WHITEPAPER

Salesforce data protection through user activity monitoring

IN ORDER TO EXPAND TRUST IN SALESFORCE, IT'S ESSENTIAL TO PLAN AND IMPLEMENT DATA PROTECTION STRATEGIES THAT INCLUDE USER ACTIVITY MONITORING.

imprivata®

Salesforce is a mission-critical application for major enterprises. A single Salesforce customer instance can store vast amounts of regulated, confidential, and proprietary information accessible by hundreds or even thousands of users. To date, Salesforce has provided authentication, access control, and user management methods as the primary tools of data protection. However, rapid forensic investigations on users, continuous user monitoring, and alerting have been lacking. This is because, historically, Salesforce audit trails have been manual, time consuming, and expensive to obtain.

Salesforce Event Monitoring addresses the availability of audit trails, enabling user activity monitoring for enhanced security and visibility.

Salesforce is often deployed in enterprises without the full participation of the Information Technology and Information Security departments. These departments approve the architecture of Salesforce but do not maintain servers, operate projects, or fully participate in information security operations. Thus, the Director of Salesforce-CRM and other data owners are held responsible for nearly every aspect of Salesforce including data protection. Specifically, the Director of Salesforce-CRM and other data are owners expected to protect the data held in Salesforce against the rising trends of data theft[1].

This whitepaper will help readers understand the need for Salesforce data protection and user activity monitoring by:

- Examining the specific types of sensitive information many businesses are already storing in Salesforce
- Highlighting statistical risks of insider threats to confidential data
- Providing an analysis of Salesforce Event Monitoring and the included capabilities
- Detailing the specific functions needed in an effective user activity monitoring solution for Salesforce

Employee beliefs are trending toward feeling entitled to take anything they work on, regardless as to how confidential the information might be[2].

User activity monitoring for Salesforce must provide the Director of Salesforce-CRM and data owners with the peace of mind that monitoring is continuous and supplies easy-to-interpret information for alerts or investigations. Furthermore, user activity monitoring must be efficient to set up flexible, and easy to maintain as Salesforce implementation grows and evolves.

Salesforce Data Protection

Salesforce is now a mission-critical application in major enterprises. For most, Salesforce started as a cloudbased Customer Relationship Management (CRM) system for holding prospect, pipeline, and customer information for a department or subsidiary. Many Salesforce customers then integrated information from their enterprise into Salesforce, empowering the platform to play a major role in ongoing business operations. The trend of integrating information from the enterprise into Salesforce is accelerating as Salesforce has launched application and analytic platforms such as Lightning and Einstein. Salesforce now influences or even empowers many aspects of the full life-cycle of an enterprise's relationship with its customers including marketing, sales, orders, fulfillment, contracts, supply chain, financials, and customer service.

As a result of Salesforce's growth within the enterprise, the information stored in Salesforce has expanded dramatically and now includes:

- Highly proprietary and valuable customer information accumulated through years of relationship building as well as automated gathering processes
- Detailed prospect information gathered through years of investment and relationship building
- Ordering systems that use price books, products, and contracts
- Financial information that feeds into corporate accounting systems which in turn generate GAAP audited financials

More specifically, information in Salesforce may include bank account details, credit card numbers, protected health information (PHI), and personally identifiable information (PII) of all kinds. This is in addition to highly proprietary information about customers and prospects that may not be subject to regulation, but is essential to an enterprise's advantage in the marketplace.

The sensitive information held in Salesforce instances will only increase as Salesforce initiatives such as Lightning and Einstein gain momentum in the enterprise. Clearly, Salesforce holds information considered to be the “crown jewels” of the enterprise.

The Director of Salesforce-CRM and Salesforce administrators intuitively understand the data theft and misuse risks of information held in Salesforce. They live through the day-to-day events associated with a departing sales executive who is believed to have downloaded customer lists on their way out. They have had business managers call and ask if a report can be generated on a specific Salesforce user who is accused of extracting details of a major European proposal when their territory of coverage is Asia. Or they have been asked by finance to recreate the changes to the financial metrics of an opportunity related to a suspected internal fraud.

In 60% of 150 data theft cases studied in the Recover Report[1], internal perpetrators stole proprietary information in order to secure a new position with a company competitive to the data owner.

In 30% of the 150 cases studied, the internal perpetrator’s motivation was to use the stolen information for the creation of a new business.

