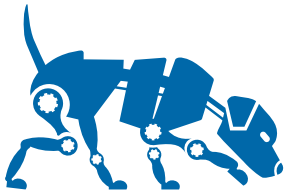
Data Loss Prevention: Data-at-Rest vs. Data-in-Motion

Despite massive security efforts in place today by large organizations, data breaches continue to occur and identity theft is on the rise. Something has to change. This paper compares the two primary prevention strategies to demonstrate the strength and value in securing Data-at-Rest and Data-in-Motion. We analyze historical research to highlight the true nature of data breaches and help you determine which strategy is right for you. In nearly every comparison, from cost to effectiveness, Data-at-Rest solutions emerge as the stronger data loss prevention strategy.



identityfinder

Executive Summary

The dramatic rise of identity theft has placed tremendous focus on data loss prevention (DLP) technologies. The FTC reported 9 million Americans have their identities stolen each year.[1] In response, federal and state governments as well as industry regulators have enacted laws requiring organizations to improve their handling of sensitive data and have stipulated monetary penalties for organizations that violate these laws. Additionally, the cost of data breaches has risen as breached organizations must often provide credit monitoring services for affected individuals while also suffering reputational damage from state mandated public disclosures.

Despite increased focus and costs, many organizations are unclear exactly what problem they are trying to solve. Managers often try to protect data while it is in motion, going off gut intuition, while in fact their institutions are suffering from exposures of unsecured data at rest. Two technology solutions now exist to help with this problem: Data-at-Rest DLP solutions to protect data stored 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 becoming much more common within enterprises because of its ability to find and protect data at its source. Data-in-Motion is more widely implemented but its strength is in preventing data from leaving the organization when users break policy and send unprotected data.

While Data-in-Motion is probably more common, only a small percent of data breaches since 2005 have occurred as the result of a breach that would have been prevented by Data-in-Motion. This white paper performs an analysis of Data-at-Rest and Data-in-Motion DLP solutions, including historical research, to present the case for a DLP strategy and solving the data leakage problem at its source.

Data Loss Prevention Technologies

The widespread usage of Data-in-Motion technologies has historically resulted in them being synonymous with Data Loss Prevention (DLP) technologies. However, today DLP technologies fall into two main categories: Data-at-Rest and Data-in-Motion:

- **Data-at-Rest:** This term refers to data stored on computers, stored on storage devices, or being used by the data owner. It excludes data traversing a network. Examples include files or e-mails saved on a hard drive or server.

- **Data-in-Motion:** This term refers to data transmitted across a network. This data can be regarded as secure if both hosts are capable of protecting the data and a third party cannot eavesdrop on the communication.

Depending on an organization's risk tolerance and the type of data breach most often occurring, the appropriate DLP technology should be used. For example, if the most frequent type of data breach is the theft of laptops with unsecured files, then a Data-at-Rest solution is most appropriate for the organization as a Data-in-Motion solution would not mitigate this risk. If the most frequent type of breach is an employee accidentally emailing data copied from a spreadsheet or other source, a Data-in-Motion solution is more appropriate.

Data Breaches

Solving an organization's data loss problems requires understanding the nature of the most relevant breach type and then building a solution with the appropriate methodology. See the table below for a list of data breach types and solutions.

Data Breach	Solution
Hacker (includes malware)	Data-at-Rest
Digital Media (lost/stolen computers, backups, etc.)	Data-at-Rest
Web Content	Data-at-Rest, Data-in-Motion
Accidental Transmission (e-mail, etc.)	Data-in-Motion
Physical Media (lost/stolen papers, etc.)	Policy
Dishonest Insider	Policy, Access Controls
Other/Unknown	Access Controls

[1] http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

As can be inferred by this table, no single solution is sufficient to protect against every threat within an organization. Based on your own risk analysis, one technology might be favored over another. Additionally, please note a complete solution involves not only the use of technology but buy-in from the people involved and strong processes.

Which Technology is Right for You?

