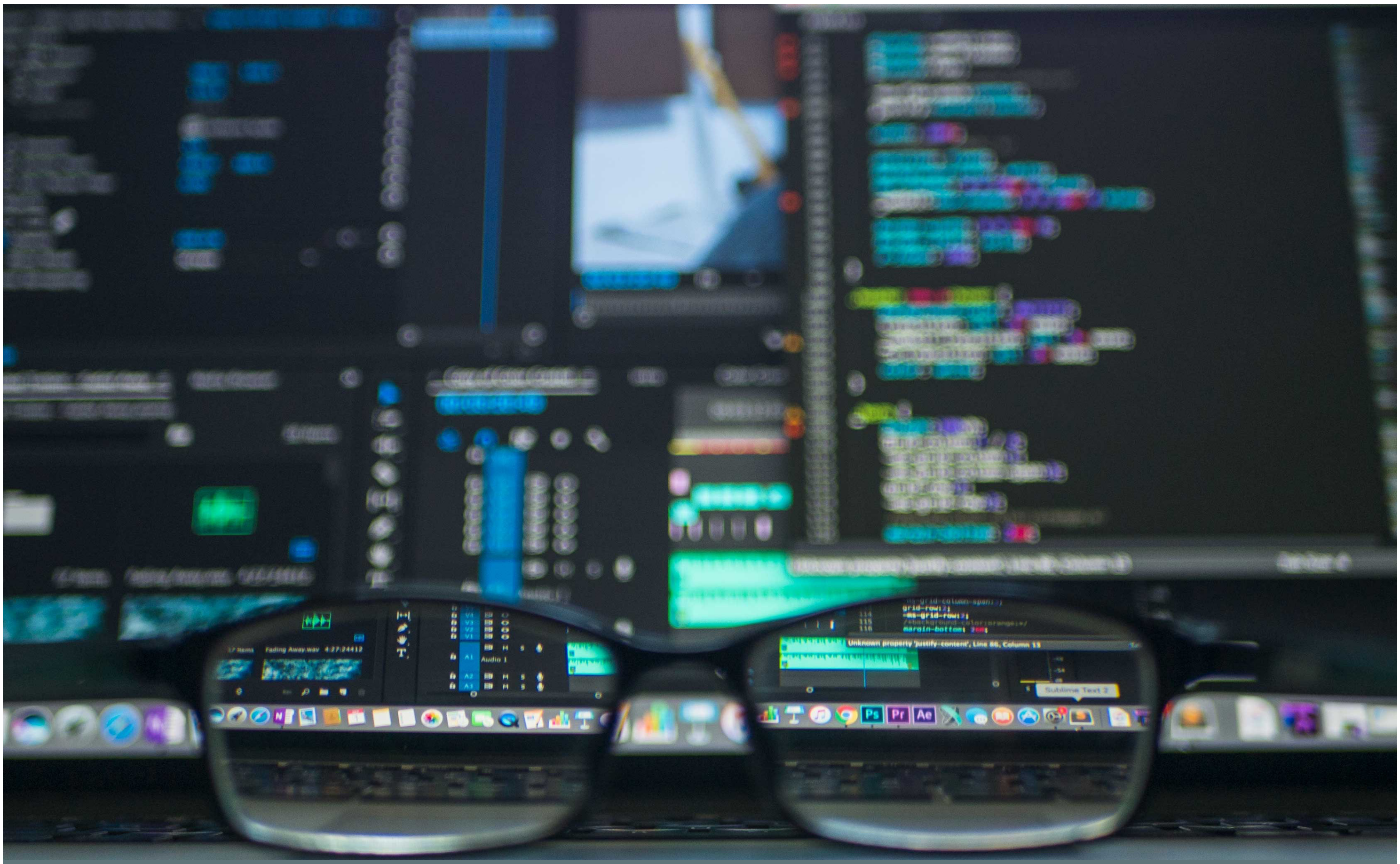


Data Security

Privacy and Architecture in Cloud-Based Services

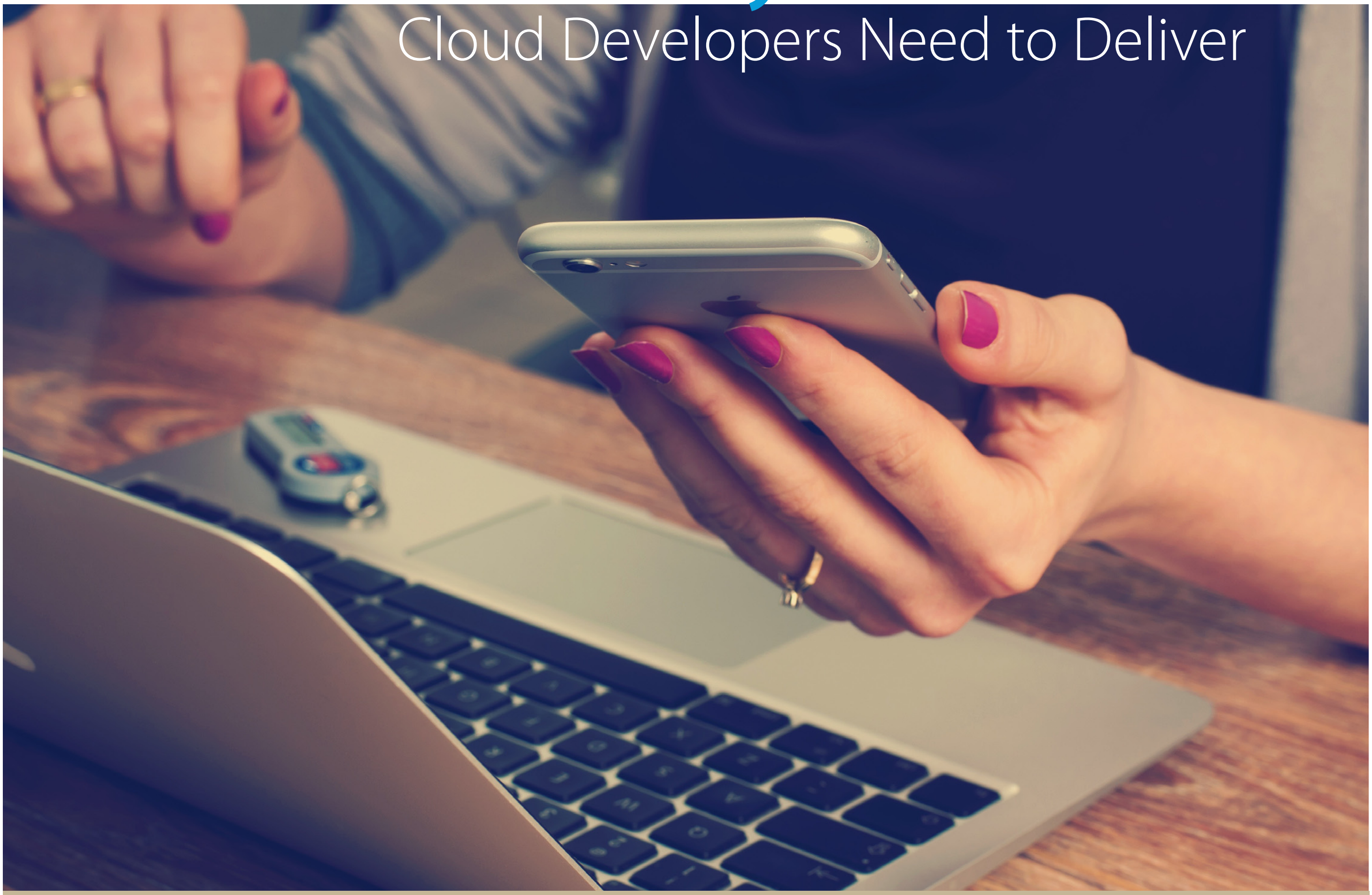
Introduction: All Roads Lead to Cloud

The world is now bracing the waves of technology disruption in almost all industries and at the epicenter of it all is cloud-integrated solutions replacing the existing technology stacks the world is currently using. The transformation and innovation in this cloud computing and smart mobility period is going at a fast speed, from various directions and occur more continuously than ever. Being in cloud business and environment requires organizations to strategize ahead of time, be really involved in customer engagement and provide swift response to maintain survival because undertaking cloud solutions doesn't give you that luxury of time to think, reflect and adjust. At the beginning of the millennium, technology companies could spare 10 years, now the velocity of change has been reduced to only months. The global value of cloud solutions is estimated to be over 3.5 trillion USD and with that, technology companies are challenged with another mammoth obstacle in the form of security issues that arise due to exponentiation of vulnerabilities and threats along with technology transitions. For that reason, cloud providers need to have viable strategies in place to make sure that security issues are addressed adequately and properly to guarantee business continuity.

TimeTec is a renowned global brand that has been providing cloud-based solutions for security and workforce management for various industries around the world. As a cloud-based system developer, TimeTec has fulfilled all the following requirements with the key objective, to maintain customer's trust and confidence in our brand.

19 Core Security Concerns

Cloud Developers Need to Deliver



Customer trust is paramount in building and sustaining a cloud business and a provider needs to be dedicated in achieving and maintaining it by providing strong security and privacy program that takes care of customer's data protection across all solutions, inclusive of data received from customers through the offered services.

1. Architecture and Data Segregation

Services operated and offered in cloud must reside in a multitenant architecture whereby Customer Data access can only be viewed based by authorization assigned by the company. It provides an effective logical data separation through unique Employee Identification that allows access the information based on role privileges. Data segregation has to be carried out by providing separate environments for different functions, i.e for testing and production.

