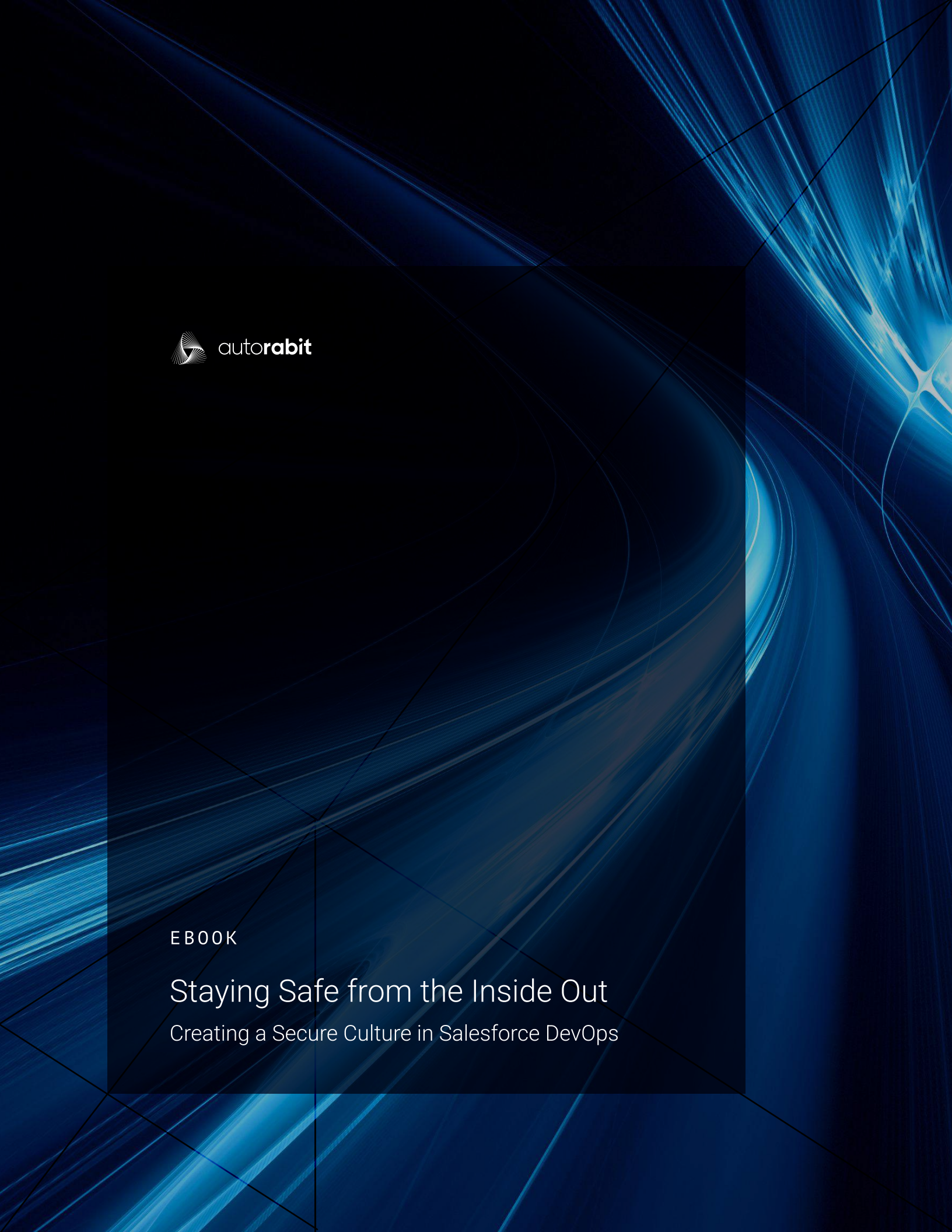


EBOOK

Staying Safe from the Inside Out

Creating a Secure Culture in Salesforce DevOps

INTRODUCTION

Data security requires constant attention. It only takes a single slip-up to create a vulnerability that could cost your organization millions of dollars, lead to compliance failures, and give your customers a reason to stop trusting you with their sensitive data.

