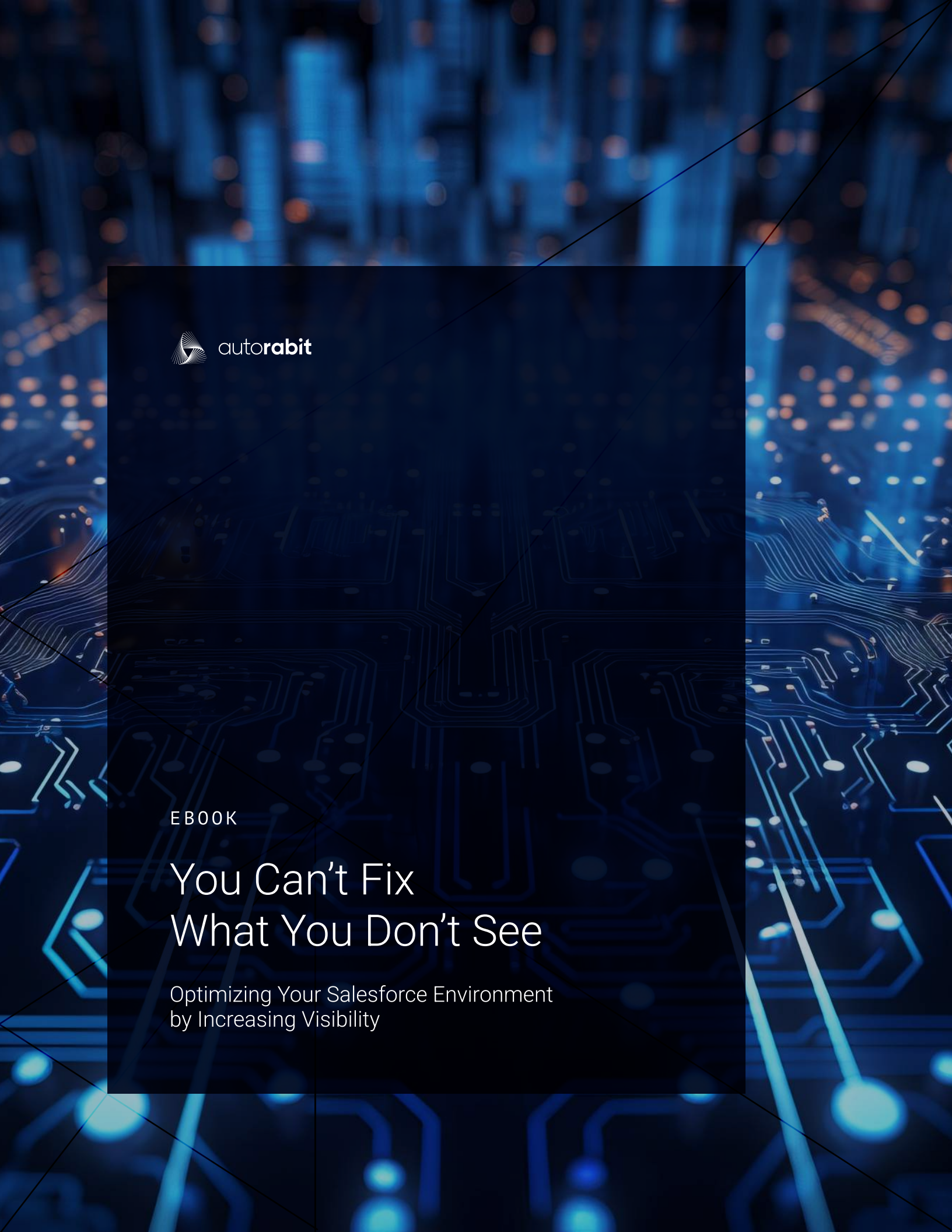


EBOOK

You Can't Fix What You Don't See

Optimizing Your Salesforce Environment by Increasing Visibility

INTRODUCTION

Quality, security, compliance—there are so many overarching considerations to keep in mind that it’s easy to get lost in the minutia. However, solidifying some fundamental strategies provides wide-ranging benefits that impact multiple aspects of your Salesforce environment.

