Introduction to software and cloud security on the Cytobank platform

This white paper will outline:

- Advantages of cloud-based analysis platforms
- Things to consider when evaluating the security of cloud-based software
- How Beckman Coulter Life Sciences protects the confidentiality, availability and integrity of data on the Cytobank platform

Introduction

The Cytobank platform enables scientists to leverage machine learning-assisted tools for discovery, as well as hypothesis-driven research. It also serves as a cloud-based platform for structured data management and sharing. Data and results are a scientist's most valuable assets and require high security standards. The fundamental concept of secure software is to make sure your data are free from danger – this could be from hackers, viruses, hardware failure, or a natural disaster. The Cytobank platform includes multiple layers of security to mitigate security threats and meet your expectations, as well as regulatory and trust requirements.

Advantages of cloud computing

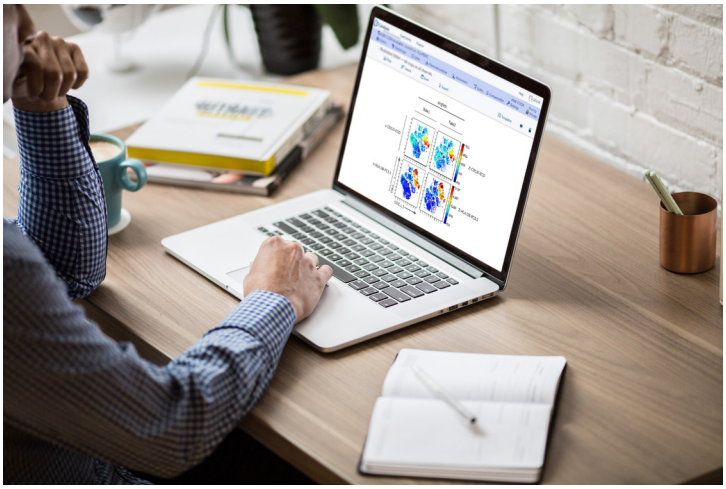
Cloud-based Software-as-a-Service (SaaS) tools like the Cytobank platform enable users to work globally, accessing their data anywhere from any web-enabled device, and can facilitate collaboration across sites. SaaS providers not only develop and provide software, but they also take care of servers, databases and computing resources required. For Cytobank users, this means they don't have to worry about compatibility with their operating system. The Cytobank team at Beckman Coulter Life Sciences takes care of any software updates, patching as well as addressing any vulnerabilities. All of the verification and validation happens behind the scenes in staging environments before release, with no impact to the user. We also have procedures and systems in place to back up data to alternate locations on a daily basis, providing peace of mind to users.

The analysis of high-dimensional single-cell data can be computationally intense, and some algorithms require specialized hardware such as graphics processing units (GPU). On cloud-based platforms, the performance of software is not limited by the user's hardware. GPUs and other high-performance hardware can be provisioned by the service provider as needed. This allows users to access state-of-the-art compute instances without making capital investments in hardware that likely has a short life cycle and becomes outdated quickly. The Cytobank platform can automatically scale up the compute instances as more users sign on at any given time, to maintain performance independently of the capabilities of a user's computer. In addition, long running algorithms don't block computer and analysis software.

Evaluating the security of cloud-based software

You're probably familiar with basic security controls that are visible to you, such as passwords, Single Sign on, and granting access to your data. However, a lot of behind-the-scenes security measures are critical to the security of cloud software.

When evaluating cloud software, it's important to ensure that a rigorous process is applied throughout software design, runs through the development lifecycle, and is actively maintained during operations of the live product. In addition, the process must be formally documented and reviewed by separate teams to remove conflicts of interest, and ultimately validated by external, certified parties.



It is important to keep in mind that robust platforms need to employ Security-by-Design methodologies such as "Threat Modeling." During this process, the platform architecture is mapped out and analyzed to identify weaknesses, as well as vulnerabilities of the codebase and infrastructure. Also, robust platforms need to go through multiple rounds of testing with security tools, such as penetration testing, where a combination of an automated program and an ethical human hacker will attempt to exploit the system using a wide array of approaches.

All this is performed in order to make sure potential vulnerabilities are identified quickly and a plan is in place to mitigate the risk and to fix weaknesses.

But a secure design is not enough. Secure systems are maintained **routinely and actively** – they are monitored continuously with automated behavioral analysis tools to check for intrusion attempts, viruses and malware, and are challenged routinely with bots that attempt to flood systems in order to cause outages. Importantly, the field of software security keeps evolving day by day, and that is why secure platforms also need to have in place automated scans that guarantee constant surveillance to check for newly identified software vulnerabilities.

