2021 WHITE PAPER

UberCloud Security on Microsoft Azure

UberCloud is dedicated to safeguarding your data

Engineering data is of strategic importance. Protection of this data from accidental deletion and unauthorized change or disclosure is a key part of any cloud implementation.

UberCloud Security

How UberCloud ensures your valuable data is kept safe

Data security is critical to organizations, irrespective of whether that data is in the cloud or not. To protect the privacy of its customers and their data, UberCloud and its partners maintain the highest standards of data security. UberCloud enforces strict internal product controls, and regularly audits its policies and procedures.

The pillars of UberCloud's security protocols are:

- Security designed “from the ground up“ in the application, network, hardware, and procedures.
- Clear guidelines for Logical Security as well as Physical Security.
- Enterprise data centers with world-class protection and monitoring.
- Industry-leading encryption options to secure data in motion and data at rest.
- Authentication procedures that leverage best practices such as multi-factor authentication.
- Mechanisms to ensure that only authorized individuals have access to data per security policies
- Code development, testing, and operations that adhere to security best practices.
- Regular review of the policies and procedures for UberCloud security and operations.

The following sections of this whitepaper cover the key areas of UberCloud security in detail. The primary areas of security including: Physical Security, System Security, Operational Security, Application and Data Security.

UberCloud uses Microsoft's Cloud Resources, which are protected by a team of 3,500 global cyber-security experts and more than $1 Billion invested each year on security

Physical Security

An important part of information security is the physical security of the hardware hosting customer data. UberCloud has partnered with Microsoft, the leading enterprise cloud provider to host its HPC cloud platform.

Because UberCloud uses Microsoft Azure as its cloud, customers automatically get a network of highly secure datacenters with a rigorous set of security controls that govern operations and support.

Microsoft datacenters are protected by layers of defense-in-depth security that include the following physical safeguards:

- Each facility is designed to run 24x7x365 with measures to protect operations from power failure, physical intrusion, and network outages.
- The datacenters comply with industry standards (such as ISO 27001) for physical security and availability.
- Round the clock 24-hour coverage by security administrators and armed guards working in shifts.
- Perimeter fencing, video cameras, retina scans to allow access only for authorized personnel.
- Background verification checks of certain operations personnel and limited access to applications, systems, and network infrastructure in proportion to the level of background verification.
- Microsoft Cyber Defense Operations Center (CDOC) manned by security response experts to help protect, detect, and respond 24/7 to security threats in real time.

Microsoft's security policies and procedures can be found at:

https://www.microsoft.com/en-us/security/default.aspx

UberCloud ensures that the networks, servers and containers that host your data are hardened and tested against attack by our seasoned engineering team.

System Security

In addition to making sure that the infrastructure containing customer data is physically secure, UberCloud also ensures that the networks, servers and containers that host the data and application are hardened and tested against attack.

This includes:

- Hardware security
    - New hardware is provisioned with a hardened operating system with only the necessary programs and services turned on
    - Security patches are applied on a regular basis to ensure the latest protection is available.
    - Provisioning follows documented policies and procedures that are reviewed regularly
- UberCloud's container technology is based on the Linux kernel. This layer enables full separation of duties between the engineering and operations teams.
- UberCloud containers enable customers to have full GUI access that is protected by SSL encryption.
- Containers provide secure remote command line access as well as remote secure file transfer with industry standard SSH encryption.
- All other network access to the container is disabled via the firewalls provided by Microsoft Azure.
- Containers are scanned for vulnerabilities by a 3rd party tool. Issues identified are prioritized by severity and addressed.
- Azure Storage offers a set of security features that help secure your storage account by using Role - Based Access Control (RBAC) and Microsoft Azure Active Directory (Azure AD).
- Azure also offers Storage Service Encryption, which will encrypt data written to the storage account.

The guiding principle of Microsoft's security strategy is to "assume breach." The global incident response team works around the clock to mitigate the effects of any attack.

Operational Security

It is not enough to have physical security and system security. The entire environment must also be operated in a secure manner.

UberCloud and Microsoft adhere to a rigorous set of security controls that govern operations and support. Microsoft deploys combinations of preventive, defensive, and reactive controls including the following mechanisms to help protect against unauthorized developer and/or administrative activity:

- Tight access controls on sensitive data, including a requirement for two-factor smartcard-based authentication to perform sensitive operations.
- Combinations of controls that enhance independent detection of malicious activity.
- Multiple levels of monitoring, logging, and reporting.

UberCloud Corporate operational security includes:

- Fully documented policies and procedures that are reviewed annually.
- All employees are trained (on hire and annually) on documented information security and privacy procedures.
- Background checks are performed on all employees who have access to customer data
- Access to the production network is limited to authorized personnel, who access it using a secure, site-to-site Virtual Private Network (VPN)
- Access to customer data is limited to authorized personnel only, according to documented processes.

UberCloud, Inc
2310 Homestead Rd. Suite:C1-301
Los Altos CA 94024
USA
www.theubercloud.com
Email: sales@theubercloud.com

Certifications

UberCloud understands that to realize the benefits of the cloud, you must be able to trust the cloud. Microsoft has been leading the industry in establishing clear security and privacy requirements and then consistently meeting these requirements. Azure meets a broad set of international and industry-specific compliance standards, such as GDPR, ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards such as Australia IRAP, UK G-Cloud, and Singapore MTCS.

Rigorous third-party audits, such as by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate.

If you have additional questions regarding UberCloud security safeguards and procedures, please contact the UberCloud team at:

Email: help@theubercloud.com