It’s impossible to correct a mistake if you don’t know it exists. Achieving and maintaining visibility over the various processes in your Salesforce environment aids every stage of your DevOps pipeline.

Both developers and admins need support in their roles with specialized tools to produce the greatest possible results.

Achieving total visibility into the health of your Salesforce environment might seem daunting, but there are ways to establish the necessary infrastructure without a massive amount of work. We’ll discuss the benefits of increasing visibility of various parts of your Salesforce environment along with how to accomplish it.

Here are 7 ways increased visibility improves your Salesforce environment:

01

Early Detection of Vulnerabilities Increases Security

EARLY DETECTION OF VULNERABILITIES INCREASES SECURITY

Data security is an essential consideration for every business. Cybercrime threats are increasing every day, and are continuing to grow in maturity and effectiveness. These threats thrive in quiet areas of our technological platforms, silently exploiting weaknesses and causing damage while victims remain unaware until it’s too late.

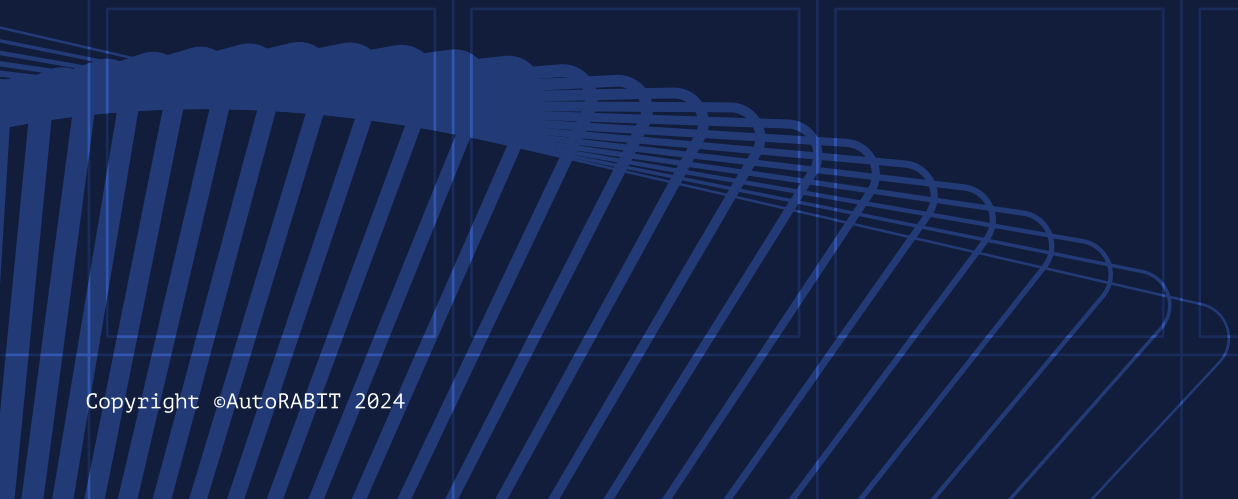
The first step in addressing a data security vulnerability—either before or after it’s been exploited—is to notice it.

Unseen breaches can be the result of a malicious actor, but they can also come from simple errors. Accidental deletions, buggy updates, and overexposed data can result in data loss events, too.

> ***How do I address this?***
>
> The first step is to address the single most influential factor in the success of an update or application: the code. Consistently strong code prevents potential vulnerabilities that result from bugs or errors.
>
> **Utilizing a static code analysis tool is the best way to enable your developers to produce quality code, every time.**
>
> Centralizing your data security efforts is a great way to maintain a consistent approach. Splitting data security oversight between devs and CISOs, for instance, creates the opportunity for gaps to emerge.
>
> Bringing all your security considerations under a single pane of glass with CodeScan allows you to keep an eye on each of these areas at once, eliminating the potential for dangerous holes in your defenses.

02

Total Coverage Enhances Quality



TOTAL COVERAGE ENHANCES QUALITY

Overseeing certain aspects of your system reduces your capacity for success. For instance, if you only have visibility over 75% of your Salesforce environment, the absolute highest success rate can only be 75%. And if you don’t have a complete security posture management tool, the chances of hitting that bar are quite low.

