UpCloud

Security Overview

February 21st, 2019

Version 1.7

Table of contents

Introduction

UpCloud is an innovative Infrastructure-as-a-Service provider from Finland with a strong technical and business background in the hosting industry. We take pride in each customer who chooses to host with us. To us, this means they trust us with their business - everything they have at stake. Needless to say, we take this trust with the utmost importance and seriousness. We also understand that it is our task to bring transparency into the way we operate to build mutual understanding on the opportunities and responsibilities when operating in the cloud. This document is one of the ways we want to bring clarity and build trust in the way we operate our business, especially from a security point of view.

Revisions

Version	Date	Note
1.0	February 26th, 2014	First version of this document.
1.1	March 8th, 2017	Added Frankfurt, Singapore, Amsterdam data centres & CISPE participation.
1.2	September 3rd, 2017	Updated the new UK data centre, upcoming Finnish FI-HEL2 data centre as well as an update to disk types.
1.3	June 14th, 2018	Updated FI-HEL1, FI-HEL2 and SG-SIN1 descriptions. Added PayPal to accepted payment methods.
1.4	June 15th, 2018	Added new US data centre US-SJO1.
1.5	January 11th, 2019	Updated with new brand.
1.6	January 21th, 2019	Refined Equinix HE6 certifications.
1.7	February 21st, 2019	Updated FI-HEL2 specifications.

Working with UpCloud

A shared responsibility model

When you build your IT-infrastructure to UpCloud you are entering a model where both parties, UpCloud and you - are responsible to obtain the best security available. UpCloud, being an Infrastructure-as-a- Service (IaaS) provider offers the technology in the physical facility where the servers are, the network connections, electricity, high-level security at the premises, networking solutions and the virtual servers as a service. UpCloud also offers readily available operating system images for your virtual servers, but you may replace them with your own if you wish.

What is run on the virtual servers and the applications it has been installed with, is completely the responsibility of the customer. UpCloud offers and is thus also responsible for some added services such as backups made through the service and firewall configurations which the customer may use on their virtual server. However, the customer is responsible for configuring these services.

In working with a sophisticated provider, such as UpCloud, it is important to understand the shared responsibility model regarding your IT-infrastructure to achieve the best possible results in terms of security and performance.

Environmental security and integrity

UpCloud has been built with the highest standards and requirements in mind. Our business is focused in providing our customers the best service from the best data centres around the world. We require the highest standards from the data centres we work with.

DE-FRA1 - Frankfurt, Germany

For our Frankfurt, Germany, data centre UpCloud has chosen Interxion (NASDAQ: INXN). Interxion operates multiple buildings in Frankfurt and it is one of the largest service providers of such kind in Frankfurt. The data centre is located directly at the connection points to multiple transit providers and DE- CIX.

Interxion has achieved ISO 27001 (Information Security Management System), SOC2 Type II (Service Organisation Controls), PCI-DSS (Payment Card Industry Data Security Standard), ISO 22301 (Business Continuity Management System) as well as ISO 9001 (Quality Management) certifications with its Frankfurt data centre.

More information on the facility is available at:
https://www.interxion.com/globalassets/_documents/_fact-sheets/english/campus/frankfurt-campus-factsheet.pdf

FI-HEL1 - Helsinki, Finland

In Helsinki, we host FI-HEL1 in the Equinix HE6 data centre which consists of 7400m2 of floor space. It also offers N+1 redundancy in cooling and electricity, with high sensitivity smoke detection as fire suppression. Security at the venue is in line with our requirements with mantraps, CCTVs, 24/7 onsite security officers and so forth.

The venue is compatible with the Finnish governmental security standards VAHTI T3 and KATAKRI. In addition it has achieved the international certifications of ISO 27001, ISO 9001, ISO 14001, OHSAS 18001.

More information on the facility is available at:
http://www.equinix.com/locations/finland-colocation/helsinki-data-centers/he6/

FI-HEL2 - Helsinki, Finland

In Helsinki, we host FI-HEL2 in Telia Helsinki Data Center. The facilities consists of 15 000 m2 of floor space. Power and cooling are provided in a redundant fashion. The venue provides the required physical security measures with camera surveillance and electronic access control.

In addition to Telia's own connections, this carrier neutral data center provides access to all major providers and local internet exchanges.

The venue has ISO 27001 certification for security standards, in addition to ISO 14001 certification for environmental management.

This data center uses renewable and carbon-neutral electricity, mainly hydropower. Excess heat is used for heating nearby buildings.

https://www.telia.fi/business/telia-helsinki-data-center

NL-AMS1 - Amsterdam, Netherlands

For our 6th data centre we continue to work with Interxion (NASDAQ: INXN). Interxion is a Dutch company and founded in Amsterdam. Netherlands has been rightly given the title of Internet Hub of Europe as it boasts one of the most important connection points regarding network infrastructure.

NL-AMS1 is also powered by 100% renewable energy. Interxion has achieved ISO 27001 (Information Security Management System), SOC2 Type II (Service Organisation Controls), PCI-DSS (Payment Card Industry Data Security Standard), ISO 22301 (Business Continuity Management System) as well as ISO 9001 (Quality Management) certifications with its Amsterdam data centre.