Your data security strategy is only as strong as its weakest link. Human error is a leading cause—if not the leading cause—of data breaches. You can have the most high-tech security tools in the world, but a singular error can give the keys to your system directly to a bad actor.

Salesforce, as a platform, is secure. However, it utilizes a shared responsibility model that puts the onus on users to implement proper security measures. Any customization or integrations are up to you to protect. Failing to do so opens your organization up to costly data loss, corruption, and exposure.

How can you ensure your Salesforce environment is protected? The first step is understanding the Salesforce data security landscape. After that, building a culture of security within your organization communicates the importance of maintaining secure practices across your entire workforce.

We’ll explore these six crucial aspects of Salesforce data security to learn how to create a culture of impenetrable security:

01

Identifying What You Are You Against

IDENTIFYING WHAT YOU ARE YOU AGAINST

Low-code development is becoming increasingly popular. It opens the world of application development up to the public, and Salesforce is leading the way as a low-code development environment. However, this comes with a series of risks.

Salesforce handles a huge amount of sensitive data. Not only are these environments vast, but they are also extremely complicated. The metadata structure within Salesforce is incredibly complex. The layers of intricacies regarding critical security considerations like access settings and permissions make it much easier to accidentally introduce potentially harmful errors.

Addressing these types of issues takes time. And team members who are focused on cleaning up Salesforce environments can't spend time pushing new applications and updates forward. This slows application delivery while simultaneously creating additional risks for both data security and regulatory compliance.

How do I protect myself?

The decentralization offered by Salesforce's development capabilities, along with its very nuanced and specific architecture that promotes the ability to quickly produce applications, requires a reframing of your data security strategy.

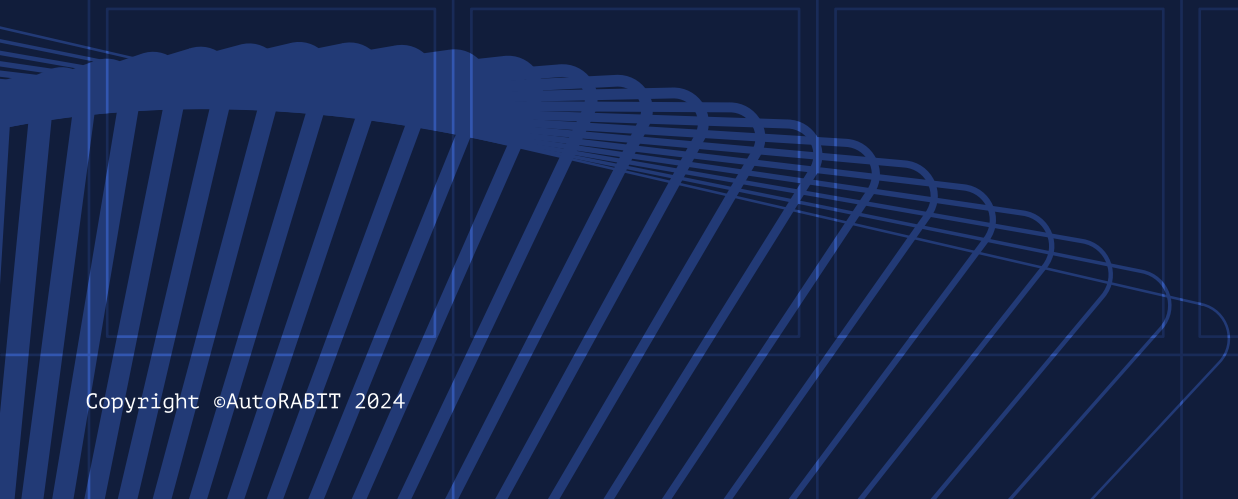
These unique challenges require attention:

- Apex code's ability to allow automatic executions
- Multi-layered, opaque dependencies
- A complex sharing model
- Unmanaged APIs that create an often-unnoticed attack surface

Specialized code analysis is a critical capability that enables your team to maintain consistent visibility over these vulnerabilities. A culture of security relies on proper tooling.

