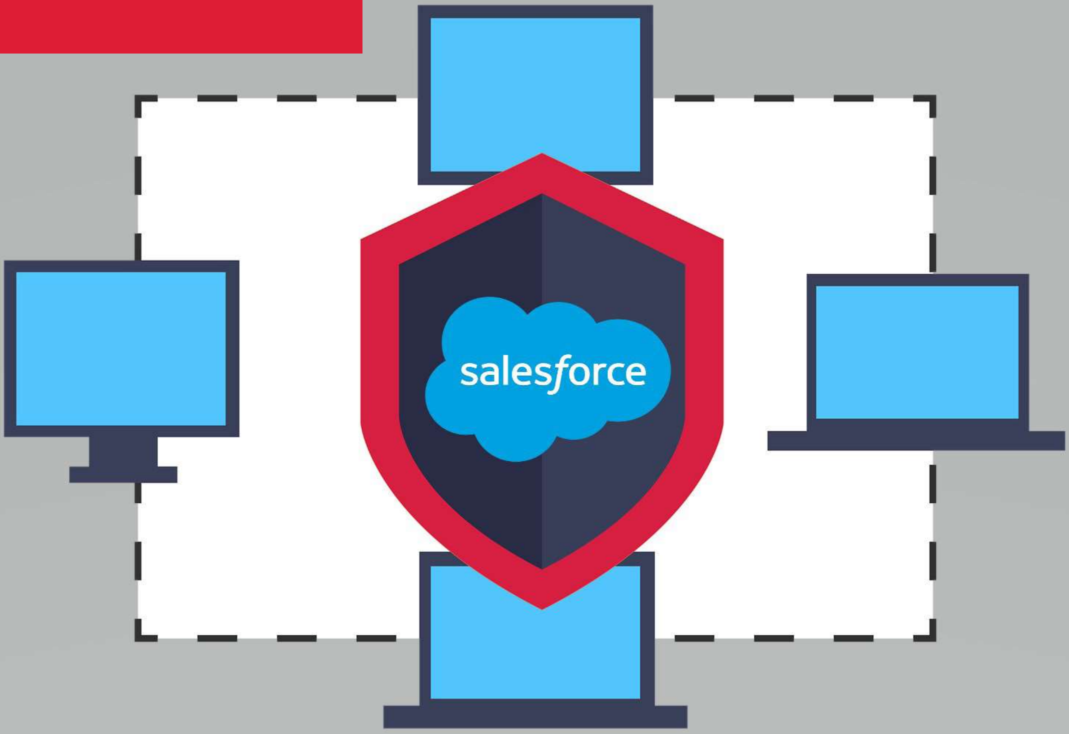
INSIGHTS

Salesforce Security and Your Organization



online business systems

LEVERAGE SALESFORCE TO PROTECT IMPORTANT DATA

Salesforce is known as an industry leader for their adoption of security best practices.

Using a proven and well established security model, they continue to make extensive investments to strengthen the security of the platorm and it's data.

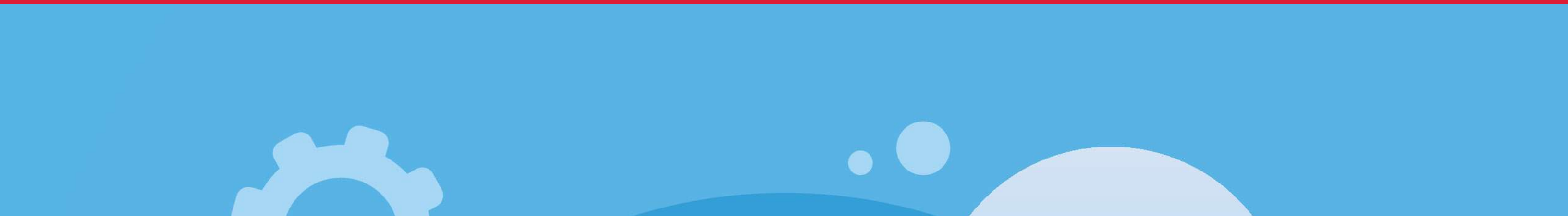
PROTECTING YOUR ENVIRONMENT

While Salesforce continually invests in the platform to strenthen its security posture, each Saleforce customer has a responsibility to leverage these features to protect their data, comply with regulatory guidelines and support the needs of their business.

