SALESFORCE APPLICATION SECURITY

2023

Expert opinions to guide CISOs, CIOs, CTOs & other security leaders

Andy Ognenoff, Accenture

Rachel Beard, Salesforce

Shay Reddy, Hanna Andersson

Renne Devasia, InCountry

Waqas Nazir, DigitSec

Frank J. Ohlhorst, eWeek

Featuring

digitsec

COPADO

hannaAndersson

InCountry

Setting the Stage

This guide contains expert opinions with key takeaways and actionable steps security teams can use now to better secure Salesforce.

Salesforce enables organizations to rapidly innovate applications and adapt to opportunities in their marketplace.

It's no longer some third-party, outside application that a small group of teams use. It is now a vital tool utilized across the enterprise that tracks most business activities and stores the most valuable assets. Moreover, it has become the system of records for key business processes.

Given the stats below, this can present a serious security challenge for CISOs, CIOs, CTOs, and other security leaders who are responsible for application security, security operations, and GRC on the platform.

- **88% of users on the platform are over-privileged**
- **85% of attacks happen because of human error**
- **59% of IT Leaders consider 3rd-party security a top pain point**

Source: Salesforce, OwnBackup

Every day internal risk is created company-wide by human error, bad coding and simple ignorance of proper security practices. It's imperative that security be ingrained into both operational and software development processes.

For the last 24 months, DigitSec has interviewed top experts to explore Salesforce security including

- The most common and often-missed security issues
- What you and your teams can do to fix them
- Real-world examples of leading companies implementing better Salesforce security

Table of Contents

Security Execs Uncover What's Often Overlooked

Security is Your Responsibility

Top Reasons for Data Leakage

Practical Security Tips

The Salesforce Shared Responsibility Model states the platform is responsible for security out-of-the-box, but Andy Ognenoff of Accenture states,

"It really is up to the client and implementation team to use all the tools available so they're not exposing data and having security issues that are, ultimately, their responsibility."

Security issues arise and impact Salesforce because

- The platform is complex and constantly being changed.
- Many companies tend to put their "head in the sand" when it comes to security.
- There exists too much of a "wait and see" mentality or seeing security as a "nice to have."

Practical Tips

1. The top reasons for data leakage in Salesforce are over-provisioned users, misconfigured security settings and/or insecure coding practices.

2. Review your permission attributes for users and guest privileges. Always implement the principle of “least privilege.”

3. Salesforce’s supply chain of 3rd-party apps, integrations, and code can be impacting your security.

4. Review all of your connected apps and make sure they’re up-to-date. If possible, default users so they need permission to connect an app.

5. Stay on top of all Salesforce updates and make sure your teams understand WHY an update was made.

6. Don’t wait until updates are automatically enforced. This results in insecure workarounds from teams experiencing an unexpected update that affects their current processes.

7. UI is not an appropriate way to protect your data. Review your field-level security, CRUD permissions and lock down your sharing model.

8. Secure guest user access and do not solely rely on the “secure guest user settings.”

Proactive Protection Against Common Threats

Human Element is Your Biggest Risk

Identifying & Classifying Data

Practical Security Tips

What security blind spot accounts for 85-90% of attacks? The human element.

Bad actors can create risk in your organization. As you're on the lookout for their anomalous behavior patterns, do you also consider the often-exploited insider risk caused by accidental misuse of data or accidental data leakage? Busy employees may find clever short-cuts that help boost productivity, but inject security and compliance risks.

Security risk continues to be an issue in Salesforce because

- Sensitive data is not being identified and classified.
- Employees don’t understand the company’s security policies or data classification.
- There’s a lack of visibility into the customizations being built on the platform.

Practical Tips

1. All data needs be identified and classified. Conduct an audit of your internal data and identify anything sensitive as such with classifications based on sensitivity levels.

2. Prevent human error by having correctly configured access controls, roles, and permissions.

3. Be ruthless when eliminating access to any user who doesn't explicitly need sensitive PII data. This goes for your sandbox and production environments.

4. An informed team is a secure team. Train your current team and new hires on your security procedures and data classification strategies.

5. Understand the customizations and applications being built on top of Salesforce.

6. Understand how your data is being manipulated, identify possible threats, and protect it accordingly.

7. Threats are constantly evolving, as is the data privacy landscape, so you're never "done" implementing security. It needs to be a continuous process of evaluating, making changes, communicating, and monitoring.

Safeguard Salesforce Development with DevSecOps

DevSecOps Empowers Users

Real-World Challenges Solved

Security & Compliance Tips

DevSecOps empowers users to de-risk the end-to-end development process and protect Salesforce builds from security and compliance issues.

