HYTRUST

Case Study

# iQues:
# The Road to EU GDPR Compliance

The new EU General Data Protection Regulation (GDPR), came into force on May 25, 2018, aimed at strengthening and unifying data protection rules for all individuals within the European Union. Among the changes are stronger consumer consent and mandatory breach reporting within 72 hours where there is a significant risk to data subjects. Failure to comply could lead to hefty fines of up to four percent of global annual revenue.

For any U.S. company that has a web presence, it must treat European residents' data in a way that ensures appropriate security, "including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures" to conform with the regulation.

iQues is a US-based solutions provider that solves business problems, enhances operations and streamlines processes by aligning an organization's vision with a tailored, powerful technology strategy. iQues helps organizations assess readiness and deploy solutions to meet GDPR compliance requirements.

For many of IQues' clients, GDPR is not only a matter of compliance, but essential to maintaining their reputation if a breach would occur.  Recently, iQues, a managed service provider and strategic partner, leveraged the HyTrust suite of products to satisfy the compliance requirements for one of its valued clients.

The business of one of iQues' clients revolves around risk management, as a multinational specialty insurance company with more than 30 offices around the globe. This organization cannot risk their reputation by failing to perform due diligence in IT security. Their reputation, and iQues' as their managed service provider, relies on their commitment to compliance. It is a business strategy therefore, to not only proactively comply with GDPR, but to show diligence in their approach to data protection, and encryption is their insurance.

By addressing data-at-rest encryption technology with HyTrust KeyControl, they were able to add the extra level of security and demonstrate competence when handling personal data.  Combined with properly managed security protocols and escalation procedures, iQues' client is assured that their approach and methodology is not only satisfactory, but a strong model to follow for personal data protection.

Until now, a lot of the traditional investments made by the CISO have focused on keeping the bad guys out, through enhancing firewall and perimeter capabilities and ensuring the secure configuration and hardening of their systems. These are still important steps to take in a security strategy, but attackers are now very familiar with those controls and they look to circumvent them.

IQUES

"iQues is a US-based solutions provider that solves business problems, enhances operations and streamlines processes by **aligning an organization's vision with a tailored, powerful technology strategy**. iQues helps organizations assess readiness and deploy solutions to meet GDPR compliance requirements."

One of the ways attackers will do this is by hijacking user accounts that are within the environment, such as using phishing emails to compromise credentials. Once they can masquerade as a user, they have full access to that user's system privileges. The techniques that attackers use to hijack user accounts are usually under the radar of the perimeter and more traditional security controls.

Monitoring can provide insights, but companies need to be looking on the inside - how communications are happening on the network, how systems are talking to each other and most importantly what are the users doing on the network. This is often overlooked. HyTrust KeyControl can integrate with a variety of hypervisor technologies allowing easy deployment of VM encryption functionality.

By encrypting VMs at the hypervisor level, data residing on those servers is protected against unauthorized access to the underlying storage layer, as the entire VM disks are encrypted and only get decrypted during VM start-up. Furthermore, by using HyTrust, VMs can be migrated between different hypervisors or between on-premise and cloud virtualization technologies in an encrypted state, thus enabling secure VM migration and protecting the VM data in transit.

Enabling Virtual Machine encryption allows organizations to protect their data. Leveraging HyTrust KeyControl, iQues was able to protect the data with an easy to deploy product and simplified administrator interface. And as the client transitions from provider to provider, they have the ability to enable encryption across a wide range of platforms, reducing overhead and administration costs while strengthening data security.

"Enabling Virtual Machine encryption allows organizations to protect their data. Leveraging HyTrust KeyControl, **iQues was able to protect the data with an easy to deploy product and simplified administrator interface**."

To learn more, visit [www.hytrust.com](http://www.hytrust.com) or [www.iques.com](http://www.iques.com)

**HyTrust**
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
1-844-681-8100 (US)
1-650-681-8100 (Intl.)