Secure platforms also require robust manual and automated patching mechanisms, and appropriate remediation timelines based on severity. Security isn't a one-time or periodic activity – it's an actively changing landscape that requires real-time attention.

In addition to safeguarding your data from intrusion, it's important to ensure your data will always be available to you. A trustworthy cloud platform will have a robust Backup and Disaster Recovery process. Data must be securely replicated behind the scenes such that if there's a failure in the storage environment, the data can be retrieved within a defined timeline. Indeed, the failure could come from a disk becoming corrupt, a fire at a facility, an earthquake or other natural disaster. If you are looking for a secure platform, you need to ensure that your cloud software provider has a defined process for restoring data in all these different situations – and depending on the scale of the disaster, the data may need to be restored within the same region, to a new region, or even to a different infrastructure.

It's also important to verify that these procedures are not just theoretical. Does the company test and document the Disaster Recovery process at least annually? Who is the hosting provider that provides the actual computers to run the software? Do they have certifications to ensure the physical and logical safety of your data? All questions you might want to ask in order to ensure you are evaluating a secure platform.

Furthermore, it is crucial to verify that the provider stores your data in ways that are compliant with your institution's or country's policies, as well as to understand whether your data will mix with data from other institutions behind the scenes in the data flow.

And finally, in terms of the integrity of your data, there should be file and database checks at various junctures to ensure integrity of the data, and verification and validation testing should be performed by the software development team to guarantee data integrity with every release.

Protecting confidentiality, availability and integrity of data on the Cytobank platform

We are proud to have a security-first approach to developing and administering our pharmaceutical, government, and academic platforms that run worldwide.

The Cytobank security approach is multi-layered and based on Security-by-Design methodologies, starting with threat modeling to screen the software architecture for vulnerabilities. We have tools for change management when we produce code and peer code review to reduce the risk of introducing errors and vulnerabilities when working on new features. We use static analysis tools to scan code that we produce, looking for vulnerabilities. In addition to this, we leverage network vulnerability tools that scan our operating infrastructure that hosts and runs the software code. The Cytobank platform undergoes regular penetration testing, where a combination of an automated program and an ethical human hacker will attempt to exploit the system using a wide array of approaches. Lastly, we have behavioral analysis tools in place, which look for patterns such as intrusion attempts, hackers trying to spam passwords to log in or trying exploits. Our team is automatically alerted to any attempted attacks.

To ensure data does not get lost and is available whenever it's needed, Beckman Coulter Life Sciences has procedures and systems in place to respond to and restore damage to computer equipment and data loss within a short period of time. Data on the Cytobank platform is backed up on a daily basis. The success of backup operations is monitored by automated systems and Cytobank personnel.

We use automated monitoring tools to detect and respond to any disruptions, capacity issues, and system failures. Disasters come at different levels, ranging from a small disk failure in one availability zone – when we just need to recover the disk -- to an earthquake that takes out a whole data center, when we restore the data using an alternate data center location.

Whether a natural disaster or a hardware failure, we have protocols in place and defined recovery time objectives to restore the data in alignment with customer expectations based on the amount of data and the type and scale of disaster. Our disaster recovery plans are actively tested on a regular basis so we can be confident they will work if needed.

Anytime you upload files to the Cytobank platform, they go through an antivirus scan. Uploaded files are then also scanned for data integrity. The Cytobank platform supports standards in the flow cytometry community. Towards this goal, we have implemented a file quality control system to provide more information to you whether or not your files match the FCS standard specifications. Processing software upstream of Cytobank can shift the bytes and how the data is written in an FCS file, and this can result in bad data problems in the analysis pipeline. We do not want to present you with bad data at the end of your analysis workflow. Even if we didn't introduce the change, we want to make sure you're aware of any integrity issues as soon as you upload the files. To safeguard against any changes during the upload process, we have these checks in place just to make sure you're getting good data at the end.

While product quality is not directly related to security, it is closely related. As a user you need to have trust in the analysis platform you use. For the Cytobank platform, we perform informal verification and validation in parallel with development, which helps us deliver new features and improvements on time and with high quality. When development has finished, we perform formal verification and validation testing to guarantee data integrity with every release.

At Beckman Coulter Life Sciences, we're proud of our mature and comprehensive security process that safeguards your sensitive data at many levels. To learn more, please review our Overview of Cytobank Platform Security Systems and Processes White Paper.

22.05.4886.FLOW