When powerful DevOps engines like **Copado** integrate security scanning from tools like DigitSec, you can practice DevSecOps throughout your entire development lifecycle and maximize ROI.

This kind of integration can help identify potential weak points in your infrastructure. This ensures all vulnerabilities are found and patched before they make it into production and disrupt supply chains.

On the next page, you will find four real-world challenges you can solve with DevSecOps and Copado.

Practical Tips

1

Stay Up-to-Date on Evolving Regulations & Policies with Compliance Checks

With automated compliance checks integrated into the development pipeline, you can ensure every code change meets the required standards before deployment.

2

Prevent Unauthorized Changes & Data Breaches with Permission-Based Access Control

Permission-based access controls allow you to define granular permissions for different team members based on their roles and responsibilities — reducing the risk of data leaks.

3

Track & Investigate Security Incidents with Continuous Monitoring and Audit Trails

Proactive monitoring of Salesforce environments with automated alerts, detailed audit trails, and incident responses can help you promptly detect and resolve potential threats before they become expensive headaches.

4

Protect Sensitive Data with Encryption & Masking

Encryption options for data-at-rest and in-transit enable safe handling of data and prevents breaches. You can also use data masking and obfuscation techniques during development and testing to safeguard sensitive data.

How Hanna Andersson Builds Brand Security and Trust

Hanna Andersson, a global provider of iconic children's apparel, needed faster and more accurate security for Salesforce Commerce Cloud to protect their brand.

Online retailer using Salesforce Commerce Cloud

Ships to 200+ countries

$100m+ in annual revenue

Hanna Andersson's Top Security Challenges

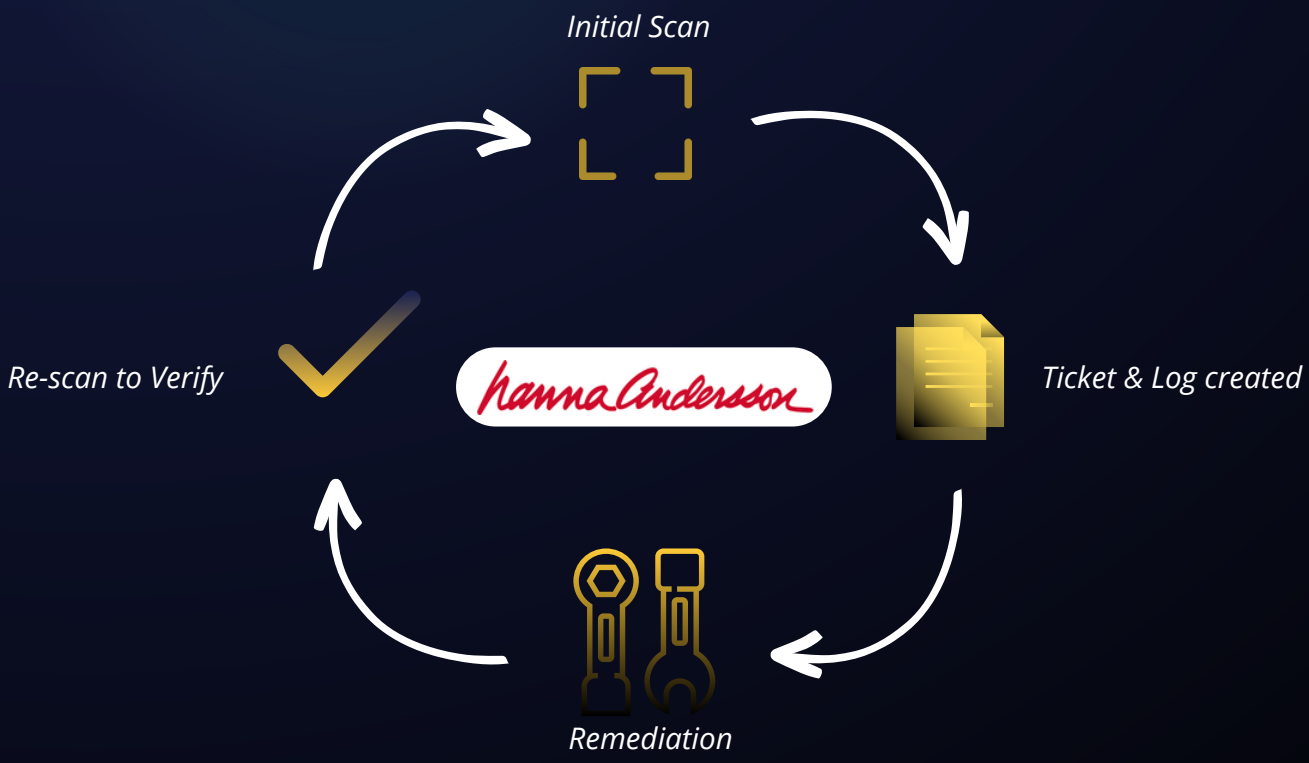
- Code was being manually reviewed which was time-consuming.
- These reviews required additional resources and were prone to human error.
- Slow security made it harder for the company to scale and have consistent results.