Salesforce offers many out-of-the box tools to help organizations customize their envionment to address risk and implement security in a way that protects their data security and supports end user productivity.

INVESTING IN SECURITY

Salesforce uses a combination of encryption, access controls and data redundancy to protect the integrity of the data held within the Salesforce platform.



Salesforce Trust

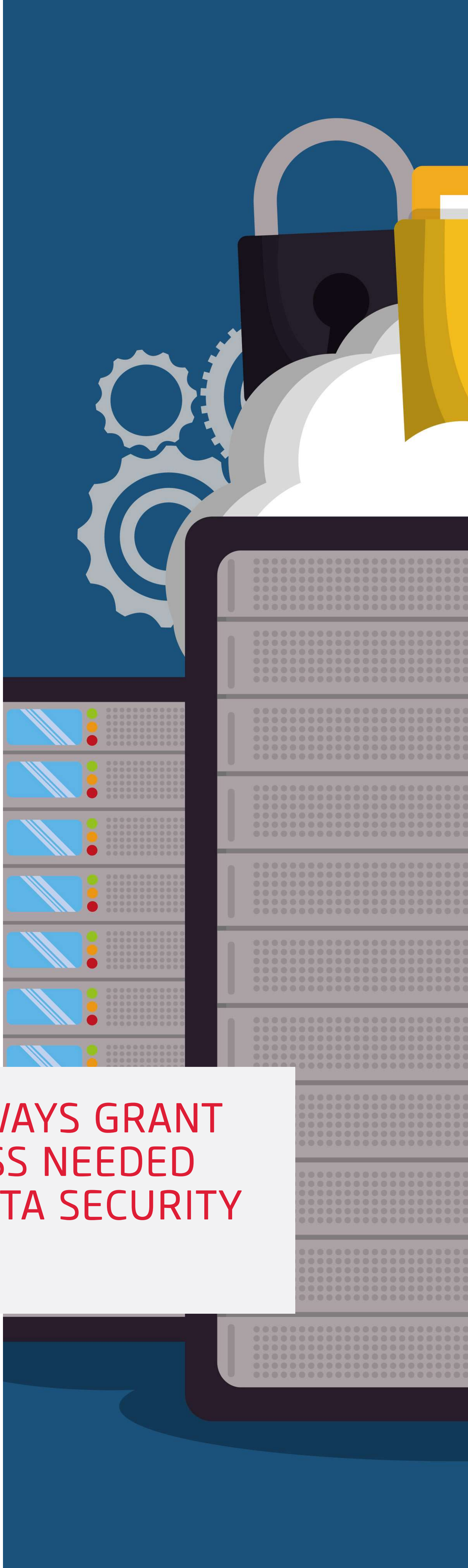
As a customer, it is important to understand the measures Salesforce takes to protect data on the platform level, but it is also very important to properly leverage their offerings within your organization to best protect the data that is important to you.

Salesforce Trust (trust.salesforce.com) is the Salesforce community's home for real-time information on security. This resource rich repository describes how security is baked into the platform and provides guidance to customers on the ways they can leverage Salesforce to protect their data.

EVALUATING YOUR NEEDS

- Do we hold industry regulated personal data?
- Do we need SOC 2 or HIPAA compliance?
- Is the data subject to GDPR or similar governmental regulations?

It is important for organizations to ask themselves these basic questions when evaluating what security needs they have. An organization should determine what the minimum requirements are, assess their internal requirements for their own workflows and reporting, look at usability to support those needs, and then determine which best practice takes into consideration all of these factors. The process will likely engage all departments that use or require access to this data.



