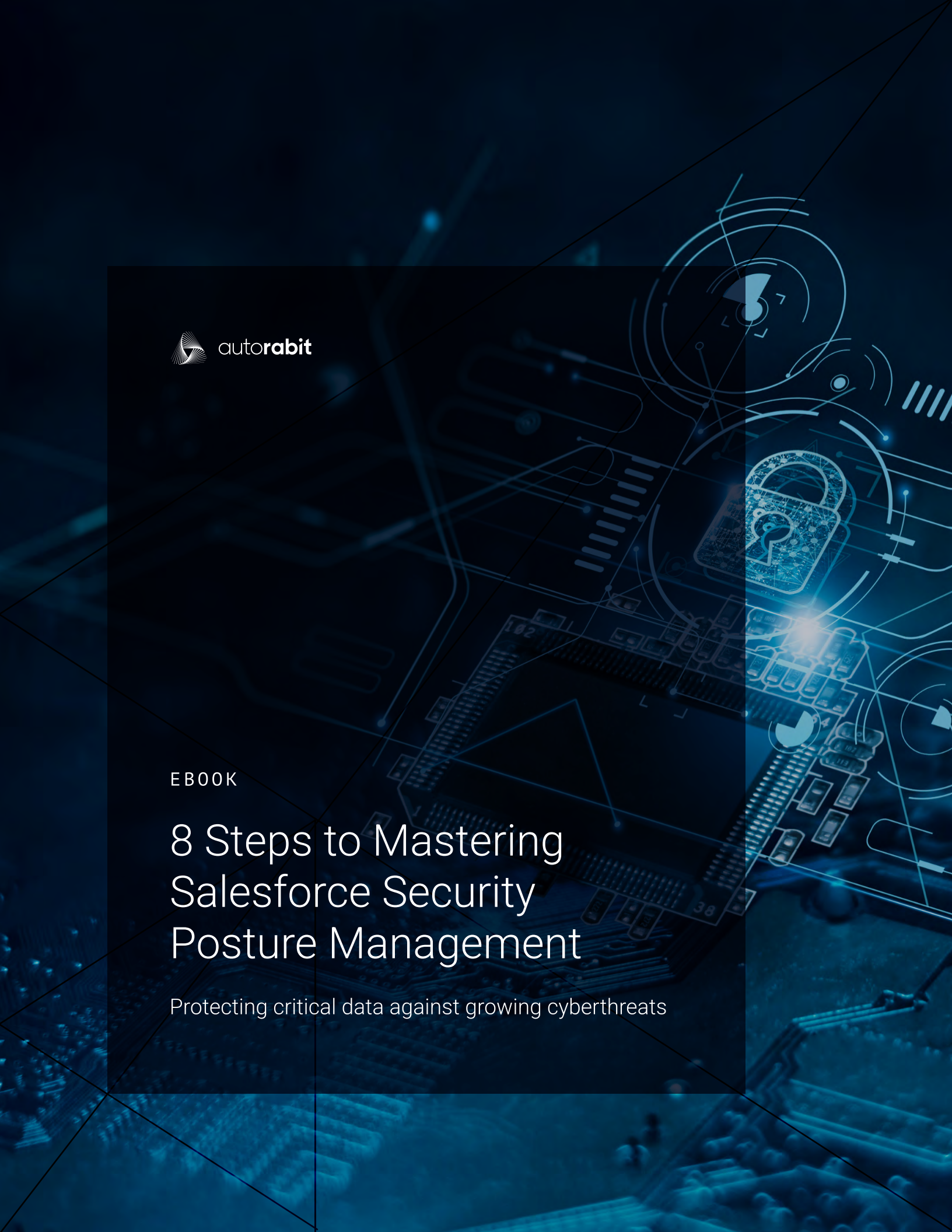


autorabit

EBOOK

8 Steps to Mastering Salesforce Security Posture Management

Protecting critical data against growing cyberthreats

INTRODUCTION

Data security should be a major concern for every Salesforce environment. Salesforce is your largest container of data. Any breaches, corruptions, or loss events can have catastrophic effects on your organization.