Shay Reddy, Senior Director of Infrastructure & Cyber Security and his team at Hanna Andersson invested in automated security scanning to replace manual reviews.

The Results

The team developed a circular process for managing risk that better protects their data. The process involves

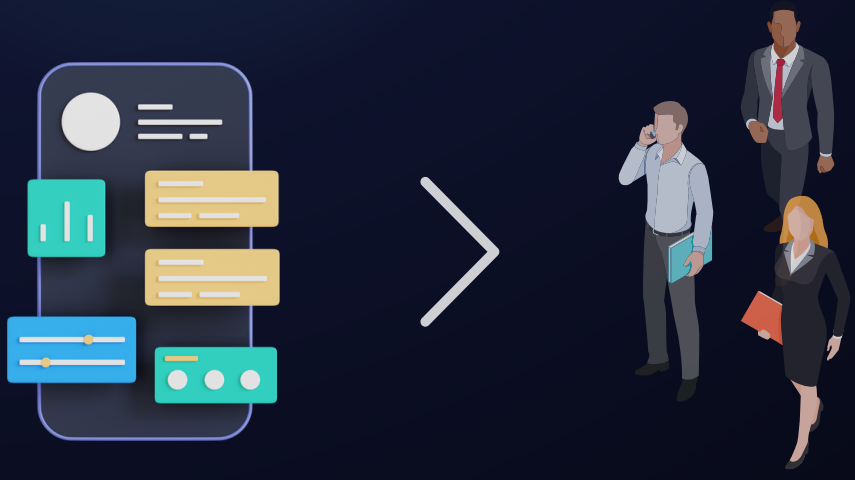
1. Automatically scanning for vulnerabilities.
2. Creating support tickets when issue are found.
3. Team fixes with included remediation guidelines.
4. Re-scanning to confirm issues were resolved.



This process saves time, catches more security issues, and can be repeated as often as needed.

InCountry Accelerates Application Security & DevOps

InCountry, a leading data residency-as-a-service platform, needed to accelerate security and development to get their Salesforce app into the hands of eager customers.



InCountry's Top Security Challenges

- Experiencing development delays due to shortcomings with their generic app security testing tools.
- Failing the stringent Salesforce AppExchange security review and delaying their app launch was not an option.
- Accelerating security without sacrificing quality.

Renne' Devasia, InCountry Chief Compliance & Security Officer, integrated automated and accurate testing that accelerated security.

The Results

The InCountry team developed a streamlined process that allows them to test, find, and fix security issues minutes after developing them.

The quick cycle of finding issues accurately and fixing them on the same day was key to accelerating their DevOps security and, ultimately, their deployment in the Salesforce AppExchange.

InCountry saved over 1000 development hours over 5 months.

Their app passed the AppExchange security review the first time.

Customers got their hands on the app months ahead of schedule.

The First eWeek Salesforce Security Review

Frank J. Ohlhorst

DigitSec Brings Much Needed Security to Salesforce & Redefines DevSecOps

eWeek, a trusted source for everything tech, confirms DigitSec “brings much needed security to Salesforce” and accelerates security by “help[ing] to redefine how DevSecOps can work efficiently in CI/CD pipelines by automating what were once difficult manual tasks.”

There’s a disconnect between Salesforce security and the “ability to create custom code.” DigitSec offers a solution to this custom development issue with it’s application security testing.

Frank gets hands-on with the tool and describes how its SAST, IAST, SCA & Config scans help “create secure code for custom Salesforce development.”

DigitSec is stated to “reduce burdens on developers" and "helps to give them peace of mind that they are delivering secure applications that follow the best practices of cybersecurity.”

Resources

Watch

Watch

Read More

Read More

Full Review

Learn More

Stay tuned for the next version of our guide with more security tips and stories of innovation.

DigitSec, Inc.

92 Lenora St. #137
Seattle, WA 98121 USA

info@digitsec.com
+1 206-659-9521

To learn more visit digitsec.com