One key differentiator between these solutions is that Data-at-Rest solutions offer organizations the ability to be corrective and proactive. They allow organizations to address the root cause of most data loss scenarios by securing data at the source. When sensitive data is found with one of these technologies, it encourages an organization to shred it, redact it, or secure it. More advanced technologies also provide centralized reporting on aggregate risk exposure. Analysis showing trends of this information over time can help organizations determine if their policies are sufficient and effective.

Changing behaviors by empowering employees to minimize overall risk is a major strength of Data-at-Rest technologies.

Data-in-Motion solutions are preventative as they block transmissions, but they do not provide root cause remediation capabilities. As such, organizations exclusively using Data-in-Motion technologies do not have information that allows them to proactively take action and minimize exposure risk. For example, Data-in-Motion technologies will not notify or give indication about the creation of new instances of unsecured sensitive data. An employee e-mailing an attached spreadsheet with sensitive data may repeatedly send the file only to have it blocked multiple times. This differs from a Data-at-Rest solution that could have simply secured the unprotected spreadsheet the first time.

Another key differentiator with these solution methodologies is that with Data-at-Rest technologies the responsibility for managing discovery and remediation efforts can be pushed from the IT staff to individual data owners. This is different than with Data-in-Motion solutions, which always require centralized administration by IT staff. By pushing the processing power and remediation tasks to an organization's data owners, an institution has the ability to inform and educate its employees and influence their behavior. Changing behaviors by empowering employees to minimize overall risk is a major strength of Data-at-Rest technologies. Employees essentially become a self-policing cloud and a part of the long-term security solution.

Similarly, because employees can be empowered with Data-at-Rest technologies, these technologies are viewed as being friendlier to an organizational environment. Data-in-Motion technologies can only be centrally managed and impose strict policies on individuals, so they are sometimes perceived by employees as being intrusive and heavy-handed. For this reason alone, some organizations prefer Data-at-Rest solutions.

Data-in-Motion technologies' key strength is their ability to prevent accidental transmission. Intentional transmissions are often not prevented as users are typically sophisticated enough to find a way around these monitoring technologies. While Data-at-Rest solutions do not prevent accidental transmission, they often do reduce their likelihood. A Data-at-Rest technology highlights the existence of unsecured files and encourages the owner to shred it or encrypt it, thereby securing the underlying data. Thus, when the data owner sends the encrypted file, the transmission does not expose any sensitive information.

The Data-in-Motion Illusion

Data-in-Motion technologies are not comprehensive DLP solutions and continue to be circumvented. Consider laptops, which often leave an organization's technical infrastructure. When these devices are used by employees in public environments they are at much greater risk because the data-in-motion technologies cannot extend their processing to these third party environments.

Data-in-Motion technologies can only prevent exposures when those exposures occur in clear text. Hackers capable of penetrating an organization's security defenses are generally sufficiently sophisticated and establish secure tunnels through which to transmit private data because they know Data-in-Motion technologies may be present. This act of encrypting data while in motion negates the effectiveness of Data-in-Motion solutions.

Data-in-Motion technologies are more complicated to implement and operate than Data-at-Rest technologies. Upfront, Data-in-Motion technologies require additional hardware and professional services expertise to deploy. They are not plug-and-play. The nature of the data transmitted is different for each organization and the exact policies desired by each organization often require special configurations. After initial deployment, Data-in-Motion technologies also require continuous tuning to optimize their behavior. Improper configuration dramatically reduces the effectiveness of the blocking technology.

Data-in-Motion solutions also require constant monitoring and place a performance strain on the network. Unlike Data-at-Rest solutions, which can be scheduled to perform scanning during off-peak hours, Data-in-Motion technologies are always on and constantly 'sniffing' the network for data. This constant sniffing can dramatically reduce an organization's productivity or force the organization to purchase more expensive infrastructure to support the increased network demand.

