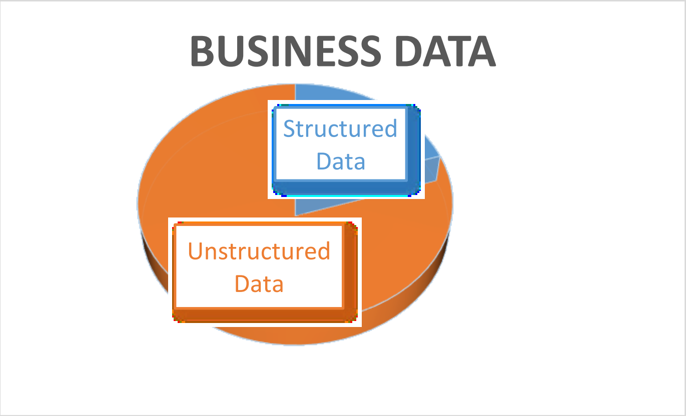
Unstructured Data Shield: The first ever protection designed for unstructured data



It may come as a shock that over 80% of the data today are complete unprotected and unmanaged, but it is the reality. Unstructured and semi-structured data, counted over 80% of all the data in an average organization, and projected by IDG to grow to 93% by 2023, is competed exposed without protection today. Those data therefore is the primary target of hacking activities and most often the direct or indirect source of the damage caused by cyber breaches.

A critical characteristic of unstructured data is that it contains a company's sensitive data or IP and probably represents in some form or another the sum total of all the knowledge that has been created or collected in the organization and current business activities. If this data was leaked it could be detrimental to the company's image and the valuation of IP, or could even result in heavy fines if you are subject to legislation like GDPR, Gramm-Leach-Bliley Act (GLBA) and New York State Department of Financial Services (NY DFS), Health Insurance Portability and Accountability Act (HIPPA) as well as Payment Card Industry's Data Security Standard (PCI DSS), and so on.

Unstructured data needs to be handled securely and this should be part of any data protection policies. "Too big to handle" is no longer a valid excuse to not manage unstructured data. Yet, those data in most cases are completed exposed with patchy solutions like centralized storage. If this situation sounds unacceptable, we at APF agrees and that is why we built Unstructured Data Shield (UDS), a first ever complete solution purposely for the unstructured data protection and management.

Unlike structured data, which is typically programmatically correct and machine readable (e.g. a database), unstructured data includes human created data like email, text, spreadsheets, video, pictures, and those created by machines like logs, and data from surveillance instrument and sensors. Those data are in human readable format and stored everywhere from heavily protected servers to laptops that travels everywhere, one of the reason that makes the unstructured data extremely vulnerable to hacking and phishing but nearly impossible to protect, until now.

The difficult to protect unstructured data is partially due to the nature of the data. It comes in different form and format and are used by various applications, and could be shared and copied freely onto many devices that belongs to different users. The centralized storage solution like Sharepoint protects only one copy and only while it resides in the storage. Once the data is downloaded to the user's device, the protection is off completely. To deal with those problems, UDS is built with the concept that the best protection is the protection of the data itself, not just the means to get to them.

Truly a disturbing technology, UDS is first ever a completed solution to protect and manage the unstructured data throughout the entire life cycle from the creation to elimination, without extra burdens on users or lose productivities. While unstructured data is often being updated and shared with many copies and versions, UDS is able to identify each copy as the same data and applies same access policies. No matter where, no matter when, the data is always being encrypted with its own random key, not password, which leaves no possibility of brutal force attach. If anyone think a password that human can remember could stop hackers, think again. A 10 character long password may last days under brutal force attack at the cost of a few dollars from cloud providers.

UDS doesn't stop at protection. It provide unprecedented manageability to the unstructured data

1. Data classification
2. Establish and Manage data ownership
3. Enforce access control in real time on every data access using organization-wise access policy
4. Ensure the same access control on all the copies of the same data
5. Tracking every data access,
6. AI powered data access monitoring and analysis
7. Maintain record of every data change
8. Eliminating access to every copy of same expired data

UDS does not only stop the data leak from external thread, it deterrents internal misuse too. By the count of Verizon, nearly 30% of the breach in 2018 started from within the organization. The centrally managed access control policies gives the organization the power to align data access with organization-wide governance policies or regulatory rules, which essentially build a data firewall not only around the organization but also within the organization. Record of actions makes the data access transparent. There is no better way to discourage disgruntled employee or simply opportunist from stealing the data for personal gain.

For any CEO or CIO who still thing protection of their 80% data in unnecessary, they should think again before the next data breach happens. With the available of UDS the chances for stake holders to accept the excuses like "we have done all we can" or "it is out of our control" is considerably remote.