Ten Things That NetIQ Data Access Governance Can Do for You

Securing sensitive data from unauthorized access is a universal objective. But unfortunately, most organizations tend to focus on protecting regulated data, with less concern for the sensitive information in le-based data. That's where NetIQ Data Access Governance (DAG) can help.

The traditional focus on data security has been on records stored in databases. Known as "structured data," this data is a primary source for personal identi able information (PII), health records, account numbers, passwords, and other con dential information that, when accessed by unauthorized individuals, can have potentially devastating consequences.

An equally vulnerable, but historically less emphasized data set, is "unstructured data" or le-based data—the word processing, spreadsheets, media, virtual images, and other les that make up more than 80 percent of an organization's stored data. Unstructured data can also contain sensitive information that needs to be protected. In some cases, it could be PII, but it can also be the "crown jewels" of a company's data. Excel les might contain pro t and loss data, Word les might include legal information, and PowerPoint les might include sales forecasts.

NetIQ Data Access Governance by OpenText helps secure access to sensitive unstructured data in many ways. Here are ten.

1. Reduces risk. Through the reporting capabilities built into NetIQ DAG, you can determine where sensitive and high-value les are being stored and who has access to them—providing the details you need to take corrective action.

2. Performs analysis and provides insight into data locations. The reporting capabilities provide extensive details on the les themselves and answers such questions as: "What les are being stored?" "When was the last time a le was accessed?" "Who owns the le?" "Who can access this le?" and "How is a user's access to a le derived?"

3.