EZPROTECT®
VIRUS PROTECTION FOR SALESFORCE.COM

Salesforce Virus Protection for Large Enterprises

Salesforce Virus Protection for Large Enterprises

According to Symantec, half a billion personal records were stolen or lost due to nine mega-breaches in 2015. The number of exposed identities jumped to 429 million. Even with security technology constantly improving, governments and businesses are more vulnerable than ever. As the hackers continue to breach the barriers of security, it is on the shoulders of governments and large enterprises to do everything they can to prevent attacks.

Salesforce does NOT provide a way to prevent users from uploading certain types of files, or to scan attachments, document uploads, or chatter for viruses or malicious content. This is a huge security risk for all Salesforce users, especially when a Salesforce application is publicly exposed through communities and sites.com. Thankfully, EZProtect® by Adaptus is a solution.[1]

EZPROTECT®
VIRUS PROTECTION FOR SALESFORCE.COM

Protecting Your Salesforce Org

With a simple, elegant, world-class solution to protect against viruses of all types.

Community Portals

EZProtect is designed to scan community portals (internal and external) for malicious software.

Chatter & Content

EZProtect scans chatter, documents and any uploaded content within Salesforce.

Customization

EZProtect was developed for flexibility and may be customized to accommodate special requirements for governments and large enterprises.

Enterprise Business Solution

Designed for large enterprises, EZProtect easily scans chatter files, documents, attachments, and content for harmful viruses within all variations of Salesforce including standard orgs, community portals, and chatter. Through careful and clean design, EZProtect makes the detection and deletion of viruses, malware, Trojan horses, and other malicious threats effortless and painless.

Key features include:

- Scans Salesforce chatter files, documents, attachments and content for harmful viruses.
- File-type scanning allowing users to specify a list of file types that are allowed or denied (white list or black list)
- Scanning of PDF files that contain JavaScript and therefore may contain malicious code
- Scanning of static resources, as well as document, attachment, and content versions
- Skip or filter scanning of one or more of the four main delivery avenues for harmful content within the Salesforce org (see threat vectors below).
- Commercial or Gov. Cloud Hosting –hosting services on Amazon AWS and/or Gov. Cloud Regions.
- Multiple “Org” connections – connect several Salesforce orgs to EZProtect. There is no limit.

By default, EZProtect scans for viruses, malware, and Trojan horses with an add-on capability to scan for JavaScript content in PDFs (JavaScript is executed when PDFs are opened in the browser). It also offers the additional ability to rescan existing files already present in the system to look for viruses and other threats that have been identified since the file was initially uploaded.

Scanning within Multiple Areas

- Communities
- Salesforce Orgs
- Public Sites

Current Threat Vectors

Simply put, any file that is uploaded to Salesforce brings with it the opportunity to carry a virus, malware, or unintended active content. There are four main avenues for delivery of these types of files within Salesforce:

1. Attachments associated with cases, leads, opportunities, etc.
2. Documents
3. Content Files, including chatter attachments
4. Static Resources

Standard Threat Scenarios

There are four standard scenarios which should be addressed within any Salesforce organization.

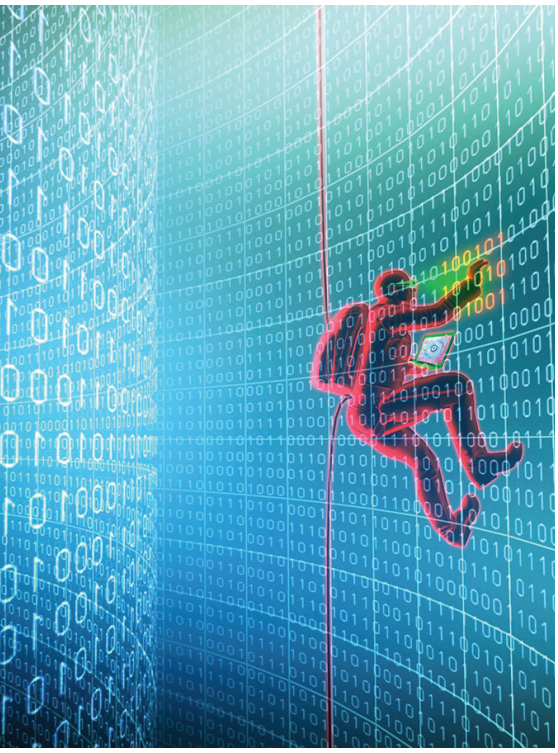
A. Files that are uploaded by customers or partners and opened by customers or partners
B. Files that are uploaded by employees and opened by customers or partners
C. Files that are uploaded by customers or partners, and opened by employees
D. Files uploaded by anyone which contains a virus that is not yet recognized by scanners, but is eventually.