Mistakes happen. Feedback often strengthens a project. And if you don’t have systems in place to provide feedback or oversight for every aspect of your environment, you’re hindering your capacity for success.

Only the highest-quality code should make it to production. And only 100% adherence to internal rules should be acceptable. Failing to cover the entirety of your platform makes achieving this impossible.

> ***How do I address this?***
>
> Institute multiple layers of testing in your Salesforce DevOps pipeline. This can include tools like CI/CD to automate these checks. Static code analysis is a non-negotiable aspect of a complete DevOps strategy. Proper systems ensure your code quality remains consistently high while streamlining your processes.
>
> The rules and policies that make up your data governance and compliance strategies also need to be uniformly addressed. CodeScan’s security posture management capabilities guarantee 100% adherence to these essential considerations.
>
> Not only will foundational aspects of your platform be covered, but you’ll also benefit from automating these processes and freeing up team member time.

03

Better Information Creates Consistency

BETTER INFORMATION CREATES CONSISTENCY

Large teams get more work done, but aligning everyone’s efforts can be difficult. This can lead to a variety of challenges: maintaining quality levels, ensuring accuracy of work, and adhering to rules and standards.

Inconsistent work leads to unreliable products. Your end users—whether they’re fellow team members or clients—depend on your services. Any failures in quality or data security create dissatisfaction and cause you to lose standing in your industry.

This can all be traced back to a lack of visibility. Improper actions and results can be addressed, but only if they’re identified.

> ***How do I address this?***
>
> A typical Salesforce DevOps pipeline has a series of quality checks. The more you verify your code, the better chance you have at producing a high-quality product. These tests provide insight into how the internal workings of your development projects operate and give you a chance to rework anything that isn’t ideal.
>
> These checkpoints create consistent results, but they don’t address other aspects of your Salesforce environment.
>
> An optimized Salesforce environment also maintains insight into how people are interacting with it, how people are accessing it, and what they do when connected to the company platform. These perspectives enable you to redirect any actions that aren’t producing the desired results.

04

Immediate Alerts Reduce Costs

IMMEDIATE ALERTS REDUCE COSTS

Every business wants to reduce the costs associated with producing its products. That’s simply good business practice. But when it comes to streamlining the efforts of your team, it can be more difficult to quantify your ROI.

Reworking existing applications and updates is extremely costly—especially if mistakes aren’t noticed until after production.

Unseen errors continue until they’re corrected. And if left unnoticed, improper procedures create real problems. This is true not only for code, but also for the actions of team members. An inability to test code or maintain oversight of team members leads to accidental—but costly—errors.

> ***How do I address this?***
>
> Static code analysis is the only way to guarantee proper coding structure from the moment it’s written. This essential DevOps tool checks your developers’ code as they write it and tests it against hundreds of preset rules. Immediate alerts to improper coding structures allow them to fix these errors before they have a chance to move further down the pipeline, where they become more complicated to fix.
>
> Your code isn’t the only possible area for costly errors. Improper settings in permission sets and profiles also lead to expensive mistakes and even data loss events if they go unnoticed for a long period of time. Correcting these settings is essential, not only to avoid costly losses and compliance failures, but also to properly secure your Salesforce environment.

05

Proper Oversight Establishes Accountability

PROPER OVERSIGHT ESTABLISHES ACCOUNTABILITY

We’ve mentioned how large teams can be difficult to manage. Imagine knowing a problem exists—either you find data security vulnerabilities, poor release quality, or even a breach—but you don’t know how it started.

Accountability is the only way to maintain a secure, optimized Salesforce platform. Any failures in tracing permissions or contributions means you simply don’t know what’s going on in your environment.

It’s almost inevitable that something will slip through the cracks when working with a big team. Attempting to keep track of all that’s going on is overwhelming—but essential. Employees who continually make the same mistakes will become emboldened in their actions. And if no one has identified the error as wrong, what motivation do they have to change?

> ***How do I address this?***
>
> Having increased visibility over settings, actions, and products allows admins—and developers—to correct any mistakes. These revisions put team members on the right path to interact with their Salesforce environment in ways that fit within their overall data governance and security strategies.
>
> The benefits of maintaining proper accountability through increased visibility are evident in many different areas of your environment.
>
> An eradication of mistakes means your releases are of much higher quality. Employee errors create the potential for significant data security vulnerabilities. Reducing—or even eliminating—these mistakes further strengthens your environment.

