

Unraveling the Quandary of Access Layer versus Storage Layer Security

InfoSecurity – February 2019

Dr. Jans Aasman was quoted in this article about how AllegroGraph's [Triple Attributes](#) provide Storage Layer Security.

With horizontal standards such as the General Data Protection Regulation (GDPR) and vertical mandates like the [Fair Credit Reporting Act](#) increasing in scope and number, information security is impacted by regulatory compliance more than ever.

Organizations frequently decide between concentrating protection at the access layer via role-based security filtering, or at the storage layer with methods like encryption, masking, and [tokenization](#).

The argument is that the former underpins data governance policy and regulatory compliance by restricting data access according to department or organizational role. However, the latter's perceived as providing more granular security implemented at the data layer.

A hybrid of access based security and security at the data layer—implemented by triple attributes—can counteract the weakness of each approach with the other's strength, resulting in information security that [Franz](#) CEO Jans Aasman characterized as “fine-grained and flexible enough” for any regulatory requirements or security model.

The security provided by this semantic technology is considerably enhanced by the addition of [key-value pairs](#) as JSON objects, which can be arbitrarily assigned to triples within databases. These key-value pairs provide a second security mechanism “embedded in the storage, so you cannot cheat,” Aasman remarked.

When implementing HIPPA standards with triple attributes, “even if you’re a doctor, you can only see a patient record if all your other attributes are okay,” Aasman mentioned.

“We’re talking about a very flexible mechanism where we can add any combination of key-value pairs to any triples, and have a very flexible language to specify how to use that to create flexible security models,” Aasman said.

Read the full article at [InfoSecurity](#).