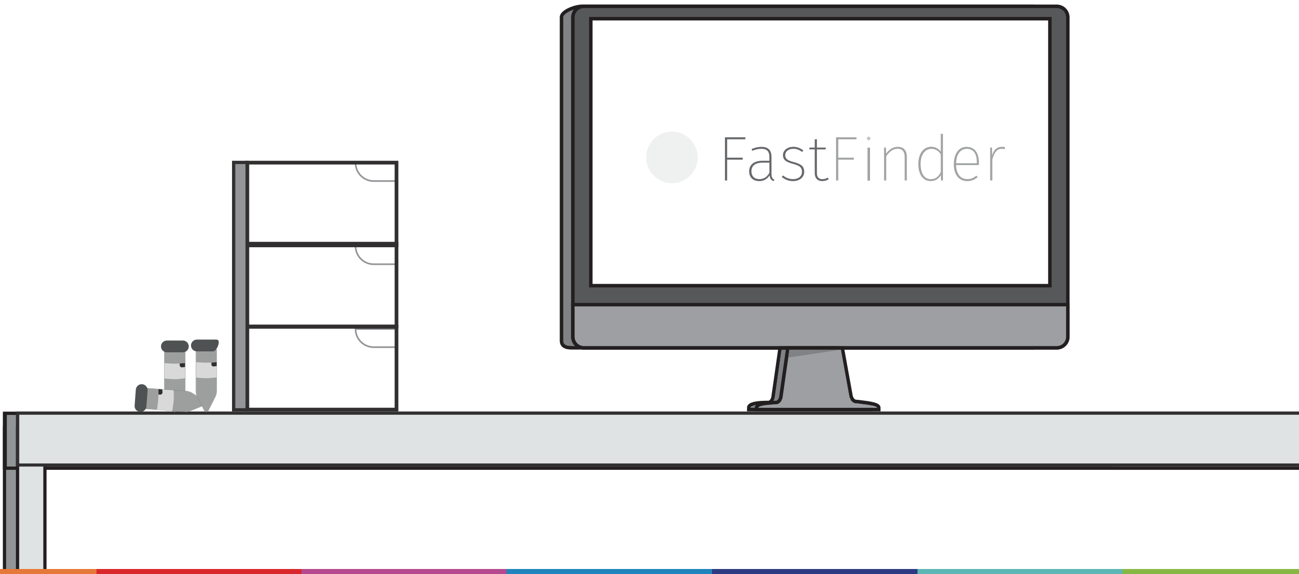
» *FastFinder: a secure and reliable platform*

Importance of security in Molecular Diagnostics

» In a molecular testing setting, labs are dealing with confidential research or healthcare related data. Data security matters highly in both in a research setting where research results and intellectual property need protection, and a clinical setting where labs deal with patient sensitive data, consent, and specific rules and regulations apply to Personal Health Information.



FastFinder is secure from the ground up

» In this brief overview, we'll discuss how the FastFinder platform was built with state-of-the-art security in mind. Built from the ground up for clinical use, FastFinder provides:

- A sound and proven security model with multiple layers of security
- Regular audits and security checks
- Implementation of industry guidelines and best practices
- Partnership with a best-of-class infrastructure provider
- Audit trails and change validation

For a more detailed discussion on UgenTec's secure platform, please consult the White Paper on UgenTec's Hosted Solutions.

Multiple layers of security

The UgenTec software maintains three layers of security, ensuring industry-grade security across the platform. All communication between the different modules of the FastFinder system is encrypted through SSL[1] as a security layer, combined with the OAuth2 protocol[2] as an authentication layer. On top of those, both the end-user facing applications and the centralized administration module provide an extra authorization layer, which allows specific user actions to be assigned to specific users through user roles.

Additionally, all data storage has additionally been configured to be encrypted at rest, thanks to features provided by Microsoft. This is not only applicable for file storage, but also the underlying data storage of databases is encrypted in the same way.

[1] Secure Socket Layer

[2] OAuth 2.0 is the industry-standard protocol for authorization

Externally audited procedures and infrastructure

UgenTec has documented procedures in place that govern its development and production infrastructure, its hosting and deployment process, its security management including user access and entitlement management, intrusion detection, and more. Moreover, UgenTec regularly tasks an independent, external party to perform a full set of manual & automated penetration tests on the UgenTec software solution.

Implementing relevant security guidelines

specific rules, guidelines and best practices apply to PHI (Personal Health Information). UgenTec ensures that its platform supports compliance with guidelines such as GDPR[3] , APP[4] , HIPAA[5] , and general industry best practices. Moreover, to ensure the highest security standards, UgenTec also implements the CAP[6] /CLIA[7] security guidelines.

