CCPro security

There are two key components to CC Pro security

CCPro is hosted on Digital Ocean

We host all CC Pro servers in the London Data Centre (LON1) of Digital Ocean which has the following security certifications:

SOC 1 Type II
SOC 2 Type II
ISO/IEC 27001:2013
PCI-DSS

DigitalOcean Infrastructure security is the foundation of maintaining secure cloud instances. This includes the physical data centre security, networking components, and virtualization infrastructure. Digital Ocean's infrastructure is continually maintained following internationally recognized security controls. Our infrastructure is monitored 24/7/365 and undergo third-party audits as well targeted testing annually. For physical security, each of our data centre colocation providers maintain industry-recognized certifications and our networks are MANRS certified.

Networking

DigitalOcean networks are collections of servers connected by wires provided by an Internet Service Provider (ISP). We develop, document, and maintain a current baseline for all machines and network device hardware. The following list is an example of controls we maintain for network security:

- Update the baseline configuration for network devices at least annually or when a significant change occurs.
- Use the least privilege method when provisioning infrastructure components. Any unnecessary ports or protocols are disabled. Network scanning is performed to validate that any ports or protocols are in use as defined.
- Use industry standard transport protocols such as TLS between devices and DigitalOcean data centres, and within data centres themselves.
- Employ a defense in-depth strategy for boundary protection, including secure segmentation of network environments through several methods including VLAN segmentation, ACL restrictions, and encrypted communications for remote connectivity.
- Define, implement and evaluate processes, procedures, and defence-in-depth techniques for protection, detection, and timely response to network-based attacks.
- Establish procedures to synchronize servers and network devices in the DigitalOcean environment with NTP Pool Project servers that sync off of the Global Positioning System (GPS) satellites.

Servers

DigitalOcean servers are hardware connected by a network housed in a data centre. Every DigitalOcean data centre implements controls that ensure physical access to the facilities, backup data, and other system components such as virtual systems and servers is restricted. The following list is an example of controls DigitalOcean and its data centres maintain for server security:

- Biometric, proximity card, and/or personal identification number (PIN) reader systems (varies by data centre facility) used to restrict data centre access to only those individuals provisioned with access; the systems are also used to monitor, log, and notify personnel of physical security alarms.
- Maintain monitoring mechanisms over infrastructure to check server performance, data, traffic, and load capacity.
- Detect and route issues experienced by hosts in real time and employ orchestration tooling that has the ability to regenerate hosts.
- Third parties provide a certificate of destruction upon destruction of physical production assets maintained in the collocated data centres.
- Documented logical access policies and procedures to guide personnel in information security practices that include, but are not limited to: password requirements, acceptable use, access provisioning, and access termination

For more information on our data centre controls, please visit their Trust Platform.

Storage

DigitalOcean storage is the physical disk on the server that runs your Droplet. These devices are encrypted at rest based on industry standards. Our storage devices have the same physical security protections as our servers. The following list is an example of additional controls DigitalOcean maintains for storage security:

- DigitalOcean's asset inventory includes serial number tracking for servers, disks, and other assets necessary to provide infrastructure for customers.
- Where full disk encryption is used, logical access is managed by FileVault for MacOS and BitLocker for Windows operating systems; Linux encryption occurs during the operating system build, alternatively the home directory is encrypted. Kollide reports on Linux configuration to ensure encryption is present.
- In-scope systems are configured to require at least one of the following authentication requirements:
- Authorized user account and password
- MFA
- SSO
- SSH

Virtualization

Cloud hosting environments are broken down into two main parts: the virtual servers that apps and websites can be hosted on, and the physical hosts that manage the virtual servers.
Virtualization makes cloud hosting possible: the relationship between host and virtual server provides flexibility and scaling that are not available through other hosting methods. Virtualization allows multiple DigitalOcean customers to host their products on the same disk with inherent logical separation. The following list is an example of security measures we maintain for securing your virtualized instance:

- Initial permission definitions, and changes to permissions, associated with logical access roles of production-impacting systems are approved by authorized personnel.
- We maintain device configuration policies on security requirements for the configuration and management of devices connecting to corporate services. The policies also apply to infrastructure and virtual instances.
- Customer environments are isolated using numerous mechanisms, technologies, policies, processes, and architectural elements. Customer tenants and Virtual Machine deployments are kept logically separated. Customer data may be encrypted in-transit and at-rest through configurable and standards-based providers using a variety of protocols.

There is a firewall with automatic IP blocking for offenders on each of the servers.

There is ability to enable whitelisted-only access to CC Pro when users can connect only from specified list of IP addresses. So, if some company wants the system to be accessible only from the company premises such functionality is already built in. Similar whitelist-only access is always enabled on the PBX servers.

All the traffic to, from and between the servers, including the voice, is over secured, encrypted connection.

Each server has automated back-ups enabled.

CCPro SIP Trunks.

Protect your business from costly phone hacking and misuse
Hacking and abuse of business telephony is becoming as big as credit card fraud. With this type of abuse, the cost of the calls falls to your business. But with our Call Guard service your business is protected from such activity.
Your calls protected from unusual usage.
Low cost for peace of mind knowing your calls are protected.
Avoid any unwanted expensive bills.
Can be applied to all of your existing numbers.
Tailor your protection – opt numbers in and out as required.

CCPro Trunks Fraud Management:

- Daily Spending Limit
- Weekly Spending Limit
- Ability to set a (%) warning level with an email notification
- Selective Outbound Call Barring (details below)

Our SIP Trunk comes with the ability for optional outbound barring of:

- Premium Calls
- International Calls
- Special Services Calls (084)
- Special Services Calls (087)
- Directory Enquiries Calls (118)