

at the edge

by Chris Aroid



Protecting PII

Sensitive data exists in the IT architecture of every industry. The digital revolution has come and gone, leaving the former dangers of physical paper trails to now reside on the desktops, laptops, workstations, servers and databases of companies both large and small.

This data—better known as personally identifiable information—poses a significant security risk to a company's IT infrastructure. Two of the biggest targets of this type of privacy breach are higher education and healthcare. They are historically more open—and less secure—networks and are natural victims of perpetrators seeking to profit off the PII of others. Naturally, their systems contain Social Security numbers, personal health information, credit card numbers and multitudes of personal identifiers that can be leveraged by cyber criminals.

Strong business processes are critical for success, but enabling them effectively and efficiently requires the technology known as data loss prevention. There are two schools of thought when it comes to protecting sensitive information: data-at-rest, DLP solutions to protect data stored in use or at rest on computers, and data-in-motion, DLP solutions to protect data in transit.

These technologies complement each other but solve different problems. Data-at-rest is now common within enterprises because of its ability to find and protect data at its source. This allows for secure actions to be taken before the opportunity for compromise exists, whether it is physical (theft or loss) or digital (encrypted tunnels) where the data can no longer be breached. Data-in-motion is limited to preventing data from leaving the organization when users break policy and send unprotected information outside the perimeter using a known form of communication, such as e-mail.

Additionally, only a small percentage of data breaches since 2005 have occurred as the result of a breach that would have been prevented by data-in-motion. Thus, if an enterprise sought to take a proactive, corrective stance on sensitive data, data-at-rest would be the preferred solution.

In higher education, with massive, sprawling campuses and community college consortiums, information security officers have fully realized the need for root source remediation. When sensitive data is found, this approach encourages an organization to shred it, redact it or secure it. More advanced technologies also provide centralized reporting on aggregate risk exposure.

Analysis and trends from this information can help organizations determine if their policies are sufficient and effective. By taking a data-at-rest approach to sensitive data, they are ensuring the safety of PII for involved faculty, staff and students. Enterprise DLP solutions like Identity Finder focus on data-at-rest because they do not just point out the problems; they help solve them proactively.

"We chose Identity Finder because it offers us the greatest ability to not only find personal information at the source, but also easily and quickly clean our systems so that we are confident

those data won't leak outside the university," said Tom David, chief information security officer at Indiana University.

Within higher education or healthcare, a typical breach could be as innocuous as a lost laptop or as malicious as a botnet targeting a network through brute force. Depending on the employee culture, the lost laptop could actually be far more dangerous than the botnet because it could contain student Social Security numbers, dates of birth or other types of PII.

Because the data-at-rest model is not a background process, but a visual interface for finding and educating the end user on the existence of sensitive data, it empowers people to actively search for and secure the data on their own time.

The data-at-rest approach is both informative and proactive in this way.

Most universities are not as strictly bound by legislation specific to securing sensitive data, but state notification breach laws—including FERPA and Massachusetts 201 CMR 17.00—mandate they take proactive steps. Healthcare organizations, on the other hand, are required to follow federal guidelines specified in HIPAA. The requirements to ensure the protection of personal health information make a DLP solution much more important.


The preventative method of data-in-motion risks the compromise of data every time it is accessed. Data-at-rest secures the PII so there is nothing to compromise in the first place.

Another feature of data-at-rest products is the option to run these types of scans without agents. A security administrator could search his local file system, remote file systems, explore remote databases, crawl websites and even scan e-mails all from one central point.

Centralized remote searches are a boon to healthcare environments that consist of thousands of devices storing millions of patient records. There is no need to put a monitor on every device that might have PII on it, which greatly reduces the implementation costs incurred when compared to a data-in-motion solution that typically requires individual machine agents.

These two industries might have very different approaches to PII, but their needs are the same. The end goal is to make sure the sensitive data is made unavailable to the people without authorization. Once it is found, the data-at-rest model provides a plethora of options for security over the data-in-motion solution of blacklisting. Solutions offer complete control from the end user to the administrator. Shredding, redaction, encryption, quarantining and even whitelisting actions can be offered or restricted however an organization sees fit.

Shredding is a critical feature because, as the FTC says, "if it's not in your system, it can't be stolen by hackers."

The data-at-rest solution provides options and scalability, and as higher education and healthcare have found, it is this flexibility that truly provides the most immersive and secure experience. 

Chris Aroid is the vice president of Identity Finder LLC.