06

Reliable Insights Lead to Better Decisions

EARLY DETECTION OF VULNERABILITIES INCREASES SECURITY

A business with a focus on its future is better prepared than one that’s constantly putting out fires. The quality of information you gather will determine whether your decisions are based on a realistic view of your efforts or not.

Using poor metrics, or failing to collect statistical information altogether, makes it more difficult for a company to properly plan its procedures and goals. Unreliable data takes this a step further and can even point a company in the wrong direction.

Which tactics provide the greatest results? How productive are your team members? Which stages of the application lifecycle can be improved? The answers to these questions start with visibility into your current processes.

> ***How do I address this?***
>
> Collecting usable data starts with DevOps tools that provide dashboards and reports. CodeScan offers two tools that provide actionable insights into the health of your Salesforce environment. This information can be used to forecast upcoming releases or analyze opportunities for improvement over time.
>
> Profile settings, permission sets, and policy parameters must be thoroughly understood to accurately plan an approach to attain your business goals. An inability to realistically grasp the status of your Salesforce environment sets your team up for costly errors.
>
> Running frequent system audits and monitoring updated dashboards produce current views of the successes and failures within your Salesforce environment. The insights gained from this analysis are key when creating an actionable plan.

07

Compliance Requires Complete Control

COMPLIANCE REQUIRES COMPLETE CONTROL

Achieving regulatory compliance requires strict attention to a series of considerations. Proper tooling is essential in order to achieve a lot of these requirements, but intentional actions by team members also factor into your company’s success in remaining within the parameters set by regulatory guidelines.

Complete oversight of these requirements is the only way to ensure your company avoids the potential fines and penalties that come along with falling out of compliance with data security regulations.

A business is accountable for the sensitive information on its platform. This includes how the data is stored, protected, and used. How can you be sure this information is consistently treated with the care it requires?

> ***How do I address this?***
>
> The first step to achieving regulatory compliance is to ensure your applications and updates are secure. A seemingly small bug can create an opening for a cybercriminal to access your system and wreak havoc. We mentioned how important a static code analysis tool is to optimize your Salesforce DevOps pipeline—and this is another major benefit of clean, safe code.
>
> Next, a company needs to be sure its employees are handling sensitive information properly. Various regulations have their own stipulations as well. Setting internal rules to address these requirements is instrumental in ensuring they’re followed.
>
> CodeScan automates the process of verifying proper adherence to these rules. Constant oversight provides the visibility companies in regulated industries need to maintain proper control over their Salesforce environments.

CONCLUSION

Ensuring the visibility of your platform—from the individual lines of code that make up your applications all the way through general adherence to internal rules—provides the infrastructure you need for regulatory compliance, adequate data security, and reliable data governance.

CodeScan is uniquely positioned to provide these essential levels of visibility into critical aspects of your Salesforce environment. This is accomplished through a multi-faceted approach to data security. First, a

best-in-class static code analysis tool helps developers create the most secure DevOps projects possible. Second,

CodeScan supports Salesforce admins in ensuring rules and policies are properly addressed. Automating these checks guarantees nothing slips through the cracks to become a costly vulnerability.

Minimizing the chances of errors, improving the quality of DevOps projects, and supporting regulatory compliance are all made easy with CodeScan. Don’t leave these important considerations to chance. Visibility is a crucial part of properly managing your Salesforce environment. Give your teams the tools they need to do their jobs right.

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.

AutoRABIT features static code analysis, automated metadata deployment, version control, advanced data loading, orgs and 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.

FlowCenter helps Salesforce delivery teams achieve heightened release velocity and DevSecOps maturity goals with flow automation, DevOps metrics, and visualization tools that can’t be found anywhere else.

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

> *“AutoRABIT has provided us with the capability to efficiently manage and tackle complex Salesforce development challenges.”*
>
> **DIEGO RIN MARTÍN,**
> HEAD OF TECHNOLOGY, SCALEFAST