The Top 3 Salesforce Security Concerns

Keeping IT Directors Up At Night

We asked IT leaders at companies with $1+ billion in revenue about their **top 3 Salesforce security concerns** and here's what they ranked most important:

#1 Unauthorized User Access

IBM recently published that the **average cost of a data breach is $3.86 million**. With so much at stake, it's no surprise unauthorized user access is the top concern. The good news is, Salesforce is an extremely secure platform and there are simple steps your organization can take to minimize external threats and breaches.

The Top 5 Salesforce Security Tips to Make Your Instance More Secure bit.ly/5sfsecurity

#2 Mass Exports or Deletes of Data

Salesforce is the single source of truth for many organizations, hosting sensitive data that needs to be protected. Being able to export and delete data in Salesforce is a responsibility that only certain team members should have.

How to Stop Users from Exporting Data from Salesforce bit.ly/exportsf

#3 Unknown or Unexpected Metadata Changes

Did you know that **66%* of data loss and corruption in Salesforce can be attributed to human error**? To mitigate this concern, your company can either:

- Have a Salesforce team member(s) audit the metadata changes in Salesforce daily
- Use a monitoring tool to alert you of these changes

The Top 5 Things to Monitor in Salesforce bit.ly/monitorsfdc

SafeGuard: Proactive Salesforce Monitoring

SafeGuard monitors your Salesforce instance and integrated tools and then notifies your team so that critical issues are resolved as quickly as possible. Interested in learning how to strengthen the security and stability of your Salesforce instance?

Request a demo today at bit.ly/safeguardforsf

cloudkettle.com | 1-800-878-4756 ext 202

© 2019 CloudKettle Inc.

SOURCE: *OwnBackup eBook: The State of Salesforce Data Protection 2018-2019 Annual Report

CloudKettle