And these risks continue to grow. In fact, the cost of global cybercrime is expected to reach $10.5 trillion by 2025. The steps you take today will either set you up for success in the future or contribute to unnecessary—and avoidable—data security risks.

Salesforce security posture management refers to the process of assessing, monitoring, and improving security measures and practices within your Salesforce environment. It is an essential strategy to protect sensitive and critical data sets against increasing cybersecurity threats.

Those in regulated industries can support compliance efforts, but every organization benefits from increased reliability of data security systems. The first step is to simply acknowledge that data security is a priority.

Security posture management may seem daunting at first, but the benefits are immediate once the systems are in place. All you need is a little help getting started.

We'll explore these 8 steps for mastering Salesforce security posture management:

01

Assessing Your Data Security Needs

ASSESSING YOUR DATA SECURITY NEEDS

The first step to establishing a beneficial security posture management strategy is to understand your goals. What aspects of your system need to be protected the most? Where are your largest vulnerabilities? Do any compliance requirements apply to your data?

Regulations such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act (SOX) have specific requirements for various types of data. It is an organization's responsibility to determine which parts of their business are covered by these regulations and put proper protective measures in place.

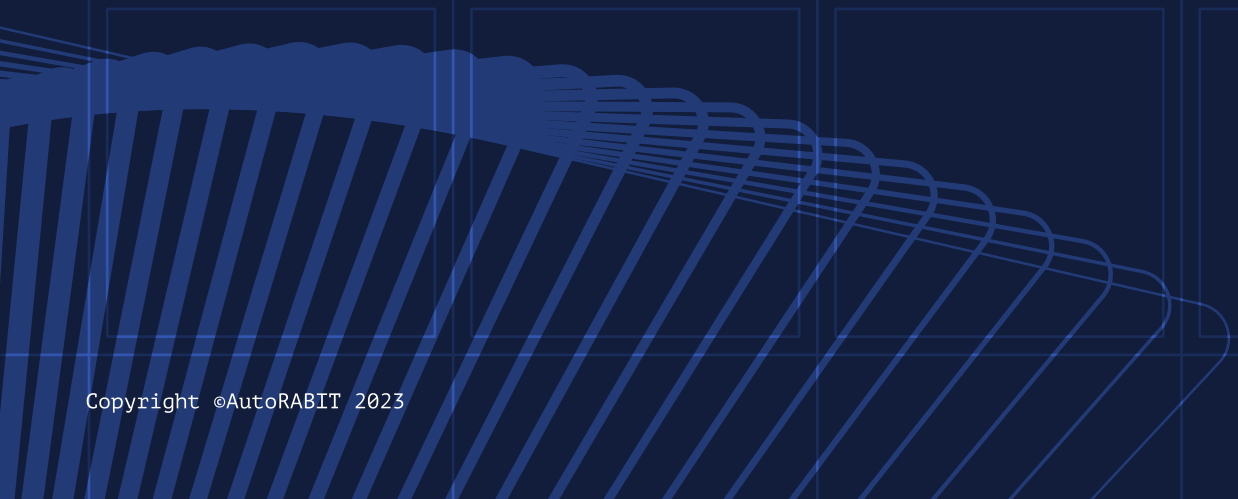
But even if these regulations don't apply, your organization still needs to analyze its data to understand where your vulnerabilities are. Personally identifiable information (PII) is a frequent target for cybercrime, along with financial information and medical data.

To identify and quantify the data, an internal audit of existing information is necessary. This includes finding, sorting, and categorizing your stored data. From there, each bucket of data should be assigned a level of risk. How damaging would it be if this information were compromised? Who would experience the negative effects—the organization or the customer?

The answers to these types of questions will help align your efforts moving forward. Your IT network needs general protections as part of its Salesforce security posture management strategy, but extra protections are necessary to further protect sensitive, critical, or otherwise guarded information.