2. Control of Processing

This gives the power back to the customer, ensuring them that the data is only processed when instructed by the customer, throughout the entire chain of processing activities and compliance of the measures implemented has to be subject to audits.

3. Audits and Certifications

On at least an annual basis, all the offered services will have to go through security assessments by internal personnel that includes infrastructure vulnerability assessments and application security assessments.

4. Security Controls

The offered Services made available through Internet Browser or Mobile App must have a variety of security features that are configurable. These controls include, but are not limited to the following:

- User IDs as unique user identifiers to make sure that activities can be traced back to the individual.
- The use of reCaptcha Controls to challenge access after several consecutive failed login attempts.
- To terminate a user session after a period of inactivity.
- To control on password length.
- To match password complexity requirements.

5. Security Policies and Procedures

The Offered Services must be operated in line with the following policies and procedures to enhance security:

- User passwords are kept using a salted hash format and are not transmitted unencrypted.
- User access log entries will be maintained, containing date, time, URL executed or entity ID operated on, operation performed (viewed, edited, etc.) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by a customer or its ISP.
- Logs will be stored in a secure centralized host to prevent tampering.
- Passwords are not logged.

6. Intrusion Detection

The Offered Services must be monitored for unauthorized intrusions using network-based intrusion detection mechanisms by the developer or the third party assigned for that task. The data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) may be analysed for security purposes to prevent fraudulent authentications, and to ensure that the Offered Services function properly.

7. Security Logs

All systems used in conveying the Offered Services inclusive of operating systems, log information to their respective application system log facility or a centralized syslog server (for network systems) will be kept in order to enable security reviews and analysis, and system and application logs will be kept for a minimum period of sixty (60) days.

8. Incident Management

A provider needs to maintain security incident management policies and procedures, and notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by the Developer or its agents of which the Developer becomes aware to the extent permitted by law.

9. User Authentication

All access to the Offered Services through Internet Browser, Mobile App or via API, demands a combination of a valid user ID and password which are encrypted via HTTPS while in transmission. After the authentication is successful, a random session ID is generated and stored in the user's browser to preserve and track session state.

10. Physical Security

If the production data centers used to provide the covered Services is handled by an outside Services, get its Security Processes details known such as this: ***https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf***

11. Reliability and Backup

All networking components, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the covered Services is stored on a primary database server with automated backup using point-in-time recovery features. All the Daily AMI backups will be retained for at least 2 days and weekly AMI backup will be retained at least one month.

12. Disaster Recovery

The Offered Services' production systems must be protected by a multi-tiered disaster recovery plan which provides for backup of critical data and services. A comprehensive system of recovery processes exists to bring business-critical systems back online within the briefest possible period of time. Recovery processes for database, security, systems administration, and network configuration and data provide a roadmap for personnel to make processes available after a service disruption.

13. Viruses

The Offered Services will not scan for viruses that could be included in attachments or other data uploaded into the Offered Services by customers. Uploaded attachments are not executed in the Offered Services and therefore will not damage or compromise the online Offered Services by virtue of containing a virus.

14. Data Encryption

The Offered Services must use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the covered Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum.

15. Return of Customer Data

Customer Data submitted to the Offered Services shall be returned to Customer upon request.

16. Deletion of Customer Data

After termination of the Offered Services, customers can request deletion of Customer Data submitted to the Offered Services, and this process is subject to applicable legal requirements. Customer Data stored on the infrastructure for the Offered Services will be deleted accordingly.

17. Sensitive Data

Important: The following types of sensitive personal data may not be submitted to the Offered Services: financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); information related to an individual's physical or mental health; and information related to the provision or payment of health care. For clarity, the foregoing restrictions do not apply to financial information provided to the developer for the purposes of checking the financial qualifications of, and collecting payments from its customers.

18. Analytics

A developer may track and analyze the usage of the Offered Services for purposes of security and helping the developer improve both the Offered Services and the user experience in using the Offered Services. A developer may share anonymous usage data with its service providers for the purpose of helping the developer in such tracking, analysis, and improvements. Additionally, the developer may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

19. Integration or Interoperation with Other Services

A developer offered services may integrate or interoperate with other services provided by the developer or third parties. The developer also could provide on many platforms and features that allow the users to learn about the products, participate in communities, connect third party applications, and participate in pilots, testing and assessments, which are outside the scope of this documentation. Communication with users that participate in such platforms and features in a manner that must be consistent with the Privacy Statement. Additionally, the developer may contact users to provide transactional information about the offered Services; for instance, through the Account Manager or through system-generated email messages. The developer must offer customers and users the ability to deactivate or opt out of receiving such messages.