Scenario A is probably the most severe threat. You don't know if the customer or partner has a virus scanning capability on their documents — either on the sending or the receiving side. You don't know if they are malicious actors trying to intentionally harm other customers or your company. You also want to show legal and compliance officers that you are making a best effort to protect your customers and partners.

Scenarios that deal with employees can be dangerous as well. Many organizations do have policies and practices to include virus scanning software on all of their internal computers. However, this software may not be up-to-date as they are often installed on each individual system, and current viruses will be missed. In addition, employees increasingly bring-their-own-devices into their work, including tablets, phones, and personal computers which may not include virus protection. Many corporate and government environments do not lock these devices out.

In Scenario D, at the time of initial upload, a file is scanned by a virus protection software and marked as clean as the virus was missed or not yet recognized. So, although the virus scanner marked it as clean, the file actually contained updated malicious content that the virus scanner missed. This scenario is quite a large threat as all virus scanners are only as good as the currently known dictionary of viruses, and hackers are constantly coming up with new pieces of malicious code.

Standard Objections



"EZProtect has worked seamlessly, and we are much more relieved to know customers who work with us in the SalesForce environment are protected."

— Qing Lin, Policy & Budget Analyst
Colorado Department of Transportation

Scanning via Email - "Why do we need EZProtect when we already have a virus scanner for our email systems? All files we upload to Salesforce would have already been scanned."

Answer: Scanning within email is not fool proof as many viruses are missed, and things can still get through. EZProtect itself is not fool proof either, but the more applications you have in place to prevent malware and viruses, the more protected a company will be.

Triggers within Salesforce - "All you have to do is create a trigger on an Attachment object."

Answer: When detecting a virus, organizations need to know when files are being uploaded in addition to detecting viruses. Triggers only handle the detection of the file being uploaded, not the detection of the virus. In addition, triggers can fail to fire when there are multiple updates to the same record within the same transaction. In other words, triggers will always fire when there is an update, but if there are multiple updates to the same record, a trigger will only fire twice to stop an infinite loop of updates to a record.

Bottom Line

Cyberwarfare is an ongoing threat that will only continue to gain more traction. Relying on virus protection on personal PC's in not a sufficient cybersecurity strategy as it will not protect against mobile uploads, community chatter, and public sites within the Salesforce application. The best way to prevent an attack within Salesforce is to install the EZProtect anti-virus software within the org (or multiple orgs) directly to fend off the four threat vectors previously mentioned. It is also important to educate IT staff and end users on the ins-and-outs of how the system works to create awareness about the multiple opportunities for hacking within Salesforce.

TECHNICAL CONSIDERATIONS WHEN SELECTING A VIRUS SCANNING SOLUTION

When it comes to the security of your organization, you should not take the decision of choosing the solution protecting your organization lightly. Not all virus-scanning solutions are created equally. Make sure you ask the following questions before deciding.

Do you scan the entire file, or just the checksum?
Many virus scanners will only scan a part of a file looking for the virus signature in the checksum. In the old days, this was effective, but now viruses are created that make this method ineffective. EZProtect always scans the entire file to ensure that nothing is missed when scanning for viruses.

How often do you update the virus definitions?
Virus definitions are the key to identifying a virus. If the definitions are out of date it is possible that a virus could not be detected. EZProtect updates the definitions not once, but multiple times per day, to ensure that we always have the latest virus definitions.

Do you just scan the files once, or do you rescan files for viruses routinely?
New viruses are discovered every day. It is very possible that a file may have a virus and was scanned, but no virus was found because the virus was not yet known. That is why you must rescan your files routinely to make sure that you do not have infected files with a virus that was previously unknown. As an optional service EZProtect can rescan your files on a routine basis.

Do you scan the content of the files to ensure there are no malicious scripts within the files?
Many files can contain scripts that are not technically viruses, but can harm user systems. Many virus scanners overlook this type of detection. The enterprise edition of EZProtect currently can detect malicious scripts within PDF files and we are currently developing other methods of detection within other types of files as well.

Once a file is uploaded how quickly do you scan the file?
EZProtect uses a polling method to scan for viruses. Once a file is uploaded the file is scanned typically in less than a minute. Some solutions use Salesforce triggers to scan for viruses. This can be unreliable since triggers do not always fire. Additionally, triggers are not supported on every Salesforce object where files can be uploaded. Therefore, we use polling since this is the most effective method to make sure all files are scanned.

Do you offer the ability to immediately scan files as soon as they are uploaded?
In certain circumstances, such as public facing websites, we can offer an immediate scanning solution that can plug-in directly to your website or community.