02

Protecting Login Portals



PROTECTING LOGIN PORTALS

Once you understand the various aspects of your Salesforce environment that need to be protected within your system, steps must be taken to protect the system itself. Cybercriminals explore every potential entry point in search of a weakness. And the first place they look are login portals.

Employee sign-ins are an easy way for a bad actor to gain access to every aspect of a Salesforce environment available to your team members. They only need to break through one screen in order to have free reign over large portions of an organization's Salesforce environment.

However, there are a several simple steps that can drastically increase the security of your login portal:

Strong Passwords

Multi-Factor
Authentication (MFA)

These solutions are so simple that they are often undervalued. But make no mistake, these two steps increase the security of your login screens—it's been estimated they prevent 99.9% of modern, automated cyberattacks.

Passwords should be at least 14 characters in length and incorporate a combination of letters, numbers, and symbols. It's surprisingly easy to hack a password that utilizes words or names, so a best practice is to avoid those, as well as using consecutive letters or numbers.

Multi-factor authentication institutes a second step to the login process. After the password is entered correctly, the system sends a passcode to the user's email or phone to verify their identity. This way, even if the secure password is somehow compromised, the additional step introduces another barrier between the bad actor and your system.

03

Scanning for Proper Profile and Permissions Settings

SCANNING FOR PROPER PROFILE AND PERMISSIONS SETTINGS

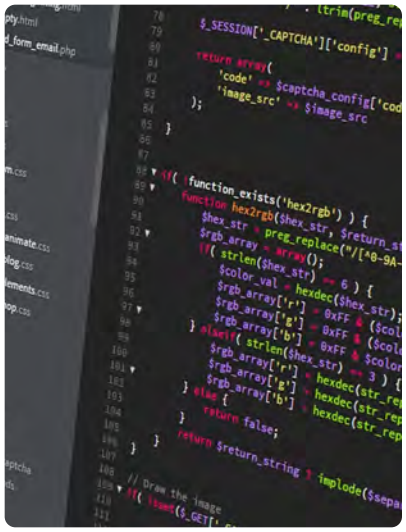
While it's easy to focus on external threats to your Salesforce environment, it's important to understand that a large percentage of data loss or corruption comes at the hands of team members. This isn't to say that employees frequently sabotage internal systems. But a simple mistake can have widespread effects that impact the integrity of critical data sets.

And since human error is unavoidable, certain considerations should be taken to minimize the potential for these mistakes to happen and to reduce their impact, should they occur.

Improper profile and permission settings are a largely unseen, but potentially dangerous data security vulnerability. The chance of an accidental deletion or exposure drastically increases with every team member who has access to a particular data set.

New and modified users need to be assigned appropriate levels of access. They should only be able to access the information they need to complete their duties. And while this might seem like a small lift for new employees, an organization's existing employees need to be checked for proper permissions as well.

CodeScan by AutoRABIT offers an automated policy scanner that can be leveraged to ensure levels of access are properly restricted across your entire Salesforce environment. Continually verifying proper permissions drastically reduces the likelihood of costly accidents that lead to the exposure, deletion, or corruption of sensitive data.



04

Producing Secure Updates and Applications

PRODUCING SECURE UPDATES AND APPLICATIONS

Flexibility is the key to not only implementing, but also maintaining your successful Salesforce security posture management strategy. And a fundamental component of this flexibility is your ability to quickly produce secure updates and applications.

Data security threats are constantly changing and evolving. Addressing new threats in a reasonable amount of time will ensure you properly protect your system data. This could include implementing patches to existing applications, performing updates to the system itself, or creating new applications altogether.

However, these updates are only beneficial if they are produced with perfect coding structures and verified functionality. DevSecOps processes and tools need to be in place to support Salesforce developers as they build new projects to address data security needs.

A static code analysis tool like CodeScan is an integral aspect of achieving perfect code without sacrificing speed. Not only does this tool reduce slow manual processes, but it also increases reliability by eliminating the potential for user error.

