Introduction . . . . . 1 . . . . .
Comparing Risk: Structured and Unstructured Data . . . . . 1 . .
Data Access Governance . . . . . 2 . . . .
Detailing DAG Requirements . . . . . 3 . . .
Coalescence with Identity Governance . . . . . 4 . .
The OpenText Approach to a Comprehensive DAG Solution 4

H

Analysts have concluded that the “elephant in the room” is the lack of governance for organizations’ unstructured data, that is, le-based data that make up more than 80 percent of organizations’ total data. When it comes to access to sensitive les in unstructured data, the NetIQ Data Access Governance by OpenText™ solution provides an integrated product approach to reporting, correcting, and certifying proper access through access reviews.

Introduction

In recent years, data breaches have been the subject of numerous news stories. In fact, the frequency of data breaches and the resulting exposure of sensitive information has become so common that these stories now tend to focus on the most extreme occurrences. Lest we forget or miss some of these reported incidents, organizations such as Business Insider, Wired, Digital Information World, and others concluded the 2018 calendar year with their rankings of the worst cases of data breaches for the year

Data has value to both the organization that owns it as well as the outsiders that want to access it and exploit it. But unauthorized access to data is not always based on nefarious intent. For example, access permissions are assigned temporarily but not removed, roles change, group memberships are modi ed, and before you know it, an internal user has access to data he or she should not have

With the rami cations of unauthorized access ranging from loss of consumer con dence to severe nes, the securing of data through access controls is a high priority objective of all organizations.

When it comes to access to sensitive les in unstructured data, the NetIQ Data Access Governance solution provides an integrated product approach to reporting, correcting, and certifying proper access through access reviews.

Comparing Risk: Structured and Unstructured Data

For analysts, security personnel, and legislators, the traditional focus on data security has been on the records stored in databases. Known as “structured data,” this data are 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. To protect PII, health information, and other sensitive data, governments have established privacy regulations for which organizations must be in “compliance” or face potentially severe consequences. For this reason, organizations are required to periodically perform “access reviews” of who can access sensitive data.

Most applications that have structured data on the back end have inherent security mechanisms in place relative to the application. NetIQ Identity and Access Management (IAM) by OpenText™ and NetIQ Identity Governance and Access (IGA) by OpenText™ software vendors provide software that authorizes, validates, and reconciles access controls to these applications, inherently controlling access to the data.