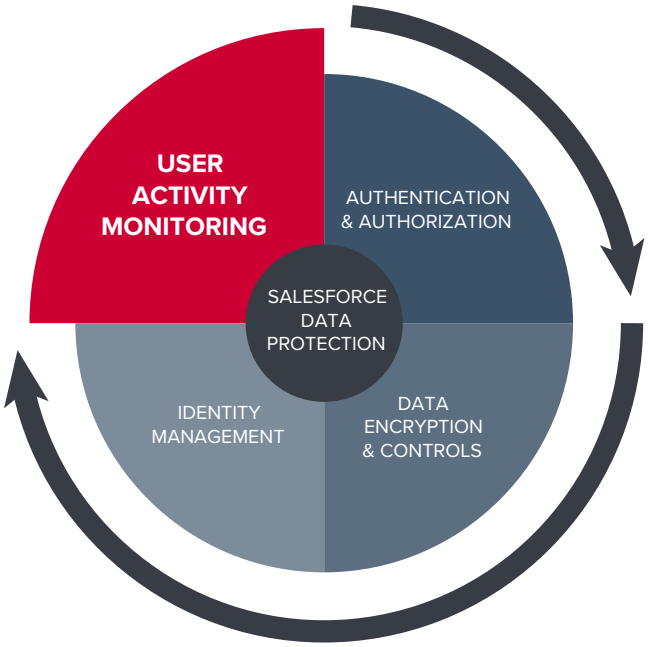


Fig. 1, User activity monitoring

While these are just simple examples, the statistics from industry studies reveal a compelling trend for the necessity of a Salesforce data protection strategy at the user level.

These statistics highlight a growing trend in which employees who perform intellectual property work of any kind have come to believe they are entitled to the intellectual property as if they owned it. A recent Ponemon Report sponsored by Symantec details this phenomena; the associated white paper is titled “What’s Yours is Mine: How Employees are Putting Your Intellectual Property at Risk”[2].

Increasingly, businesses are prepared to bring suits against those who commit data theft. The Identity Theft Resource Report, www.idtheftcenter.org, cites numerous examples of businesses that have brought lawsuits against former

employees who are accused of stealing confidential customer information across financial services, wealth management, telecommunications, and healthcare. In the case of a lawsuit, it is essential to have professionally documented every aspect of an investigation so the data owner's legal position is defensible.

Furthermore, there has never been more regulatory enforcement of privacy and security standards by industry and across the globe.

A comprehensive data protection program increases confidence to store sensitive information in Salesforce, therefore enabling greater business velocity through central data views and improved work flows. Additionally, Salesforce customers expand their reputation for trust by protecting shareholders against theft of proprietary information, protecting their customers against theft of personal information, and by improving their privacy and security compliance posture.

Privacy, security, and industry regulations often carry with them a requirement to conduct some form of user activity monitoring. HIPAA for example requires an examination of access through audit logs of all systems that access protected health information. This requirement also applies to healthcare providers storing protected information in Salesforce.

Without data protection strategies in place for Salesforce, the theft or misuse of information held in Salesforce elevates risk to the business:

- Competitive losses due to data theft
- 30% of those who stole internal data did so to start a competitive company according to a recent study[1]
- 60% of those who stole internal data did so to secure a new position with a competitive firm according to a recent study[1]
- Integrity of sales operations through product and price book deletions or manipulation of sales opportunities after they have fed financials
- GAAP Financials are often fed by Salesforce
- Regulatory non-compliance with privacy and security laws such as HIPAA, PCI, SOX, JSOX, EU and UK Data Protection Acts

DATA PROTECTION FOR SALESFORCE

Modern enterprises are more dynamic than ever before. Mergers, acquisitions, partnerships, temporary employees, outsourced functions, and attrition all contribute to an information security environment that is dynamic, growing, and complex.

In response to these information security demands and others, Salesforce has improved core security features. System administrators can configure security settings in Salesforce to limit IP ranges of user access, enforce strong authentication and password policies, and periodically expire passwords. Salesforce administrators can also create detailed user profiles with role-based access controls. These controls can even be supplemented by dynamic, field-level access rules.

These security features are positive strides; however, access control schemes in complex and dynamic environments come with limitations. Specifically, complex access control schemes may result in performance degradation, require constant time and attention to maintain, and most often cannot fully keep pace with the dynamics of the business. Thus, modern data protection and governance strategies need to include user activity monitoring.

