SOLUTION BRIEF

Communications Service Providers
Network Security

Accenture* Helps Protect Virtual Environments with HyTrust Technology*

Accenture Network Services helps organizations protect virtual environments utilizing HyTrust Encryption Technology.

Open, dynamic, and agile are great descriptions of the advantages of network functions virtualization (NFV)-based services. But these terms also describe a network situation that is a data security challenge. In particular, the ability of virtual environments to migrate to new servers during a virtual machine (VM) swap can expose sensitive data. Accenture Network Services,* an Intel® Network Builders ecosystem member, is working with technology from HyTrust Inc.* to provide more secure virtual environments.

The Challenge

The dynamic nature of NFV environments provides new levels of network service agility allowing communication service providers (CommSPs) to roll out new services easily by remotely installing virtual network function (VNF) software. It's also easy to provide more resources to a constrained NFV-based VM through a built-in mechanism that migrates the VM to a new server that provides those resources.

The downside of this dynamism is that it introduces security challenges. VM swapping, in particular, introduces a security challenge in that the sensitive information in these memory segments may be transferred without encryption, making it possible for a bad actor to copy and steal the information. Encrypting both of the VM swap areas allows companies to help protect this data through the VM migration process. However, the crypto operations needed to encrypt this data are very compute-hungry and can divert resources from other vital VM migration functions slowing the migration process. Encryption helps with the major security challenge posed by multiple VNFs sharing the same server; the hacking of one of the VNFs could affect the users of all of the VNFs.

Working with HyTrust, Accenture Network Services is creating encryption solutions for CommSPs worldwide.

Accenture NFV Security Framework

To help CommSPs evolve from traditional service providers into integrated digital service providers, Accenture has established the Accenture Cloud Innovation Center. The Cloud Innovation Center offers the space, technology, and Accenture expertise to brainstorm, build, and test cloud solutions before implementing them in real-world networks. Cloud Innovation Center services include:

- Cloud strategy, assessment, and roadmap
- Cloud transformation and migration
- Cloud management and optimization

Accenture NFV Security Framework with HyTrust DataControl

Accenture has created its own NFV Security Framework to help protect virtual environments utilizing data encryption and specific security embedded services for each layer in addition to help provide protection for software-defined networking (SDN) communication and the hardware infrastructure.

Accenture leverages HyTrust's DataControl product for its consulting work on encryption for VM migration security. HyTrust DataControl is part of the HyTrust Cloud Security Policy Framework (CloudSPF), which includes HyTrust CloudControl, KeyControl, BoundaryControl and CloudAdvisor.* The framework enables multicloud deployments with advanced access controls and audit capabilities, strong encryption, key management, workload geo-fencing, and data discovery and classification solutions.

HyTrust DataControl both encrypts VM data and manages encrypted data across multiple infrastructures, which is the key to protecting VM migrations. DataControl's granular encryption goes beyond the hypervisor and data storage to the encryption of individual virtual machines. In every VM, individual partitions are equipped with unique encryption keys, including the boot disk (OS) and swap partitions. Extensive access controls also prevent root users, system admins, or cloud service provider admins from accessing sensitive data. Some of the key features and capabilities of HyTrust DataControl include:

- FIPS 140-2 Level 1 compliant encryption key management.
- Zero downtime encryption with automatic re-keying.
- High availability (HA) support with active-active clustering supporting up to eight key management servers (KMS) per cluster.
- Increased protection for encrypted workloads against unauthorized access with boot and clone protection.
- Support for third-party hardware security modules (HSM) for increased key security
- Workloads are always encrypted. With HyTrust DataControl, end customers always own and control their keys, even if a workload is moved to a different cloud on purpose (such as for development purposes) or is exfiltrated by a rogue administrator or hacker.
- Full lifecycle logging of all encrypted VM actions helps uphold compliance and GDPR (General Data Protection Regulation) with audit support.

A Typical Installation

Transferring encrypted data is more processor intensive than transporting unencrypted data, so Accenture has established a hardware/software platform that delivers the performance needed for these transfers. The foundation for this system starts with servers featuring dual Intel® Xeon® E5-2699 v4 processors each with 22 cores. The HyTrust solution makes use of Intel® AES New Instructions (Intel® AES-NI), an encryption instruction set that accelerates the encryption of data on Intel® Xeon® processor powered servers. For attestation, HyTrust utilizes Intel® Trusted Execution Technology (Intel® TXT) for processor-level attestation of the hardware, BIOS, and hypervisor. Intel TXT provides the assurance that the virtualized platform will be trusted.

To virtualize these servers, either VMWare* or OpenStack* environments can be used.

On this foundation, Accenture offers virtualization layer flexibility to include either Windows* or Linux* operating systems or both. This platform also features security technology including SSH (Secure Shell) and RDP (Remote Desktop Protocol) functionality, data encryption, and HyTrust's KeyControl.

Upon deployment, Accenture utilizes a 15-step test workflow that includes installing and deploying the server, creating security, domain, and cloud admin groups and assigning users to those groups, then creating the new VM on the tenant. Once this baseline configuration is complete, the script creates a HyTrust KeyControl Mapping and installs the DataControl Policy Agent on each VM.

The disk drive is encrypted using AES-XTS-512 with a 256-bit key; then the VM is cloned and data is moved to a different VM. The data is then checked on the new drive. Because the encryption software is part of the VM, encryption travels with the VM from one physical host to another or from private to public cloud and back again if authenticated.

Conclusion

More pervasive encryption is an essential component of a comprehensive security solution for NFV solutions. Working with HyTrust encryption technology running on Intel® Xeon® processor-powered servers, Accenture is able to demonstrate a VM migration security solution that does not leave data exposed during the process.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

About HyTrust

HyTrust's mission is to make private, public, and hybrid cloud infrastructure more trustworthy for enterprises, service providers, and government agencies. HyTrust provides solutions that automate security controls for software-defined computing, networking, and storage workloads to achieve the highest levels of visibility, granular policy control, and data protection. HyTrust customers benefit from being able to accelerate cloud and virtualization cost savings while improving their security posture by automating and enforcing security policies in real time, adapting quickly to compliance requirements and preventing unplanned outages.

About Intel® Network Builders

Intel® Network Builders is an ecosystem of infrastructure, software, and technology vendors coming together with communications service providers and end users to accelerate the adoption of solutions based on network functions virtualization (NFV) and software defined networking (SDN) in telecommunications and data center networks. The program offers technical support, matchmaking, and co-marketing opportunities to help facilitate joint collaboration through to the trial and deployment of NFV and SDN solutions. Learn more at http://networkbuilders.intel.com.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. **No product or component can be absolutely secure.** Check with your system manufacturer or retailer or learn more at intel.com.