More information on the facility is available at:
https://www.interxion.com/globalassets/_documents/_fact-sheets/english/campus/amsterdam-campus-factsheet.pdf

SG-SIN1 - Singapore, Singapore

In Singapore UpCloud operates out of Data Centre SG's data centre that spans 10 050 m^2 and offers up to 20MW of power. Data Centre SG's Singapore facility offers manned security on a 24/7/365 basis including key card access, biometric scanners and video cameras.

Data Centre SG Singapore has achieved the following certifications: UTI Tier III design, SOC1 Type 2, SOC2 Type 2, ISO 27001, Bizsafe and TVRA.

More information on the facility is available at:
https://www.dcsg.sg/data-centre/

UK-LON1 - London, UK

In London, UpCloud hosts its servers at a Volta facility. The data center offers approximately 8450 m^2 (91000 sq ft) of floor space. It covers four floors and offers N+1 redundancy in cooling and electricity. Total cooling capacity is 8.3MW and it enjoys two separate 33kV electricity supplies from two independent grid substations.

The facility has achieved the following certifications ISO 9001, ISO 27001, ISO 14001, ISO 14644-8, OHSAS 18001, PCI DSS and PAS 99.

More information on the facility is available at: https://www.voltadatacentres.com

US-CHI1 - Chicago, USA

In Chicago, UpCloud works with Coresite (NYSE: COR). Their Chicago facility is located right next to the Chicago Board of Trade and thus serves customers from one of the largest financial districts in the world. The premises offer some 180 000 square feet of floor space for customer capacity. Coresite's Chicago facility offers manned security on a 24/7/365 basis including key card access, biometric scanners and video cameras.

Coresite's Chicago facility is also SSAE 16 Type 2 compliant, meaning it can be used by customers in highly regulated industries such as financial services, healthcare, government, legal, biosciences, cloud computing and many others. The compliance assures CoreSite customers of the reliability of power and cooling, the security of premises and the quality of technical support.

More information on the facility is available at:
https://www.coresite.com/data-centers/locations/chicago

US-SJO1 - San Jose, USA

In San Jose, UpCloud works with Coresite (NYSE: COR). We operate from CoreSite's newest Santa Clara campus data centre that features the latest in data centre efficiency and redundancy designs. Coresite's Santa Clara campus facility offers manned security on a 24/7/365 basis including key card access, biometric scanners and video cameras.

Coresite's Santa Clara campus facility has achieved the following certifications ISO 27001, PCI DSS, HIPAA, SOC 1 Type 2 and SOC 2 Type 2.

More information on the facility is available at:
https://www.coresite.com/data-centers/locations/silicon-valley/sv7

Network

UpCloud treats its network with equal care and attention as it does with the other parts of its infrastructure. The network is built in a fault tolerant and resilient manner, while maintaining a high level of security. In addition, UpCloud monitors its networks in all service locations on a 24/7/365 basis in multiple different ways.

Network access

As customers create their service contracts with UpCloud Ltd (registered and located in Helsinki, Finland), all initial customer connections to the Control Panel are made to servers located in Finland. The Control Panel interface is further in touch with UpCloud's management servers which are located behind API- access.

All UpCloud data centre facilities are connected to the API-endpoints in a secure and fault-tolerant manner for the provisioning of services inside the data centres. Each data centre has only access to the management servers through the API and thus do not directly communicate with any other data centre, due to UpCloud's security requirements.

Management network segregation and identity management

UpCloud's management network is segregated from the service infrastructure network. Those with requirements to access the production environment and network for maintenance purposes do so through specific access points and servers, which require all users to log in with their specific credentials. These access points log all user activity for potential audit requirements later on.

Designed for resiliency and redundancy - N+1 by default

One of the most important guiding design principles in all of UpCloud's technology, including its network, is the resiliency and redundancy of the services in the most unexpected situations. UpCloud's network architecture has been built with this in mind. We try to anticipate the most unexpected situations when we architect our infrastructure.

With this principle at the core, all UpCloud's data centres are connected to multiple transit connection providers. As we move inside the data centre on the networking level, all devices have been installed with the N+1 mentality in mind. If a core router, for example, breaks down, there is always at least one pair to take over its job in a matter of seconds. While this increases redundancy, it also increases the overall performance available to our customers. All networking devices follow this N+1 principle by default.

Firewall

UpCloud's infrastructure firewall works in two separate stages. At the core level, we take care of the most common malicious attacks in addition to stopping DDoS-attempts.

At the second stage, the firewall is topologically located right in front of the customers' server instances. All traffic to and from the server instance always goes through the firewall first to prevent L2-level threats (such as ARP poisoning attempts) and to also further separate the server instances from each other.

The customer may also configure and use the L3-level firewall from the UpCloud Control Panel or through the API.

Compute resources

In this section we will give an overview of the security measures used in building and designing our compute resources.

