10 Proven Methods to Prevent Salesforce Cyberattacks

EzProtect
By Adaptus

10 Proven Methods to Prevent Salesforce Cyberattacks

EzProtect
By Adaptus

These 10 tips are the proven BEST ways to protect your sensitive data in Salesforce from attackers. By utilizing these methods, you'll have fortified your security and closed the loopholes that make it easy for cybercriminals to accessing your company's data.

1 Require Multi-factor Authentication

THREAT:

Cybercriminals have access to billions of credentials that are readily available to them over the dark web and other resources. If they choose one of your user's credentials, your company's and customer's data and secrets could be at risk.

SOLUTION:

Multi-factor authentication is most effective ways to protect against this type of attack, requiring users to enter at least two factors to gain access to Salesforce. Typically, one of these factors is a username and password, which is something you already know. The other could be either something you have like a cellphone, a key card, or other device that could verify your identity.

Adding this secondary factor as a requirement for all of your Salesforce users is very easy to setup, protects your privacy, and is a very effective deterrent against would be attackers.

---

2 Lock sessions to the domain in which they were first used

THREAT:

A common type of attack called session hijacking can occur where an attacker could potentially gain access to your Salesforce resources from a domain that is different from the original domain to which the session was initiated.

SOLUTION:

With this setting enabled, this helps to prevent this type of attack.

One example of this could be a community user who decided to try to jump over to another community where they should not normally be able to access. Since Salesforce had already authenticated the user, they could potentially access data that would not normally be exposed in the originating community.

CONTINUED »

3 Lock sessions to the IP address from which they originated

THREAT:

Attackers will commonly use session hijacking where they use a user's valid session to access a site as if they were that user. Once successful, an attacker can do anything that the user can do on the site. This is typically performed by stealing a user's session cookie or token that is temporarily stored on their computer to access the site.

SOLUTION:

Since in most cases, an attacker would have a different IP address than that of the user, locking a session to the IP address from which the session was initiated shuts out the attacker.

Although this is a very effective security mechanism, many times it is just not possible to enable since many integrations sometimes will use multiple IP addresses to deliver a service.

Take care to test that enabling this security setting doesn't adversely impact your end users.

---

4 Require HttpOnly attribute

THREAT:

Many attackers will try to inject client-side scripts that try to access and steal an end user's browser cookies that could grant an attacker access to Salesforce as that user.

SOLUTION:

The HttpOnly attribute is a protection mechanism that protects from this type of attack. Once enabled, this prevents access to browser cookies through client-side scripting.

CONTINUED »

5 Setup maximum invalid login attempts and lockout effective

THREAT:

A commonly known way that hackers try to penetrate systems is by using what is called a brute force attack.

During this attack, a hacker will use a trial-and-error process to guess a user's password to try to gain access to a system.

SOLUTION:

Setting the maximum number of invalid login attempts blocks this type of attack, as after a user attempts to login a specified number of times with an invalid password, their account is then locked for a specified amount of time.

Using these security features in Salesforce will limit the number of passwords that an attacker can guess, making it almost impossible for them to guess a user's password.

In order to limit an attacker from performing a brute force attack, you should set the "Maximum invalid login attempts" setting to 3, and the "Lockout effective period" to 15 minutes.

CONTINUED »

6 Setup Strong Password Policies

THREAT:

A commonly known way that hackers try to penetrate systems is by using what is called a brute force attack.

SOLUTION:

Another way to avoid a brute force attack is to ensure that you have configured Salesforce to enforce strong password requirements for all your users. This helps to ensure that your users do not create passwords that can be easily guessed, and so that they do not keep reusing the same password.

The following are the recommended minimum strong password policies that should be set in Salesforce:

Password Complexity Requirements – Set to "Must include 3 of the following: numbers, uppercase letters, lowercase letters, and special characters"

Minimum Password Length Requirement – Set to a minimum length of 12 characters.

Password Expiration Policy – Set passwords to expire at least every 90 days

Enforce Password History – Set to "24 passwords remembered". This should limit users ability to reuse the same password.

