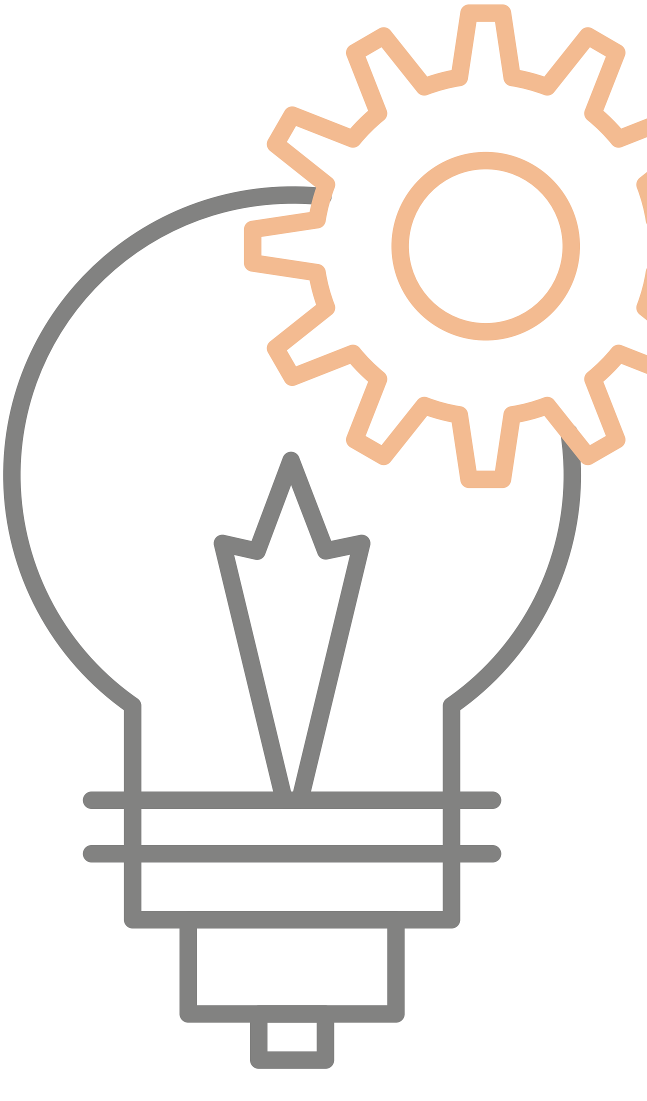
stackup

# Stacbloc HCI

# Security feature
# Guest VM perspective



Hyperconvergence
Product

# Stacbloc HCI
# Security feature - Guest VM perspective

Is my VM data secure in Stacbloc HCI environment ?

The primary security concern of Enterprise customer on the virtualization environment is on the data leak or loss of control of the guest VMs.

Stacbloc Hypervisor makes efficient use of existing Linux KVM, Qemu, Libvirt and related technologies in foundation parts. Many additional functionalities are built for Enterprise grade consumption and enhancement.

Note: While running VMs on top of hypervisor, the VMs are not aware that they are running on top of hypervisor but are aware as if they are running on top of direct hardware resource allocated for them. The hypervisor catches all commands from VMs on the fly, processes them and return them the execution results.

Stacbloc uses KVM kernel modules and Qemu emulator in user space on top of Linux. All the instructions from guest VMs run on non-root mode. This non-root mode prevents guest VMs executing any privilege instructions on the the hypervisor host. Using Intel VTx or AMD-V extensions, the kernel achieves separation between user space and kernel space. This provides isolation between guest VMs and hypervisor host, preventing a guest VM to control host and vice versa.

KVM, Storage virtualization are integrated right into Linux Kernel. KVM guest processes are subject to all the usual user space process separation that is integral to the Linux kernel's operation.

Copyright Stackup Technology Solutions

# Stacbloc HCI
# Security feature - Guest VM perspective

Inside the kernel, discretionary access control (DAC) prevents user space processes from unauthorized access of resources or other processes.

DAC is set of access controls in which users own their own resources and can manage access to those resources at their discretion. All the operation requests from guest VMs are handled as a separate thread or a process. Thus the process separation allows isolation between the guest VMs; resulting in no guest VM or it's data is shared to other guest VMs; providing inter guest VM isolation.

This ensures data and applications are fully protected, even in multi VM environments where multiple clients are served from one hypervisor instance.

Stacbloc hypervisor has built - in firewall, that allows users to define access control at network level. Users could create rules that allow or deny traffic from VM to VM or host. Exercise control with RBAC permissions to users. Enforce user controls with local PAM or domain systems like AD or LDAP. Implement password access policy at Host hardware BIOS level, Power On level, Administrator level, Host Hypervisor application level and VM workload level. Trusted Platform Module to ensure Host hardware security.

## How can I keep up my data health ?

Data availability of VMs could be enabled with usage of backup and restoration.

Data reliability of VMs could be enabled with storage clusters like CEPH or DRBD or with RAID-ed disk volumes.

Edge network security of VMs could be enabled with UTMs comprising multiple security protection technologies.

Copyright Stackup Technology Solutions