The failure to properly test applications and updates in order to prioritize speed leads to bugs and errors that make it through production and into a live environment. This has the potential to create faulty applications that corrupt critical data sets. It also creates back doors for cybercriminals to gain access to your Salesforce environment. Incorporating an automated code scanner maintains the speed you need without sacrificing reliability.

> *“CodeScan tools help in writing the most secure and quality code on the Salesforce platform. It's the best in the market.”*
>
> - TYRONICA O.

05

Archiving Unused Data

ARCHIVING UNUSED DATA

You Salesforce environment continues to gather more and more data over time. This is an unavoidable aspect of maintaining an IT infrastructure. However, much of this data is likely to become outdated, unused, or unnecessary. The sheer amount of data contained within Salesforce makes it difficult to find this unused information, which only exacerbates the problem.

Archiving unused data is an essential aspect of cleaning up your Salesforce environment and enabling streamlined Salesforce security posture management. It's much easier to protect smaller sets of data compared to an unmanageable, overwhelming magnitude of information.

Regularly archiving your data provides other business benefits as well, like reducing storage costs, streamlining operations, and assisting with regulatory compliance.

Reducing the amount of data in your Salesforce environment minimizes your potential attack surface. Simply put, a smaller amount of data creates less opportunity for failure. Along with that, getting rid of unused data unclogs your monitoring and protection efforts.

AutoRABIT Vault not only facilitates the archiving of unused data, but also helps you locate it. Automated scans allow you to find and flag data sets that haven't been accessed in years. This information can then be used to direct your security posture management strategy and reduce the workload of your security tools by putting unused data in secure storage outside your Salesforce environment.

06

Monitoring User Activity

MONITORING USER ACTIVITY

Establishing proper tools and strategies to secure your Salesforce environment gives you the best chance of avoiding a data breach or loss event. But simply putting these practices into action shouldn't be the end of your security posture management efforts. You must also maintain visibility over your environment to verify the success of your efforts.

You can't address a security issue if you don't know it exists. And often, breaches can occur in the background without making themselves immediately known.

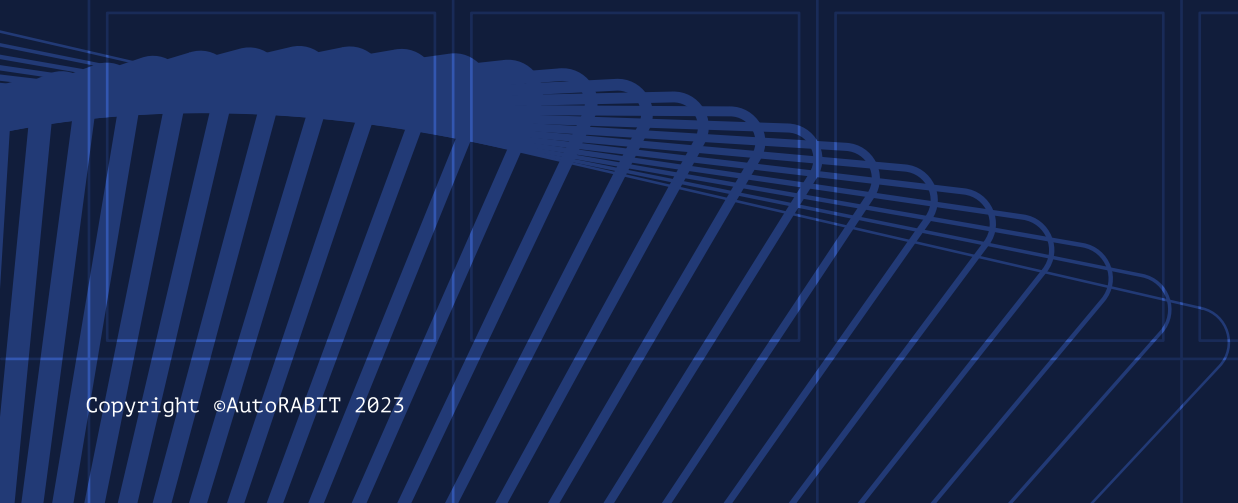
For instance, the hackers involved with Equifax breach of 2017 gained access to company files in March but weren't noticed until July. During this time, the hackers accessed millions of customer records.

