yubico

# Cloud-Based Hosting Provider Secures Virtual Machine Keys with YubiHSM 2

Case Study

intility | The Enterprise Cloud Solution

**Industry**
Cloud-Based Hosting Technology

**Benefits**

- Supports open industry security standards
- Enhanced protection for cryptographic keys
- More cost-effective than other solutions to deploy and maintain

**Deployment Info**

- Type of YubiKeys: YubiHSM 2
- Type of users: Corporate clients in multiple industries
- Date of initial deployment: September 2019

## About the organization

Intility is a complete multi-cloud platform service utilized by more than 600 companies across 2000 locations in Norway and around the world. Intility offers unlimited and scalable access to compute, storage, network, as well as integrated tools for productivity, security and mobility. Intility's goal is to act as a catalyst for companies that want to exploit the power of technology in order to increase their own productivity and competitiveness.

## The challenge: Securing Virtual Machines and Master Key

Intility instantiates many and diverse virtual machines (VMs) for its clientele across a wide geography, as a cost-effective way of deploying servers. As a cloud service provider, Intility needed to ensure that its clients' VMs and the applications and data contained within are secure against external and internal threats. An intruder or malicious administrator could make a copy of a VM, steal it away from the data center, and boot it up in another environment to access clientele information.

In order to raise the virtualization security bar, Microsoft Windows Server 2016 introduced the concept of Guarded Fabric to increase the security of Hyper-V Virtual Machines (VMs). Intility implements Microsoft Guarded Fabric to protect and secure mission critical systems, custumer data and services. A Microsoft Guarded Fabric consists of a Host Guardian Service (HGS) comprised of the Attestation Service and the Key Protection Service, a Guarded Host and a Shielded VM. The Key Protection Service stores and protects the master key in software. For enhanced security purposes, Intility wanted to deploy hardware protection for the master keys used by the Host Guardian Service. Intility was looking for a hardware security module that was both cost-effective and easy to deploy.

**Arne Klæboe, Technical Manager, InCloud Applications & Security, Intility**

"Intility sought a mechanism to encrypt the root of trust associated with the encryption methodology used with Host Guardian Service. YubiHSM was the best solution."

Case Study

intility The Enterprise Cloud Solution

**Industry**
Cloud-Based Hosting Technology

**Benefits**

- Supports open industry security standards
- Enhanced protection for cryptographic keys
- More cost-effective than other solutions to deploy and maintain

**Deployment Info**

- Type of YubiKeys: YubiHSM 2
- Type of users: Corporate clients in multiple industries
- Date of initial deployment: September 2019

## The solution: YubiHSM 2

Intility deployed the Yubico YubiHSM 2 hardware security module, based on USB-A hardware RSA keys. YubiHSM secures the Host Guardian Service signing and encryption keys which validates the hosts ability to run a VM, as well as decrypt it.

The YubiHSM hardware security modules are inserted into a USB-A port on the servers running the Host Guardian Service. The Host Guardian Service protects the encryption keys needed to decrypt and start VMs.  Because YubiHSM provides protection for the keys on hardware that is physically isolated from operations on the server, it adds an additional layer of security that is safe from software-based attacks.

> **Anything that needs a high level security on the machines is also eligible for being protected with an encryption on the virtual machine.**

## The results: Enhanced security with a simple and cost-effective solution

- Running VMs under Microsoft's Host Guardian service, results in encrypted VMs that are protected using YubiHSM.
- The YubiHSM compatibility to protect other Active Directory Certificate Authority applications, and/or those needed for Linux (or in conjunction with both Windows and Linux instances running on Hyper-V) provides optional functionality for clients.
- YubiHSM is easy to install and deploy, and is easily administered under standard Microsoft administration software.
- YubiHSM offers a low cost and high security alternative to traditional, expensive hardware security modules on the market.

**About Yubico** Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at **www.yubico.com.**

**Yubico AB**
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

**Yubico Inc.**
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088