Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 11, Issue 5

Cybersecurity from the Inside: Protecting Structured, Unstructured, & Semi-structured Data

By Eran Leib

Data is everywhere, exploding, and growing exponentially. It's structured. It's semi-structured. It's unstructured. It's stored across different platforms, networks, systems, on premise and in the cloud. But, it all has one thing in common: data is data, and it all needs to be controlled and protected.

Data is critical intellectual property at the core of the business. Meanwhile, its volume – we're talking exabytes here – has spiraled out of control and become unmanageable. The larger the organization, the greater the data sprawl, exacerbating the danger from internal and external threats such as social engineering, malicious activities, corporate espionage, theft, and even simple errors.

Who's accessing your data? Should they be allowed to? You need systems in place that will protect it. You need intelligent solutions that can determine who can and has accessed structured, semi-structured, and unstructured data to ensure that unauthorized data breaches can be easily prevented and detected.

All companies should be able to do the following:

- **Determin**e the data's degree of sensitivity;
- **Monitor** who is actually accessing the data;
- **Understand** who can access which types of data, via what means, and within what parameters (time of day, department, devices, etc.);
- **Detect** unauthorized access in real-time;
- **Track** data access patterns;
- **Automatically** review, assign and authorize access;
- **Perform** forensics after the fact; and
- **Achieve** and maintain compliance with regulatory requirements.

The latest Verizon and Symantec data breach investigation reports demonstrate that breaches are on the rise, especially the ones from within. Internal users are responsible for almost 60 percent of the data breaches, where 88 percent of these breaches involve privilege misuse. At the same time, the amount of data breaches amount have tripled year over year.

The key problem in every organization of any size is "data blindness." Most IT security teams have no idea about how the data is being utilized, where the sensitive data resides, and who has access to it. Many IT security professionals don't know where to start or what to do to get a handle on it because of volume and sprawl.

Meanwhile, the business side wants answers. Business users want to know who deleted their data. The auditors want to make sure that the company complies with the incredible volume of regulations operators need to fulfill, well beyond SOX and PCI.

To protect and govern data, you need to be able to answer the following questions:

- Where does the sensitive data reside?
- How do we classify data: content, metadata, or usage?
- How do we identify sensitive information like Personal Identity Information (PII) or credit card information (PCI)?
- Who is accessing what, in real time?
- Who has changed privileged groups' membership?
- What user, machine, and data context is necessary to fully identify all actions?

Complete data access governance for enhanced cyber security requires that management, IT, and the auditors have complete visibility into users' permissions across all the organizational applications. They must be able to easily identify over-exposed information inappropriately accessible to many, such as the CEO's inbox.

NOT FOR DISTRIBUTION OR REPRODUCTION

© 2014, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

Permissions management is also critical. Especially in organizations such as large as communications service providers, where users frequently change roles. The accounts receivables clerk who got promoted to marketing sales rep should no longer have access to credit card information. Enhanced permission management, combined with data classification, adds an additional level of compliance control and security by ensuring that only certain roles are allowed to read or modify information like credit cards. Permissions management also entails keeping track of who reviewed, approved, and revoked access. Being able to tie granted access to those approved is critical for security investigations as well as compliance audits.

Real-time protection is the ideal; you need to be able to identify who has violated organization access policies as they happen. Time is of the essence when dealing with data protection; the access policy solution must identify violations and respond to them in real-time.

Cybersecurity and compliance

Operators are awash in structured, unstructured, and semi-structured data, whether in SAP or Oracle systems, homegrown billing solutions, roaming systems, reporting systems, or other support systems. They need to report to multiple local, regional, and national government regulators, financial regulators,and industry standards associations, among others. Audit and discovery expenses can escalate into the millions of dollars. Compliance should be an integral part of every data access governance and cybersecurity system, allowing the easy creation of reports, the ability to generate information about activities in real-time, and easily perform forensics to ensure that everything has been done as it is supposed to have been – and have a clear audit trail when it wasn't.

