

Unstructured Data Shield: The first-ever management and protection solution for unstructured data

APF Technologies, LLC

<https://www.apftechnology.com/enterprise>

Leaving unstructured data, mostly in the form of files and emails, unprotected is no longer a nuisance .

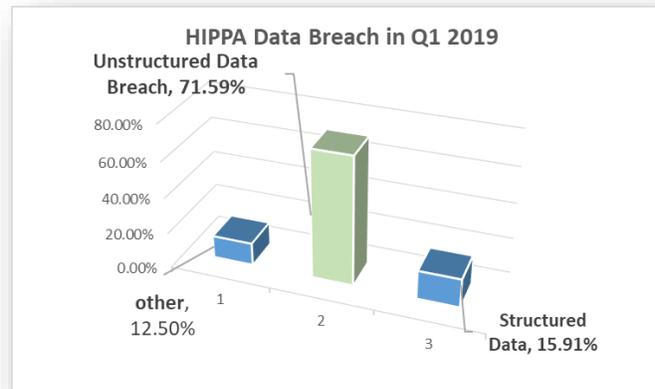


Consumer data loss today will seriously damage a business's financial wellbeing and reputation with customers, and if negligence is found, the jobs of top executives are at stake, thanks to a string of consumer privacy protection laws around the world, including GDPR, HIPPA and the upcoming CCPA. The Capital One breach, which is expected to cost the firm **\$150M** in 2019 alone, is putting the consequences of data loss on full display.

Unstructured data that contains consumer information are vast and being actively used

everywhere by everyone, from call centers to back offices to AI and ML, and even third-party contractors. Because of commercial value and legal reasons, those files are also kept for a long time. The traditional way to protect small amounts of unstructured data with limited access scope like virtual desk top (VDT) becomes cost prohibitive and not practical, let alone it still leave many holes. The Capital One incident revealed that VDT doesn't help at all in that case. As database security has become more heightened, the unstructured data is quickly becoming the primary target of hacking activities. To further complicate the matter, regulations require companies not only to stop the data loss to outsider, but also unauthorized access by internal users.

The HIPPA data breach report in Q1 2019 shows that 72% of data loss is from unstructured data. Still, most businesses don't include unstructured data management and protection as part of any data protection strategy. They simple rely on traditional perimeter defenses and "best practice" advice. Nearly all companies have no way of knowing how many files contain customer information and who owns and accesses those data, let alone how to protect them. If this situation is unacceptable to the board, we at APF Technologies agree. Unstructured Data Shield (UDS) is built to provide visibility of the information that needs protection in the environment, and protect



those data anywhere at any time to stop data loss and unauthorized access, while ensuring businesses stay compliant with regulations, by providing the complete access history.

UDS builds the protection on the foundation of UDS's innovative, patent-pending design to manage the unstructured data (files) as assets. UDS tags the data permanently so it can trace every access of the data and all its copies, a sticky problem unique to unstructured data. UDS is designed to

1. Classify data based on the sensitivity of the content
2. Establish and manage data ownership
3. Enforce access control in real time on every data access using organization-wide access policies
4. Track every data access
5. Utilize AI-powered data access monitoring and analysis

Truly a disrupting technology, UDS manages and protects the unstructured data throughout their entire life cycle, from creation to elimination, without extra burdens on users or loss of productivity. While unstructured data are often being updated and shared through many copies and versions, UDS is able to identify each copy as the same data, to apply the same access policies to each version of the data. No matter where, no matter when, the data are always being encrypted with their own random key - not passwords - which leaves no possibility of brute-force attack from hackers. If anyone thinks a password that a human can remember could stop hackers, think again. A 10-character long password may last days under brute force attack at the cost of a few dollars from cloud providers.

UDS does not only stop the data leakage from external threats, but it also deters and prevents internal misuse. By the count of Verizon, nearly 30% of the breaches in 2018 started from within the organization. Audit trails make the data access transparent. There is no better way to discourage disgruntled employees or simple opportunists from stealing the data for personal gain.

UDS makes being compliant with GDPR and HIPPA ridiculously easy. The data covered by the regulation are categorized and classified when they enter the system so they are protected by UDS's access control, and the entire access history report is just a few clicks away.

For anyone who still thinks the consumer protection laws have no basis or they may just get lucky, it is time to think again before the next data breach happens. With the availability of UDS, no business leader and board should put consumer privacy and their own financial wellbeing in jeopardy.