5 Critical Cloud Security Questions

Srivats Ramaswami, CTO at 42Q

Published in https://www.securitynow.com/author.asp?section_id=613&doc_id=738700 12/13/2017

Manufacturers deal with sensitive data each and every day. This includes test and quality data, warranty information, device history records, and especially the engineering specifications for a product that are highly confidential. Trusting that data to a cloud-based application or cloud services provider is a major step, and manufacturers need to fully educate themselves about the security risks and advantages of cloud-based software.

Consider the five questions below as a guide to use when discussing application infrastructure and operations with cloud providers.

Question #1: What do you do to keep my data safe?

This is the big one: the most important question a manufacturer should ask a cloud provider.

The answer should be long and multi-faceted. Because no single tool will defend against every kind of attack in any network, cloud providers must deploy multiple layers of defense using: internal systems; protection provided by Tier 1 cloud platforms; and security service providers. All of these elements come together to provide complete protection.

Below are some examples of these layers:

- Physical defense: Cloud platform providers can and should exercise tight control of access to the physical devices on which the software systems reside. In best-case scenarios, independent auditors attest to the safety of this access. This control and documentation must be reviewed on a regular basis.
- Barriers to entry: Firewalls built into the cloud service can limit access to ports managed by the application. Unneeded ports should be blocked so that they cannot be accessed.
- Application password protection: the best-designed cloud applications allow your organization's identity management system to provide authentication and password management, limiting access to your data and following your internal security policies. This should also support two-factor authentication if your internal policies require it. Some of the more advanced systems can also provide an identity management service as an alternative to your internal solutions, if required.
- Application firewalls: Most enterprise-class application designs will include a Web Application Firewall service that uses the latest technology to defend against such things as denial-of-service attacks and other types of malicious access.
- Activity monitoring: State-of-the-art cloud platform providers continuously monitor for suspicious activity that could be the result of hacking or malware. Again, in best-case scenarios, warnings are sent automatically and steps taken to protect the data and the integrity of the platform.
- Malware monitoring: Both the application provider and the hosting platform provider must run active checks for malicious code to ensure each piece of code that is executed matches the published signature for that code. Be warned: this is a step that many providers have not migrated to yet.
- Code standards: Good security starts with good code. Security standards must be included in the system development lifecycle, governing every aspect of the system. Be sure to review the code standards of the application developer.

- Third-party code scanning: The most advanced application providers use a third-party firm to scan code looking for opportunities to improve security and look for known vulnerabilities with each new version of the application. Ask for details about this, as there are many different levels of scanning available; a once-a-year scan is obviously not as valuable as regularly scheduled scans before each new release of software.
- Data encryption: Generally accepted practices for data encryption provide different options for data in different modes: data in transit (being communicated within the system or between the database and your user interface) and data at rest (data that resides within the database and is not currently being accessed).
    - Data in transit can be encrypted using industry standard encryption through the browser. Additionally, APIs that access the data should use encrypted data and include encrypted tokens to increase access control.
    - Encryption of data at rest protects against accessing data from outside the application's control. As the physical access to the system is protected and the data is in password-protected databases, at-rest encryption may not be essential for every customer -- but the question is still worth asking.

Question #2: How do I know that my data can't be accessed by other customers?

There are many ways to ask this question: Do you mix my data with other companies' data? Can other people see my data? What's your database structure for each customer? The answer to each of these is data separation. The system architecture should ensure separation of customer data by customer organization, usually by individual factory or site. This allows even customer administrative tasks such as assigning roles to be limited in scope. While many applications are multi-tenant (meaning the application is shared across multiple customers), transactional data should still be separated by customer factory, meaning there is no commingling of customer data. In other words, your data will be separated from every other customer, giving the highest level of data separation.

Question #3: What do you do to prevent the data from being hacked and stolen?

"Hacking" or stealing data is the number one security concern of most people considering a cloud solution. Note, however, that some common misunderstandings often drive this concern.
According to the latest "Data Breach Investigations Report" from Verizon, approximately 50% of all security incidents are caused by people inside an organization. Good user management and password security policies are the best way to prevent these types of attacks. This is the underlying purpose of application password protection, as described above.

For preventing external hacks and data theft, the system must be architected to prevent as many types of attacks as possible (see above). Also, application providers must use internal personnel and external consultants to run frequent penetration testing. These tests look for common paths that attackers use to gain access to systems through the internet. The tests help ensure there are no doors left open for hackers. Be sure to ask about penetration testing, including both the frequency and the methodologies used.

Question #4: Are there any security certifications from third parties that I should know about?

Rather than trusting the word of a technology provider, many companies have come to rely on third-party certifications for judging the security architecture and processes used by cloud providers. One of the most important of these is SOC 2 certification.
Developed by the AICPA, SOC 2 is specifically designed for service providers storing customer data in the cloud. That means SOC 2 applies to nearly every cloud or "software as a service" company.

So what does SOC 2 require, exactly? It's considered a technical audit, but it goes beyond that: SOC 2 requires companies to establish and follow strict information security policies and procedures, encompassing the security, availability, processing, integrity and confidentiality of customer data. SOC 2 ensures that a company's information security measures are in line with the unique parameters of today's cloud requirements. As companies increasingly leverage the cloud to store customer data, SOC 2 compliance is becoming a necessity for a wide variety of organizations. Consider making it one of your requirements for any cloud provider.

Question #5: How does cloud security compare to on-premises security?

This is a question to ask internally as well as externally. There is a common misperception that a set of servers running on-premises at a corporate office is more secure than a cloud-based application. Owning the hardware and software often gives a false sense of security; most on-premises systems fall far short of the security that the best cloud providers have deployed.
For example, the cloud storage system utilized by my company was designed for 99.999999999% durability and up to 99.99% availability of objects over a given year. That design and those numbers are virtually impossible to duplicate with an on premise solution. In addition, the comprehensive access control described above is nearly impossible to duplicate on-premises. To deploy tools like these in an on-premises environment would require not only large investments in infrastructure, but large teams to manage them too.

Ask yourself: how big is your security team? How much is your budget for security around your manufacturing data? Then remember, the best application providers and data centers have large, dedicated security teams who have implemented automated threat monitoring systems that operate 24x7. In the end, the best cloud software companies have dedicated more time, resources and budget to securing our systems than most organizations are able to provide themselves.

More security today, in the cloud

The security issue for cloud manufacturing software is perhaps best summed up by this quote from LNS Research, a leading independent market research firm:
By moving to the Cloud, security is usually enhanced rather than diminished as Cloud suppliers devote huge efforts to ensuring their underlying systems are as secure as possible and are constantly updated to react to potential threats. No individual manufacturer could devote such efforts, and they should focus on plant security working with their MES and plant software vendors to ensure maximum security and properly maintained systems. Do not get caught out by obsolete and vulnerable systems.