Salesforce Cybersecurity & Virus-Scanning Myth Buster Fact Sheet

EzProtect
By Adaptus

Salesforce Cybersecurity & Virus-Scanning Myth Buster Fact Sheet

EzProtect By Adaptus

If your company uses Salesforce, you might think you're covered when it comes to virus detection and prevention. With hundreds of thousands of users storing confidential information on the platform, Salesforce is widely renowned for the amount of key company information they store. But without proper Salesforce cybersecurity precautions in place, your company could be at risk of losing millions or even billions in business.

As a trusted Salesforce partner, EzProtect has compiled several little-known myth busters to ensure your team is up to speed with Salesforce cybersecurity and virus scanning best practices - minimizing your risk for loss.

MYTH:

All my employees' and customers' files uploaded to Salesforce are scanned for viruses.

REALITY:

Salesforce does not directly scan files uploaded to the platform for malware, ransomware, or other threats. Instead, Salesforce relies on partners like EzProtect who specialize in virus scanning to help keep customer data safe.

MYTH:

Salesforce blocks users from uploading file types that are considered high risk for infecting my employees with a virus.

REALITY:

Salesforce lets you block users from uploading files that have specific extensions or mime-types. Although this is a semi-effective method at blocking users from who do not have any malicious intent, this safeguard is completely ineffective against professional cybercriminals who target your organization for attack. Many attackers bypass this safeguard by changing the extension of a file to fool users and systems that block extensions.

Mime-types are a self-reported file type reported by the web server sending the file. Many attackers will stand up their own server with the purpose of sending malicious files that are executables with a virus, but tell the receiving server, in this case — Salesforce, that the file is a plain text file, completely bypassing the blocking mechanisms in Salesforce.

With EzProtect's true file type detection and virus scanning capabilities, you can easily detect the true type of a file and block users from downloading these files.

CONTINUED »

Salesforce Cybersecurity & Virus-Scanning Myth Buster Fact Sheet

EzProtect
By Adaptus

MYTH:

My email server already scans all files for viruses for me.

REALITY:

If you're using Salesforce for email-to-case, you aren't as protected as you may think. Email-to-case makes you vulnerable to downloading malware sent as attachments.

The risk here is twofold.

Email servers don't catch as many threats as you may think, allowing malicious content to pass into your Salesforce hub via email-to-case. Even if you use trusted email servers like Gmail or Office365, you're still at risk of malicious files making their way past server scanners and uploading directly to Salesforce.

Salesforce also doesn't have the capability to scan email-to-case attachments for viruses. This opens up another opportunity for malicious content to enter, bypassing gateway, desktop, and email virus scanning solutions and downloaded directly onto your computer.

EzProtect closes the email-to-case virus loophole — detecting and removing malicious files and content, protecting you and your users, powered by Sophos, an industry leading scanning engine, proven to stop threats in their tracks.

MYTH:

My employees' computers already scan for viruses and malware.

REALITY:

Especially in a remote work environment, how certain are you that employees are keeping their technology updated? Think about how many times you ignore the notification that it's time to update your own computer.

Without knowing all your company-distributed technology is regularly updated, the virus engine and definitions itself on a computer could be out of date. With remote work becoming a more widespread common practice, there are less employees protected by corporate networks making it much more difficult to control and ensure that all systems are closed secure loops.

CONTINUED »

Salesforce Cybersecurity & Virus-Scanning Myth Buster Fact Sheet

EzProtect
By Adaptus

MYTH:

Salesforce protects me while my team interacts with the public to resolve tickets.

REALITY:

If your work involves the general public (e.g. submitting tickets or uploading files to your Salesforce environment) you need a Salesforce virus scanning software. By the very nature of interacting with the general public, you don't control their computers and are not able to authenticate or verify their intentions the same way you would employees. Files that carry malware within them can easily be uploaded to your Salesforce system. Use EzProtect to keep your systems secure.

MYTH:

My employees have to connect to VPN to log in to Salesforce and are protected by our virus scanning gateway.

REALITY:

Most cloud systems, including Salesforce, only require that you are connected to VPN to authenticate. Once authenticated, employees are free to disconnect from the VPN, making them, and your client data, vulnerable to cyber-attacks.

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