For more information related to this topic, reference Gartner's "Consider a People-Centric Security Strategy"[3] and "Prevention is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence"[4].

Reliable and legally sound user activity monitoring is not possible without audit logs. Salesforce administrators know all too well that Salesforce audit logs have historically been available only through customer service at considerable expense and complexity. The lack of automated audit logs has made monitoring impossible and forensic investigation time-consuming and expensive. The lack of audit logs also leaves a void in all security, certifications, and regulatory requirements that relate to audit controls.

To address this limitation as well as provide for additional capabilities, Salesforce developed and released "Event Monitoring." Salesforce Event Monitoring files are automatically generated by Salesforce and accessible through APIs (see specific edition limitations). For the first time, information governance and data integrity controls are possible in conjunction with a Salesforce customer instance. This enables user activity monitoring and more robust data protection strategies.

Salesforce Event Monitoring

Salesforce Event Monitoring is powerful and produces comprehensive audit files that programmatically enable important aspects of data protection for Salesforce including:

- Forensic investigations
- Continuous monitoring with alerts and filtering
- Flexible, multi-criteria reporting with filtering
- Governance reporting
- Audit log storage, encryption and archives

Salesforce Event Monitoring files are a series of files accessible through a programmatic API. The files are clear-text but not human readable without programmatic or manual manipulation.

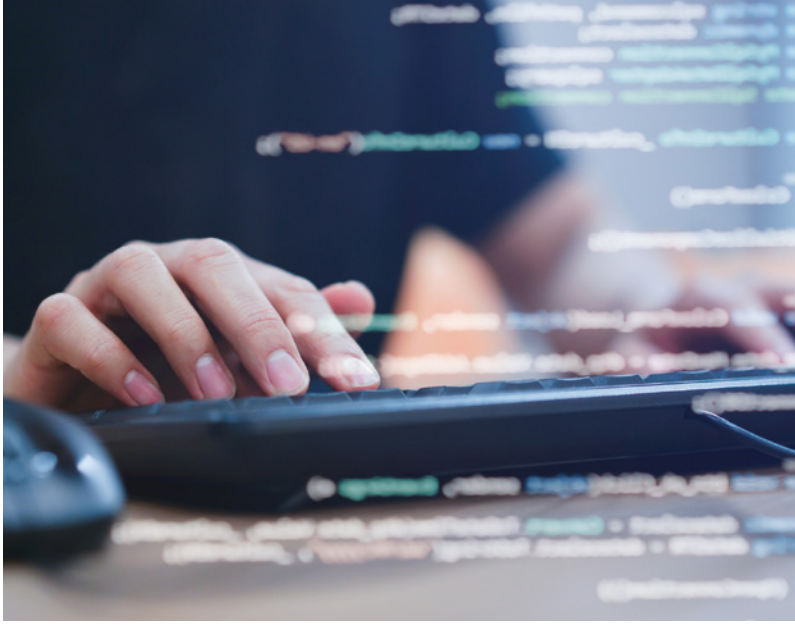
User Activity Monitoring for Salesforce

Below is an overview of the essential features of a user activity monitoring platform capable of supporting a robust Salesforce data protection strategy. As previously discussed, Information Security departments are overwhelmed by an unprecedented level of external attacks and while they recognize the risks of internal data theft, it is nearly impossible for them to engage at the tactical level of data protection within Salesforce. Thus, the responsibility and actual operation of Salesforce data protection will likely fall to the Director of Salesforce-CRM, Salesforce administrators, and other business users. With that in mind, the platform must present information that is easy-to-understand in business terms, and straightforward to act on.

ARCHIVING OF EVENT MONITORING FILES

Salesforce Event Monitoring files are produced by Salesforce and retained on their customer's behalf for a very short time period - often a matter of days. A strategy for capturing, encrypting, and archiving the Event Monitoring files must be put in place by Salesforce customers in order to meet the most basic requirements of a data protection and governance strategy for Salesforce.

Event Monitoring files are clear-text, but not human readable without detailed API calls, or through very detailed, laborious, manual intervention. A robust user activity monitoring platform must automatically



decode the files so that a business user can easily interpret the results.