Compliance for strengthening cybersecurity needs to occur on an ongoing basis. Companies shouldn't focus on reporting and then become lax on enforcement. Compliance itself should not be a focus of cybersecurity; it should be the natural consequence of ongoing cybersecurity activities. Real-time monitoring is key, as it allows you to catch any breaches immediately and stop them. Systems also need to be in place to address any breaches immediately, for both data loss control and public damage control. To do this you should:

- Get everyone in the organization involved in the process. Create individual and departmental performance metrics to encourage and reinforce compliance with both compliance and cyber-security.
- Protect yourself against a full range of scenarios by having strong rules-based compliance and data access governance that allow you to.
- Alert the CISO when someone is accessing sensitive information through VPN (ungoverned workstation).
- Catch and respond to over-exposing permissions changes as they happen, for example, whenever someone grants everyone access on a folder that contains sensitive information.
- Notify the organization's security operations center when someone from IT accesses sensitive business data.
- Understand what compliance controls are violated, and by whom, not only before an audit, but all the time, in real time.
- Being able to automate a great deal of the audit process and avoid audit day surprises, can be directly translated to saving money on fines and loss of reputation while keeping regulators happy.

Benefits of an active system

The benefits of an active system are numerous. Such a system tracks sensitive data. Organizational data stores such as file servers, NAS devices and SharePoint portals store tens of millions of files. Information is constantly being added, duplicated, edited, and very rarely deleted. An active system helps identify data owners and delegate responsibilities. Data owners usually are the creators of the information; they know who should have access to their information. They also have the motivation to take active part in protecting it. Active systems streamline compliance with access requests management, access reviews, and compliance controls and the more control IT has about who is accessing the information, the better.

Visibility is crucial in security. Who is doing what, where, when and how? How is the information being used? Who is accessing sensitive information? Who is deviating from the organizational policies? Active systems can answer these questions. In the process, they can reveal who in the organization can do what. Looking at the big picture of granted entitlements across the enterprise is vital to accurately estimate potential exposure and risk factors to sensitive data. Having entitlements information from millions of files, folders, mailboxes, and sites, centralized and analyzed can easily answer important questions such as who should have access to sensitive information (HR, medical, financial, etc.) and what types of information are accessible to what audiences (IT department, domain admins, etc.). Add this information with knowledge about the actual activities and you can find out who is using his entitlements, who is not and, what permissions are stale.

NOT FOR DISTRIBUTION OR REPRODUCTION

© 2014, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

These activities and capabilities help organizations achieve real-time protection. Organizations need to know about and treat violations as they happen; otherwise the information is as good as lost. Defining real-time policies based on various user, machine and information attributes dramatically increases the odds of preventing information leaks and the damages that comes with it.

Cybersecurity and separation of duties (SOD)

You have hired the best people to do the best job possible. Or so you think. Maybe Joe in customer service had a girl friend who recently broke up with him and wants to doctor her mobile bill for revenge. Maybe Jane in accounts receivable has decided that she needs a few thousand dollars to pay off some debts. You need to ensure that you have strong separation of duties policies and enforcement in place to ensure these types of scenarios cannot happen. Managing exceptions is key to managing risk. Ensure that each access requirement matches up to clearly defined security controls. Fine-tune the defined roles to lower their number and increase efficiency. Integrate what-if analysis to access requests processes. Strong internal controls on SOD will further strengthen the barriers to fraud driven from within the organization itself.

Security in action

The full security context is far and beyond the most important thing for telling rightful activities from violations. Knowing that someone has accessed the highly sensitive HR payroll spreadsheet is one thing. Knowing that they are in IT is another. Knowing that this activity occurred at 4 a.m. from an external, unmanaged workstation via the organizational VPN is great. Getting the alert by 4:01 a.m. is critical. Your cybersecurity data access governance system needs to be able to deliver the who, what, when, where, and how in real-time to fully protect your greatest corporate asset – your data.

Hidden ROI from a highly efficient data access governance & cybersecurity system

A really good data access governance-focused security system can protect the organization against theft, legal liabilities, reputation loss, and potential fines and even jail time for senior management.

A few more benefits are hidden within an efficient system include: identifying and removing unused data from high-end storage reduces storage costs; eliminating inactive accounts reduces license costs; and streamlining compliance processes such as preparation for an audit or access requests frees a noticeable amount of manpower.

Strong cyber-security, compliance, and data access governance policies will allow you to take specific steps to protect your structured, unstructured, and semi-structured data and pay significant dividends well beyond.

NOT FOR DISTRIBUTION OR REPRODUCTION

© 2014, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.