TimeDock data centre and server security

Last updated - Jun 02, 2020 at 2:55PM

Web:	https://timedock.com
Email:	info@timedock.com
International:	(+64) 9 444 1384
Local phone:	(09) 444 1384

Excerpt from TIMEDOCK's cloud services provider of Database, Application, Cache, Service Bus etc.

Through cutting-edge security practices and unmatched experience running some of the largest online services around the globe, Microsoft delivers enterprise cloud services customers can trust.

Design and Operational Security

Microsoft has developed industry-leading best practices in the design and management of online services, including:

Security Centers of Excellence. The Microsoft Digital Crimes Unit, Microsoft Cybercrime Center, and Microsoft Malware Protection Center provide insight into evolving global security threats.

Security Development Lifecycle (SDL). Since 2004, all Microsoft products and services have been designed and built from the ground up using its Security Development Lifecycle - a comprehensive approach for writing more secure, reliable and privacy-enhanced code.

Operational Security Assurance (OSA). The Microsoft OSA program provides an operational security baseline across all major cloud services, helping ensure key risks are consistently mitigated.

Assume Breach. Specialized teams of Microsoft security engineers use pioneering security practices and operate with an 'assume breach' mindset to identify potential vulnerabilities and proactively eliminate threats before they become risks to customers.

Incident Response. Microsoft operates a global 24x7 event and incident response team to help mitigate threats from attacks and malicious activity.

Security Controls and Capabilities

Azure delivers a trusted foundation on which customers can design, build and manage their own secure cloud applications and infrastructure.

24 hour monitored physical security. Datacentres are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.

Monitoring and logging. Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts. In addition, multiple levels of monitoring, logging, and reporting are available to provide visibility to customers.

Patching. Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.

Antivirus/Antimalware protection. Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real-time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.

Intrusion detection and DDoS. Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.

Zero standing privileges. Access to customer data by Microsoft operations and support personnel is denied by default. When granted, access is carefully managed and logged. Data center access to the systems that store customer data is strictly controlled via lock box processes.

Isolation. Azure uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users. Virtual Machines do not receive inbound traffic from the Internet unless customers configure them to do so.

Azure Virtual Networks. Customers can choose to assign multiple deployments to an isolated Virtual Network and allow those deployments to communicate with each other through private IP addresses.

Encrypted communications. Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacentres, and from Azure to administrators and users.

Private connection. Customers can use ExpressRoute to establish a private connection to Azure datacentres, keeping their traffic off the Internet.

Data encryption. Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to implement the methods that best meets their needs.

Identity and access. Azure Active Directory enables customers to manage access to Azure, Office 365 and a world of other cloud apps. Multi-Factor Authentication and access monitoring offer enhanced security.

Internal IT and Procedures

Production Data (i.e. Live Customer Data), protected by strong security implemented on the servers which they are hosted, still pose potential risk with outside interfaces (i.e. 'the human element').

To minimize risk we:

- Implement strong identity and password-based authentication at many stages between the development, staging and deployment environments.
- Never download or share live data with any of our development or staging environments.
- Implement demilitarized-zones for segregating departments, and people.
- Run extensive manual and automated testing, before deploying production features that could expose or harm tenant data.
- Educate all staff, even the receptionist, on common fail-points such as rogue emails, unknown attachments, suspicious phone calls, USB drives of unknown origin, etc.
- Implement other standardised IT practises (i.e. Antiviruses, Firewalls, regular security update checks, etc.).

Data Backup

To minimize risk of data loss and corruption we utilize several strategies, standardized for a cloud-based setup.

1. Geolocation redundancy –Databases are replicated (near-live) on up to four secondary instances to ensure high availability and disaster continuity.
2. 35-day point-in-time database recovery backups.
3. 12-hour differential backups.
4. Weekly backups, retained for 10 weeks.
5. Monthly backups, retained for 12 months.
6. Yearly backups, retained for 7 years.

Note: As per the SLA customers are required to back up their own data, as a secondary measure, by utilizing reporting and data export functions made available by the service.