The hypervisor and isolation of instances

One of the most critical issues in running an environment where multiple customers share physical hardware and rely on the same software for virtualisation is the isolation of instances in a secure and thorough manner. UpCloud relies on KVM due to its strong guest isolation procedures.

Because KVM is built into Linux, the KVM guest processes are subjective to the same principles that a Linux operating system follows regarding its user process separation. Despite the continuous development of separation processes, the most basic separation mechanisms have existed since the beginning and have thus undergone thorough testing and certification.

KVM's Type 1 design is similar to other x86 hypervisors, such as VMWare and Xen. KVM further uses virtualisation specific processor instructions to ensure isolation of guests from the hypervisor and from each other. A third level of isolation and protection is added by Intel's virtual machine extensions (VMX) and AMD Secure Virtual Machine (SVM) instructions.

KVM is an open source initiative and is thus continuously inspected and tested for flaws by a wide community of users.

Host operating system

Those UpCloud personnel with a need to access the host operating system for administrative purposes do so through specially defined procedures. In addition to unique credentials to identify all users, all user activity is logged.

Guest operating system

The guest operating system is the software deployed by the customer onto the virtualized server. UpCloud's personnel have no access to the guest operating systems whatsoever. In other words UpCloud has similar capabilities as anyone else attempting to access the server from the public internet. Thus it is extremely important that you configure your server security in such a way that you are able to access it at all times.

Storage resources

In addition to the compute resources (CPU and memory) a core part of the service are the storage resources UpCloud offers. In this part we go over how we have designed the services from a security point of view and what this means for the customer.

Storage backends - HDD & MaxIOPS

UpCloud offers two types of storage backends to its customers, HDD and MaxIOPS. There is no distinction in how these storage systems have been produced regarding security. Because the storage backends utilise Infiniband based fabric, it is not possible to access the storage systems from the public internet.

To further build redundancy to the storage backend, UpCloud always keeps all customer data on two separate storage backends in the same data centre. On both storage backends the data is further RAID- secured. This is a standard procedure for all disks deployed and used on UpCloud.

Backups

Customers are also able to set scheduled backups to further increase security and redundancy. Backups on UpCloud are handled on a third, separate storage backend from the live production data in the same data centre. Therefore if a loss of data occurs in the production environment, the backed up data is not affected in any way.

Scrubbing deleted disks

Once customers delete their disks on UpCloud, the disk enters a process where UpCloud thoroughly writes the disk with non-meaningful data to clean it completely for new use. This process is commonly called scrubbing and it is a standard procedure applied to all disks that are deleted from customers’ servers on UpCloud, be it through the control panel or the API.

Additional services

In addition to the core features, UpCloud offers some additional functionalities that are part of the overall service. The security of these services is outlined below.

VNC access

VNC access enables server management in a similar manner to that of being directly connected to the server with a monitor and keyboard. VNC access is especially useful in situations when you are not able to connect to the server through traditional remote connection methods, such as SSH or RDP.

As the VNC access enables complete control of the server, we have disabled access by default and customers must enable it to use the feature. Customers can also change the VNC access password through the settings in the UpCloud Control Panel.

We recommend customers only use their VNC access in non-standard situations, such as a maintenance window, so that by default the access would be disabled for added security.

API access

Connections to the UpCloud API access point always proceed through SSL-secured connections. Authentication takes place through the HTTP Basic access method using a unique username and password.

By default, the API connection credentials are not available for newly registered accounts and the customer must create account specific credentials through the UpCloud Control Panel. It is also possible to limit API access further by source IP-address.

Control Panel

All connections to UpCloud control panel are passed over SSL / HTTPS. Users need to have a valid functioning username and password to enter the Control Panel. In the case of a lost password, users need to retrieve it with access to both the e-mail and telephone number used during the registration process.

Payment mechanisms

Customers are able to pay with either credit cards, PayPal or in the case of Finnish customers, direct bank payments. Credit card payments are handled by Braintree Payments, which is a company owned by PayPal (NASDAQ: EBAY). Braintree Payments is PCI-DSS compliant. For the direct bank payments for Finnish customers UpCloud works with Paytrail. Paytrail is a licensed payment institution by the Finnish Financial Supervisory Authority to handle payments online. Paytrail is also PCI-DSS compliant.

UpCloud’s efforts in promoting data privacy

UpCloud is a proud member of CISPE (Cloud Infrastructure Service Providers of Europe) and our CEO is a member of its Board of Directors. CISPE promotes a proactive approach to data privacy and an industry built compliance towards GDPR.

CISPE is a non-profit organisation registered in Brussels, Belgium with more than 20 corporate members from around Europe, including, but not limited to Amazon Web Services, OVH, Hetzner, Leaseweb, Aruba and naturally UpCloud. The goal of the organisation is to promote a unified approach to data privacy within the industry and build adherence to its code-of-conduct launched in October 2016.

More information on CISPE and its code of conduct can be found below:
https://cispe.cloud
https://cispe.cloud/wp-content/uploads/2017/02/CISPE-CodeOfConduct-27012017.pdf