrust.com/boundarycontrols or ask for a demonstration.