This incident should've been flagged by internal scans, but something went wrong. This is why it's essential to implement a monitoring strategy and to keep it up to date.

Access logs, event reports, and regular reviews of user activity can point to anomalies that have sneaked through your data security measures.

07

Connecting External Applications



CONNECTING EXTERNAL APPLICATIONS

One of the most frequent ways Salesforce users introduce new data security vulnerabilities into their environment is by connecting third-party applications. Utilizing a platform like MuleSoft to connect a Salesforce environment to external applications can streamline many business processes. However, improperly configured settings can lead to problems.

Sensitive information is stored inside the configuration files that flow between the Salesforce environment and the third-party platform. A failure to properly protect this data can result in costly exposures and breaches—and even falling out of compliance with data security regulations.

AutoRABIT's MuleScan analyzes the security settings of these configuration files to ensure vulnerabilities aren't introduced into the system. For example, this tool can check if the credentials for a third-party database are properly defined to guarantee files are properly encrypted.

The configuration files associated with MuleSoft APIs are scanned to identify and remediate potential vulnerabilities and cybersecurity risks.

A comprehensive Salesforce security posture management strategy addresses all aspects of a Salesforce environment—this includes the external applications linked to your platform. Software like MuleSoft can be a huge help in getting the most from your Salesforce environment, but only if it's properly configured and protected.

08

Providing Ongoing Security Training

PROVIDING ONGOING SECURITY TRAINING

It’s important to remember that there is no such thing as being 100% secure. There are simply too many threats to completely guard your system against data loss events. Awareness is essential to remaining vigilant against cybersecurity threats.

A vital aspect of a stable Salesforce environment is ensuring your team members are not taking unnecessary data security risks. And the best way to do this is by keeping lines of communication open between departments and instituting ongoing security training.

Phishing, for example, continues to pose a major threat to an organization’s data security. A simple employee mistake can grant a cybercriminal access to your Salesforce environment and expose sensitive information. The best way to protect your data is by keeping your team vigilant against these types of threats and continually reminding them how to spot phishing attempts.

The types of training offered to employees depends on their role in your company. Data protection training, incident response, and continuous auditing should all be addressed by various team members. However, basic cybersecurity awareness training should be offered to every employee on a repeating schedule.

Your Salesforce security posture management strategy is only as successful as its weakest link. Continued training on spotting threats, compliant processes, and threat intelligence raises the bar for data security.

CONCLUSION

Salesforce security posture management is a broad strategy. There are numerous tools, processes, and considerations to keep in mind to adequately protect critical data. Failing to address these concerns can lead to costly outages, exposure of customer data, and falling out of compliance with data security regulations.

Carefully considering the 8 steps outlined in this ebook will provide a flexible roadmap that organizations of all sizes can use to increase their levels of data security.

But remember, data security is not a one-time consideration. Proper security posture management is an ever-evolving strategy. New threats continue to emerge daily. Organizations will grow and find new security vulnerabilities along the way.

It’s important to maintain oversight and attention to data security measures. You can’t guard against every potential threat, but you can take every precaution possible to protect your most sensitive information.

ABOUT AUTORABIT

AutoRABIT is a DevSecOps suite for SaaS platforms, which automates and accelerates the entire application development and release lifecycle. 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 comprehensive backup and recovery solution that streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery, and provides endpoint 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.

Record Migrator enables automatic bundling of all feature dependencies for Salesforce-managed packages. The deployment of templates ensures fast, efficient, and seamless releases.

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 helped us add a lot of automation to our software development lifecycle. I highly recommend it!"*
>
> - FORREST COOK