Scanning files is a very processor intensive process. What measures have you taken to ensure that your infrastructure doesn't get overloaded with requests?
We designed EZProtect with performance in mind from the ground up. Our infrastructure is load balanced and has built-in monitoring that will automatically scale up our resources to ensure that we always have the resources to meet the demand of our customers. Be careful when looking at solutions built entirely on Salesforce, as Salesforce limits the ability for the scanning solution to scale to large volumes.

EZProtect FAQs

Where is the EZProtect application hosted?
Our standard is to host on Amazon AWS EC2 nodes. We also have servers in the Gov Cloud Region where appropriate. If a client requires an on-premises environment, we may accommodate with customization services, but it is significantly more expensive.

Why is EZProtect not hosted directly on Salesforce?
The nature of scanning files for viruses is a very processor and memory intensive process. The Salesforce platform is currently not a good fit for these types of tasks. Although it is technically possible to build a scanner directly on the Salesforce platform, doing so would limit the scanner's ability to scale to fit large enterprise needs.

How many Salesforce orgs can we connect to EZProtect?
There is no hard limit to the number of Salesforce orgs that may be connected.

How long does it take for a new file to be scanned?
The standard offering polls for new files every minute. The files are scanned immediately after the query. The exact timing depends on the number of files that need to be scanned.

How was the polling interval chosen?
The polling interval was set to balance the desire to have the files scanned as quickly after uploading as possible against the constraints of the API governor limits. There are four different objects that hold files in the system. Querying all four every minute incurs almost 6,000 api calls per day, even without any API calls from scanning files or reporting results.

Where do you get your virus definitions?
EZProtect primarily uses an open source virus database, which is actively maintained with daily updates.

How often are the virus definitions updated?
The virus definitions are updated four times per day to ensure that the most up-to-date definitions are always being used for scanning.

Can you scan files before they are uploaded to Salesforce? If no, why not?
No. Unfortunately not. But there are certain instances that you could scan certain types of files before they are uploaded into Salesforce through communities and portal users with customization. We're happy to discuss requirements and discuss options.

What happens when a file with a detected threat is found?
In a typical configuration, after an infected file is found, the file is deleted and a notification is sent. There are a number of different options for handling of notifications that may be set during the EZProtect configuration.

What happens to a file that is deleted?
EZProtect makes use of the Salesforce standard mechanism for handling of deleted files. They are stored in the recycle bin for up to 15 days. There is also a storage size limit for deleted files, so if the limit is reached, the deleted files may not last the full 15 days. See the Salesforce documentation for more details: https://help.salesforce.com/apex/HTViewHelpDoc?id=home_delete.htm

Do you scan existing files or re-scan files periodically as new virus definitions are found?
We recommend initiating a scan of all existing files (as an additional service) at the time of service activation. The standard offering of EZProtect scans newly uploaded files only.

Once the files have been scanned, the client may determine the frequency in which they are re-scanned (weekly, monthly, quarterly).

Are files securely transferred between the Salesforce org and EZProtect application?
Yes. EZProtect uses the same secure transport that customers use to connect their browsers to the Salesforce system (HTTPS/TLS).

How are files transferred to the EZProtect Application?
Using the same, industry standard, secure transport (HTTPS/TLS) that customers use to upload their files to Salesforce.

Are files persisted (saved) to disk on the EZProtect server?
Files are cached to a RAMdisk for the duration of the scanning process and then immediately deleted. There is no long-term storage of files, and the temporary storage does not use persistent media.

What options do we have for notifications?
Notifications can be sent via Chatter or Custom Objects. We recommend these updates post to a private Chatter group for full transparency. Notifications may also be written to a specifically configured custom object by Adaptus, or one may be configured by your SFDC Admin.

ABOUT ADAPTUS

Adaptus, LLC is an application development and Salesforce architecture consulting firm based in Austin, TX. Founded in 2012 on the premises of collaborating with customers to solve real problems, Adaptus products are used by large, Fortune-500 companies with thousands of users. Adaptus provides reliable, high-quality and cost effective information technology solutions and custom cloud-based computing applications designed to integrate with Salesforce.com. Our applications and architectural consulting services help businesses optimize their operations by working smarter, while increasing productivity and profitability. Led by certified Salesforce architects, Adaptus specializes in customer-driven product solutions to provide highly relevant, efficient and cost-effective solutions for large-enterprise users around the globe. For more information about our products, or to request consulting services, please visit www.adaptus.com.

CURRENT CUSTOMERS

E*TRADE® CalEPA California Environmental Protection Agency CDOT CO COLORADO Department of Transportation

---

Download 30-Day Free Trial

www.adaptus.com/ezprotect

800-955-0573

Footnote: (1) Cybersecurity Research: Weak Links, Digital Forensics, and International Concerns, Tech Pro Research, September 2016.