information management

NEWS

Big Data Executive Offers Insights on New Directions for 2017

Kon Leong

JAN 3, 2017 6:30am ET

ZL Technologies is a provider of big data management solutions that help its corporate customers better perform tasks like eDiscovery, compliance, records management and analytics.

From his vantage point as ZL's CEO, Kon Leong has offered up several compelling predictions for new directions that the information technology industry will take in 2017.

The industry will look at the cloud from both sides now.

While migration to the cloud will maintain momentum, some cloud business will start drifting back to, and get anchored on, the ground, while others will evince hybrid qualities between "Heaven" and "Earth." This movement will be especially pronounced in the large enterprise applications space.

One reason is economics: Beyond a certain size/volume, on-prem may be more economical than cloud.

But another is infrastructure manageability. Each cloud deployment effectively becomes a silo, making management information across clouds much more difficult.

When the data becomes too critical to the enterprise, or when the data analytics becomes too complex or demanding, it may make sense for the data to stay on the ground. This trend may be further accelerated by security breaches in the cloud.

Unstructured analytics of external and internal data will converge.

Unstructured analytics will begin to distinguish between external and internal data. Thus far, much of analytics has focused on external data, e.g., for marketing insights. Going forward, the treasure trove of internal unstructured data, such as email, files, and social media, promises to yield far more valuable insights on the characteristics and dynamics of an enterprise's human players. It should be noted that much of this internal data is already under governance functions, e.g., compliance.

Insider threats to data security will grow.

The insider threat has emerged as a legitimate danger to companies with sensitive information spread across their network. In the past, organizations have been preoccupied with defending against the anonymous hacker, and so have focused efforts on maintaining the integrity of their firewall to prevent an external breach. While this is still important, the modern threat to data security often wears a familiar face. Employees and contractors are often most knowledgeable about where important files lie within the enterprise, and how to access them, making them a liability if files are not properly managed.

Unstructured analytics will undergo a sea-change.

Practically all unstructured analytics today use the “sandbox” architecture, which makes governance functions very difficult. Going forward, analytics will begin taking a more holistic approach which leverages existing governance capabilities such as e-discovery, compliance, records management, etc.

Analytics and information governance will converge.

Analytics and Information Governance will begin convergence from both directions. Analytics will begin to factor in governance capabilities, in order to mitigate compliance and litigation risks. From the other direction, governance of enterprise data will begin to add unstructured analytics.

Control of content control will be emphasized over network security.

Companies need to be able to map files across the enterprise to identify exactly where sensitive information lies and regain control of their data. Absolute control of content is the only way to protect data from within. Fortunately, file analysis and behavioral analytics have made large strides, giving CSOs, CIOs, and IT new tools to secure sensitive information and detect suspicious behavior within their network. Accelerated content analysis can offer organizations insight into where their most important data lies—personally identifying information, credit card information, proprietary property—which can then be locked down or quarantined. Access privileges can be updated, and ongoing remediation policies standardized. Communication patterns and file access can be analyzed to detect unusual behavior and stop potential security hazards in progress.

Mobile Version