Top notch hosting professional partner

In selecting a partner for its hosted solutions, UgenTec has chosen MicroSoft Azure, a PaaS (Platform as a Service) provider that's highly secure by design, and that has a track record of providing services to software companies that manage and process PHI. For example, MicroSoft has a long history of developing highly secure & safe software for enterprises and medical device industry that allow customers to be HIPAA compliant. For a full list of their compliance & quality efforts, navigate to the Microsoft Azure trust center, at https://www.microsoft.com/en-us/trustcenter/cloudservices/azure.

[3] The General Data Protection Regulation (GDPR) is a European piece of legislation which covers personal information and how consumers and businesses interact with it

[4] The Australian Privacy Principles (APP) are part of the Privacy Act law that governs privacy of data in Australia

[5] The Health Insurance Portability And Accountability Act (HIPAA) is a USA piece of legislation which provides security provisions and data privacy, in order to keep patients' medical information safe

[6] College of American Pathologists

[7] The Clinical Laboratory Improvement Amendments (CLIA) are United States federal regulatory standards that apply to all clinical laboratory testing performed on humans in the United States, except clinical trials and basic research

Audit trails, change documentation, and robust authentication and authorisation

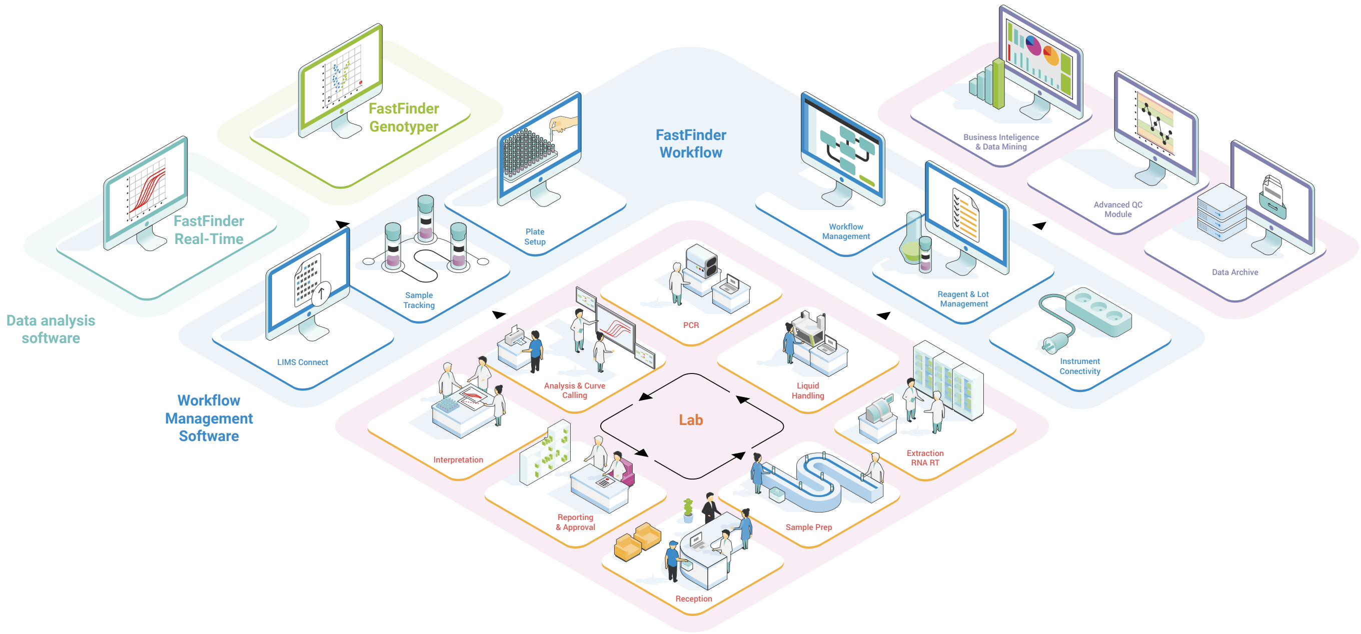
The FastFinder platform is built with a user-centric authentication and authorisation model, which enables features like 2-step validation (where a result by 1 operator has to be confirmed by a second scientist) and audit trails. For example, whenever a user overrides an assay result in the software through the "Resolve" function, she/he is required to enter a rationale, which is stored in the audit trail for future reference.

CFR 21 Part 11, a set of regulations put in place by the United States Food and Drug administration, describes the controls it requires to be in place to make sure electronic data is subject to signed document audit trails, record keeping, and access controls.

Conclusion

» With FastFinder, you get access to a powerful platform that is built from the ground up with quality and regulatory compliance in mind. Equally, you'll be able to rely on an experienced team of experts that will help you with the software portion of your IVD submissions to regulatory instances. And you'll be able to rest assured that UgenTec's FastFinder platform supports your lab or diagnostic kit provider in its compliance needs.

UgenTec



FastFinder

Belgium office (Hasselt)
Kempische Steenweg 303/105
Hasselt 3500
Belgium

US office (Boston, MA)
One Mifflin Place, Suite 400
Cambridge, MA 02138
USA

www.ugentec.com

info@ugentec.com