CONTINUED »

7 Require VPN access for all employees that login to Salesforce

THREAT:

Attackers are constantly trying to penetrate company systems and applications by trying to gain access to your users' systems, sessions, and by cracking their passwords. Once an attacker is able to successfully gain access to valid user credentials, they have complete access to your company and customer data, just as the user would.

SOLUTION:

VPN access is key to securing your network and application, giving you a higher level of control of who can access company data. Even if an attacker has valid credentials, without access to the VPN, the attacker won't be able to access your company resources.

Whitelisting your company IP addresses is a must—preventing users who are not connected to VPN from logging into Salesforce.

If employees are working from home, they must log in to the company VPN to connect from one of those whitelisted IP's. Otherwise, they must log in from a company office. This makes it easy to spot IP addresses you don't recognize that may be accessing your data, saving you time and resources from having to shoot down threats as they pop-up.

Increase/Upgraded Security

BE SURE to require employees to stay logged into your VPN once they are logged on to Salesforce, otherwise they may bypass your network virus scanning gateways, making them vulnerable to malware and hackers. This can be done by enabling the feature "Enforce login IP ranges on every request" in Salesforce.

CONTINUED »

8 Set all Objects to Private in Sharing Settings

THREAT:

Salesforce allows for very granular controls for how users are able to access company and customer data. It is because of this that it is also very easy to accidentally open up access to private data that users should not see.

With Salesforce Digital Experiences (Communities) this is even more of a risk as you could accidentally share company and customer data with users outside of your company.

SOLUTION:

Sharing settings in Salesforce control at the highest-level what records users are able to see.

It is a best practice to enable the most restrictive setting of “Private” by default for all objects. This will help to ensure that you do not accidentally provide access to data that users should not see. Specifically, since sharing setting defaults can be applied to both internal and external community users.

Once you have locked down all of your object by setting them to “Private” access, you can then open up access by creating “Sharing Rules” allowing users to access only the data they need to see to perform their job function.

CONTINUED »

9 Run Salesforce Security Health Check

THREAT:

Salesforce is an amazing business tool, but also is extremely complex. There are a large number of security related settings and controls to help protect your company and users from attackers and data leaks.

Because it is so complex, it is very easy to misconfigure these security controls, allowing attackers easy access to your company and customer private data.

SOLUTION:

Salesforce provides a tool called “Health Check” that available in the setup menu that informs you of how well your Salesforce environment meets Salesforce security standards.

This tool helps you reduce your security risk and help prevent the loss of sensitive data. The tool will analyze your Salesforce environment and identify areas where your Salesforce security may be at risk, and in many cases can even fix the issues right from the tool!

CONTINUED »

10 Proven Methods to Prevent Salesforce Cyberattacks

EzProtect
By Adaptus

10 Conduct audits to ensure compliance with cybersecurity best practices are up to date

THREAT:

Security is not a one-time activity, but more so an ongoing activity. The security landscape is constantly changing with attackers finding new ways to penetrate systems. It is because of this that software vendors such as Salesforce are constantly adding new way to block these attacks.

Additionally, because system administrators are constantly servicing access requests for end users, it is very easy for your existing security settings to become stale, or misconfigured, opening up holes for attackers to penetrate your systems.

SOLUTION:

Auditing gives your team peace of mind that all cybersecurity best practices are up to date and properly adhered to. It also allows for self-reflection on where your team can improve.

Regularly checking the Salesforce Security Health Check, Setup Audit Log, and Salesforce field history in Chatter will help to ensure that your Salesforce security is locked down tight and help you to know who accesses your data and when, so that you can better identify irregular patters of access.

Additionally, Salesforce Shield event monitoring can also provide you with an additional advancer layer of monitoring that is not available out of the box.

Make sure you create a cadence for running these reporting tools, and promptly review them to make sure all user access levels are what you expect.

IN SUMMARY: If your company practices good data protection and uses Salesforce, you might think you're covered when it comes to virus detection and prevention. But unless you are using a 3rd party system to scan files for viruses in Salesforce, you are vulnerable to cyber-attacks. EzProtect can help!

For more Information about how you can protect you and your business assets, visit www.adaptus.com