FORENSIC INVESTIGATIONS

A wide range of scenarios requires forensic investigation of Salesforce access activity. For many enterprises, a review of access of a departing employee is a mandatory step in the off-boarding process, and a simple forensics report supports this step. Numerous other unexpected scenarios may warrant probing. For example, conducting an investigation of how a price book was deleted that lead to errors in hundreds or even thousands of Salesforce opportunities.

CONTINUOUS MONITORING WITH ALERTS & FILTERING

User activity monitoring and alerts provide peace of mind as well as visibility into suspicious user behaviors. The most obvious scenario is monitoring for the export of a customer report and exports in general. However, it should be noted that monitoring and alerting on "exports" of reports is insufficient for most enterprises. In fact, unless more details regarding an export, as well as fine-tuned

filtering, are enabled, alerts on exports become more noise and stress. Target monitoring carefully, and tune alerts so they are meaningful enough to require investigation when they do occur.

FLEXIBLE, MULTI-CRITERIA REPORTING WITH FILTERING

Every Salesforce instance holds standard fields and objects such as Accounts, Contacts, Opportunities, Leads, and Cases. And virtually all major enterprises have tailored their Salesforce instance by adding custom fields to support the specifics of their business. Furthermore, customers add custom objects, which enable workflows and applications supporting the business. Reporting and filtering must be capable of providing salient information rapidly, which includes the ability to support on standard Salesforce fields and objects as well as custom fields and objects.

INVESTIGATIONS, LEGAL DOCUMENTATION, AND GOVERNANCE REPORTING

Inevitably, enterprises operating user activity monitoring in Salesforce will discover users demonstrating behaviors that are in violation of appropriate data use policies, codes of ethics, and, from time to time, involve data theft and fraud. As visibility into these types of activities grows, enterprises quickly recognize they must have a legally defensible position in the event an accused party contests a termination. Thus, a user activity monitoring platform should seamlessly support documenting investigations and provide associated governance reporting.

Lessons Learned from User Activity Monitoring in Salesforce

- Event Monitoring files in their raw form are difficult to interpret.
- Event Monitoring files are retained by Salesforce for a very short time period. Unless a Salesforce customer puts in place an active capture, encryption, and archival strategy, the most basic data protection and data governance needs will not be met.
- Information security alerts from “export” notifications are overwhelming without multi-field filtering criteria.
- Multi-field filtering criteria and domain rich context must be available in order to avoid alert fatigue.
- Ensure reporting and filtering features work with Salesforce standard fields and objects as well as custom fields and objects.
- Forensic investigations will arise unexpectedly for scenarios of all types, not just departing employees.
- The ability to conduct a “Quick Search” is an anchor in your data protection program for Salesforce.
- Fully document investigations for legal defense including reports, audit logs, policies, and related documents.
- Audit log retention is essential to legally defensible investigations and regulatory compliance.

Conclusion

A Salesforce instance may hold vast amounts of regulated, proprietary, and confidential information. The sensitive information held in Salesforce instances will only increase as Salesforce initiatives such as Lightning and Einstein gain momentum in the enterprise. Data theft trends by internal users continue to increase in damage and studies suggest that, more than ever, employees who work on intellectual property project believe they are entitled to take it.

With Salesforce Event Monitoring files, proper data protection and governance programs should now be implemented and supplemented by user activity monitoring. The responsibility for a data protection program is most likely to fall on the Director of Salesforce-CRM and supporting Salesforce administrators. This means that tools and platforms needed to support Salesforce data protection must be easy-to-use and support multi-field filtering to rapidly gain access to salient information. In addition, these tools and platforms must be extremely flexible to support Salesforce standard fields and objects as well as custom fields and objects which are part of nearly every Salesforce instance.

A comprehensive data protection program increases confidence to store sensitive information in Salesforce, therefore enabling greater business velocity through central data views and improved work flows. Additionally, Salesforce customers expand their reputation for trust by protecting shareholders against theft of proprietary information, protecting their customers against theft of personal information, and by improving their privacy and security compliance posture.

References

1. MIshcon de Reya. 2014. The Recover Report. Summit House. In Media.
2. Ponemon. 2013. What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk. Symantec Corporation
3. Tom Scholtz. 2013. Consider a People-Centric Security Strategy. Gartner.
4. Neil MacDonald. 2014. Prevention is Futile in 2020: Protection Information Via Pervasive Monitoring and Collective Intelligence. Gartner.

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com.

FW-WP-SF-dataprotectionthroughuam-0321