THE BEST PRACTICE IS TO ALWAYS GRANT THE LEAST AMOUNT OF ACCESS NEEDED AND TO COMPLY WITH ALL DATA SECURITY REQUIREMENTS.

MORE QUESTIONS TO CONSIDER

- What data do we have?
- What legal and contractual requirements do we have around that data?
- Who needs to see which data?
- Do we have a need for external access to our records?

Based on what is found during the evaluation process, the next step is to see where an organization currently is, versus the requirements that come out of that process.

Although these questions are a good place to start, there may be many more questions that need to be answered depending on what industry an organization is a part of.

INVESTING IN SECURITY

Salesforce provides two helpful tools, Health Check and Optimizer, which organizations can use get to assess their compliance with general security standards, and to receive an overall security evaluation.

Health Check and Optimizer provide baseline information on the security and usability of an organization, as well as recommendations for ways in which issues can be resolved.

Health Check, in particular, can be very useful in quickly allowing an organization to become much more secure through clear steps. The areas highlighted by Health Check are based on industry best practices and should be an important part in guiding security planning.

> Based on the compliance requirements of the industry, it might be necessary to utilize internal resources or engage external consultants to evaluate an organization and to ensure compliance with specific standards. Online's Risk Security and Privacy Practice can provide direction on what may be needed.

10 WAYS TO GET STARTED

Here are 10 ways you can begin to leverage the built-in security options of Salesforce to protect your organization.

1. Review Sharing Settings to make sure they are compliant with the organizational needs. The rule of least permission should be a guiding principal when considering the access levels.

2. Use Profiles and Permissions Sets to give users the minimum access they require. A clear understanding role access requirements and a well defined permission model using Profiles and Permissions is a critical priority.

3. Leverage field level security to enable a further layer of data protection by helping organizations control which data is visible at the field level on records, increasing their security.

4. Restricted hours limits access for login by groups of users to certain business hours. This type of security restriction is very suitable for groups of users that have clear hours of access, such as help desk users.

5. Any Apex custom code can be secured through several means: limiting base access to classes based on chosen criteria, mitigating common attack vector and granular control of the access granted to the functions in classes themselves.

6. Two-factor authentication (2FA) is an important step in reducing risk from malicious logins. Salesforce offers methods to enable 2FA across an organization while allowing specific exceptions where a requirement might exist.

7. Salesforce supports restricting access to certain IP addresses or ranges, also called whitelisting. This practice is easy to implement in cases where access is only necessary from certain endpoints and offers a good level of mitigation.

8. Single sign-on (SSO) is a good way to control, track and later audit Salesforce access. SSO provides a good balance between access control and usability for end users. It is also generally more secure than traditional password sign-in.

9. When higher levels of encryption are needed beyond the out-of-the-box encryption capabilities, Salesforce Shield should be used. Salesforce Shield offers enhanced platform encryption and customer-controlled security keys.

10. Reviewing user login history and other forms of external access is critical to maintain security. In industries subject to additional compliance requirements, active auditing of record changes and access may be necessary to maintain compliance.

NEXT STEPS?

Online's Security Control Assessment service focuses on how you manage your security needs taking into consideration people and processes as well.

Our goal is to uncover areas of concern, provide a list of preventive measures, and corrective controls. We will then work with you to prioritize opportunities and gaps identified during the assessment and ensure those are reflected in our recommendations.

Results. Guaranteed.

Contact Us

Marshall Cram

Managing Director,
Salesforce Practice

e: mcram@obsglobal.com

c: 403-561-8899

online

Founded in 1986, Online Business Systems is North America's leading Digital Transformation and Cybersecurity consultancy. We help enterprise Clients by designing improved business processes enabled with secure information systems. Our unsurpassed delivery, our people, and the Online culture of loyalty, trust and commitment to mutual success set us apart.