02

Understanding Data Security



UNDERSTANDING DATA SECURITY

On average, a breach is not detected for 270 days, allowing the cybercriminal to dig into your IT environment and spread. The results of this can be incredibly damaging. Companies in regulated industries like healthcare and finance could face fines and penalties for compliance failures for not properly protecting personal identifiable information or protected data.

The average cost of a data breach in the US has reached $9.05 million, but the damages can actually be much higher than that. There is another classification known as a “mega-breach,” which averages $401 million for the affected organization.

The risks of failing to protect your system are huge. This is why it’s so important to understand the data that exists within your system, which is a major challenge in Salesforce because it’s done manually.

There is no way to calculate the risk associated with Salesforce data without data classification.

It is critical for developers and administrators to understand what data is sensitive—with a higher need for protection.

How can I understand my Salesforce data better?

The data security model in Salesforce helps secure data at multiple levels from an org perspective down to an individual record.

This model provides you with the ability to secure the organization data at four levels:

Organization-Level Security: Use Org-level security measures like trusted IP ranges and Salesforce Shield as mentioned above to set up organization-wide security policies.

Object-Level Security: Use Profiles on your Salesforce org to enforce access privileges on the object level for a given domain or by provisioning specific accounts on a given profile.

Field-Level Security: Use field-level security on a given object to restrict specific fields within particular screens and reports to hide or provide read/write permission.

Record-Level Security: Use record-level security in Salesforce to customize access and share records for each profile depending on specific roles and criteria.

03

Preventing Vulnerabilities in Application Development

PREVENTING VULNERABILITIES IN APPLICATION DEVELOPMENT

A culture of security is based on an infrastructure of knowledge. The more your team knows, the better they'll be able to protect your Salesforce data. We've discussed the different ways to organize your data so you know what will need increased attention, but that is only half the equation.

Your team members also need to understand the potential types of attacks they will face. This will help them recognize vulnerabilities, so they can be addressed before being exploited.

Here are seven common vulnerabilities in Salesforce DevOps:

1. **Cross Site Scripting (XSS Attacks)**

   Applications with dynamic webpage content can potentially trick users into compromising their interactions to an attacker, who can take control of the session and execute malicious code.

2. **Cross-Site Request Forgeries**

   In a similar scenario to dynamic webpage content, attackers can incite a user to perform unintended actions to enable their malicious motives.

3. **Potential Security Leakages**

   Personal identifiable information (PII) can potentially be exposed when using a system debug and looking at your code. These references can often remain in the production code.

4. **Permissions**

   Correct user profiles need to be assigned to users according to the practice of "least privilege." Failing to assign access according to the user's intended tasks risks overexposure of data and a higher likelihood of corruption.

5. **Phishing Attacks**

   Within code, the system will check users against locations and redirects. There is an open redirect vulnerability when an application allows a user to control a redirect to forward to another URL.

6. **SOQL Injections**

   If an external system is not properly sanitized or validated before being used in a SOQL query, an attacker can inject malicious code or syntax into the query, potentially leading to data breaches, data loss, or unauthorized access to sensitive information.

7. **Duplications**

   Different variable fields should not have public access. The levels of access, such as read/write or view only, need to be reviewed to prevent exposure.

04

Navigating Salesforce API + Communities

NAVIGATING SALESFORCE API + COMMUNITIES

The infrastructure that surrounds your Salesforce environment also needs to be considered when building your data security strategy. The initial settings for these considerations can both help and hurt your security standings. An incident in 2023 highlighted this vulnerability.

The pandemic forced a lot of organizations to quickly expand their online capabilities. A rushed digital transformation led to an expediting of processes that might otherwise have been subjected to greater scrutiny.

A misconfiguration in Salesforce Community settings caused numerous organizations—including those in regulated industries—to leak private information. Unauthenticated users were able to access records that were only meant to be available after a verified login.

How can I protect my APIs and Salesforce Community websites?

The Salesforce platform is flexible in its ability to open its functionality to developers and social communities alike. This flexibility could also create possibilities for multiple security incidents outside a well-secured Salesforce instance.