Total Cost of Ownership

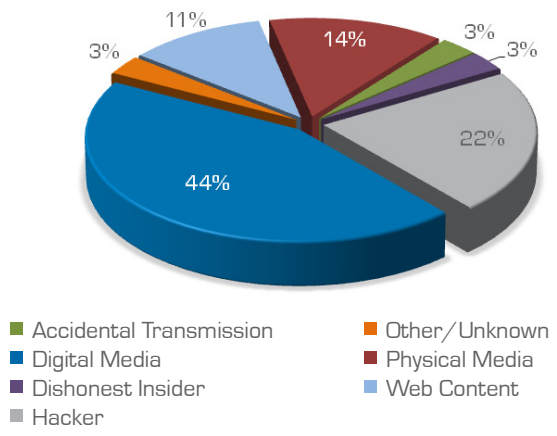
Data-at-Rest solutions are far more affordable than Data-in-Motion solutions. Data-in-Motion systems typically carry more expensive initial software costs, hardware costs, professional services costs, and ongoing maintenance costs. Minimum infrastructure requirements, including network bandwidth and hardware, can cost anywhere from $25K-$150K depending on the size of deployment. Additionally, the professional services required to initially configure Data-in-Motion systems are quite substantial and can cost as much, if not more, than the software itself. The greater the level of configuration and sophistication desired by an organization, the higher the cost.

Conversely, Data-at-Rest solutions only have software and maintenance costs and minimal, if any, hardware requirements. Most Data-at-Rest solutions can be installed on preexisting hardware and are relatively simple to use. They do not usually require any professional services for configuration and setup. All in, the total cost of ownership for a Data-at-Rest solution will typically be less than half of a Data-in-Motion solution.

Historical Research

If the saying "history repeats itself" is true, then performing historical analysis should give managers insight into the nature of the data loss most likely facing their organization. According to Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy organization, since January 2005 more than 260 million records containing sensitive personal information were involved in security breaches in the United States.[2] Identity Finder has manually classified this dataset by type of data breach and solution methodology to develop the following charts.[3]

Data Breaches by Type

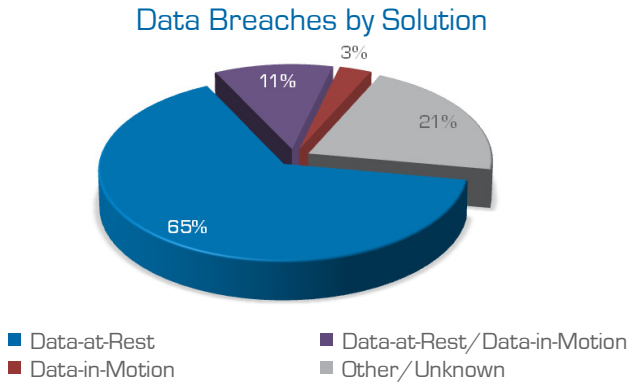


From this analysis, it is clear that the two most frequent types of data breaches involving personal information occur from loss of digital media (44%) and hackers (22%). These could have completely been prevented by a Data-at-Rest solution if the data had been found and secured before the incident. Note that the typical types of data breaches often discussed socially, such as an employee accidentally

[2] http://www.privacyrights.org/ar/ChronDataBreaches.htm
[3] Classified data available upon request.

emailing sensitive information or resulting from a dishonest insider, account for only approximately 6% and are not major sources of data breaches.

Diving deeper into the analysis, we can see the percentage of data breaches could have been prevented by various DLP strategies.



From historical analysis, it is clear that a Data-at-Rest solution would have prevented the most data breaches and is the most appropriate data loss prevention methodology for organizations to implement. The nature of data breaches is such that securing Data-at-Rest will most likely have the greatest impact toward reducing data loss.

Conclusion

Organizations must consider the relevance of a DLP strategy before implementing a solution methodology. From historical research it is clear that most data breaches occur because of unsecured Data-at-Rest. Best of breed solutions that implement both Data-at-Rest and Data-in-Motion technologies are complementary and increase the level of protection for an organization. However, most managers must maximize the impact of limited budgets and choose one methodology over another. Therefore, managers should realize that the greatest threat facing their organizations is unsecured Data-at-Rest and implement a security solution to address this risk and maximize the return on investment of their budget.

About Identity Finder

Identity Finder, LLC was founded in 2001 by innovative security experts. Its security and privacy technologies provide businesses and consumers the ability to prevent data leakage and identity theft. The company has quickly grown to become a leader in identity theft prevention by helping millions of consumers, small businesses, and enterprises in over fifty countries.

identityfinder