Here are five best practices for these potentially vulnerable considerations:

1. Enable permissions only for specific roles and enforce these permissions as ‘API only.’
2. Allow read-only access unless necessary and enforce password-level policies and location-specific restrictions as with other roles in your Salesforce org.
3. White-list apps on a case-to-case basis and review periodically to revoke access to dormant apps.
4. Allow users the least level of privilege and selectively grant higher privileges on a case-by-case basis.
5. Enforce authenticated access of your communities, if possible.

05

Building Security Into Your Pipelines

BUILDING SECURITY INTO YOUR PIPELINES

Security considerations need to be addressed throughout your entire development cycle and into production. A constant focus on data security makes it far less likely a vulnerability will slip through the cracks—especially if everyone on your team is on the same page.

This requires a *shift left* approach to data security.

Continuous monitoring is made much easier with the help of an automated security scanning tool like CodeScan. This gives your team members the support they need to identify errors, bugs, and vulnerabilities early, so they can be addressed before they cause massive disruptions in your DevOps pipeline.

Combining the power of CodeScan's static code analysis and security posture management capabilities with other CI/CD processes offers the comprehensive visibility necessary to produce reliable updates and applications.

Not only does manually approaching security verifications slow processes, but it also increases the chances of missing something. Manual processes are prone to errors. Protecting your system from the inside out requires the use of the latest DevSecOps tooling to ensure total coverage.

Increased productivity enables organizations to expedite the release of security patches and new capabilities. CodeScan's automated capabilities double developer productivity by reducing redundant work and eliminating highly repetitive code reviews.

Proper tooling goes a long way toward supporting a successful data security strategy.

06

Supporting a Culture of Security

SUPPORTING A CULTURE OF SECURITY

An emphasis on awareness, accountability, and ownership is critical for creating and harboring a company culture focused on data security. Education is everything. This includes providing employees with initial training on how to use the tools in their daily jobs, as well as all the considerations we talked about earlier—from common attacks to vulnerabilities in the infrastructure.

Resources and support need to be available to team members at all times. Comprehensive training programs and updated information on common vulnerabilities should be continuously offered. Encourage employees to raise a concern without hesitation if they see something that might impact the security of your Salesforce environment. Open communication is critical. Your team digs into your Salesforce data every day. This is a great resource for constant oversight into the health of your system, but only if these individuals are empowered to speak their mind when they see something off.

This communication needs to go both ways. Data security awareness needs to be reinforced through various channels like frequent emails, workshops, and internal announcements.

Your team members should understand that their role in supporting security is crucial for keeping data safe. Security is not the sole responsibility of the InfoSec team—it’s up to everybody.

CONCLUSION

A successful Salesforce data security strategy requires a holistic approach. Your team members interact with your data every day, so it's essential to give them everything they need to keep these interactions from introducing new vulnerabilities.

A combination of education and access to critical DevSecOps tools will create an environment of security. Emphasizing the importance of secure practices to your team while also giving them everything they need to achieve them shows you are invested not only in your Salesforce platform, but also in them.

It can be difficult to get team members to care about security. To some, additional layers of security like two-factor authentication can become annoying. But if you successfully communicate their role in staying secure, highlight the risks of failing to protect your environment, and give them the ability to communicate their ideas, they are more likely to take a greater interest in protecting sensitive data.

Data security requires consistent efforts across your workforce. Give your team members the tools and empowerment they need to keep your data safe.

ABOUT AUTORABIT

AutoRABIT is a DevSecOps suite for SaaS platforms that automates and accelerates the entire application development and release process. This enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. AutoRABIT tools help enterprises achieve higher release velocity and faster time to market.

Features include static code analysis, automated metadata deployment, version control, advanced data loading, orgs, sandbox management, test automation, and reporting. Its services complement and extend Salesforce DX.

AutoRABIT Vault is a backup and recovery solution that streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery, and provides end-point data protection in the cloud.

CodeScan gives Salesforce developers and administrators full visibility into code health from the first line written through final deployment into production, along with automated checks of Salesforce policies.

Visit us at www.autorabit.com to learn more.

CERTIFIED
+ COMPLIANT

SOC 2 TYPE II CERTIFIED

CALIFORNIA CONSUMER PRIVACY ACT

GDPR

ISO 27001 INFORMATION SECURITY CERTIFIED

HIPAA COMPLIANT