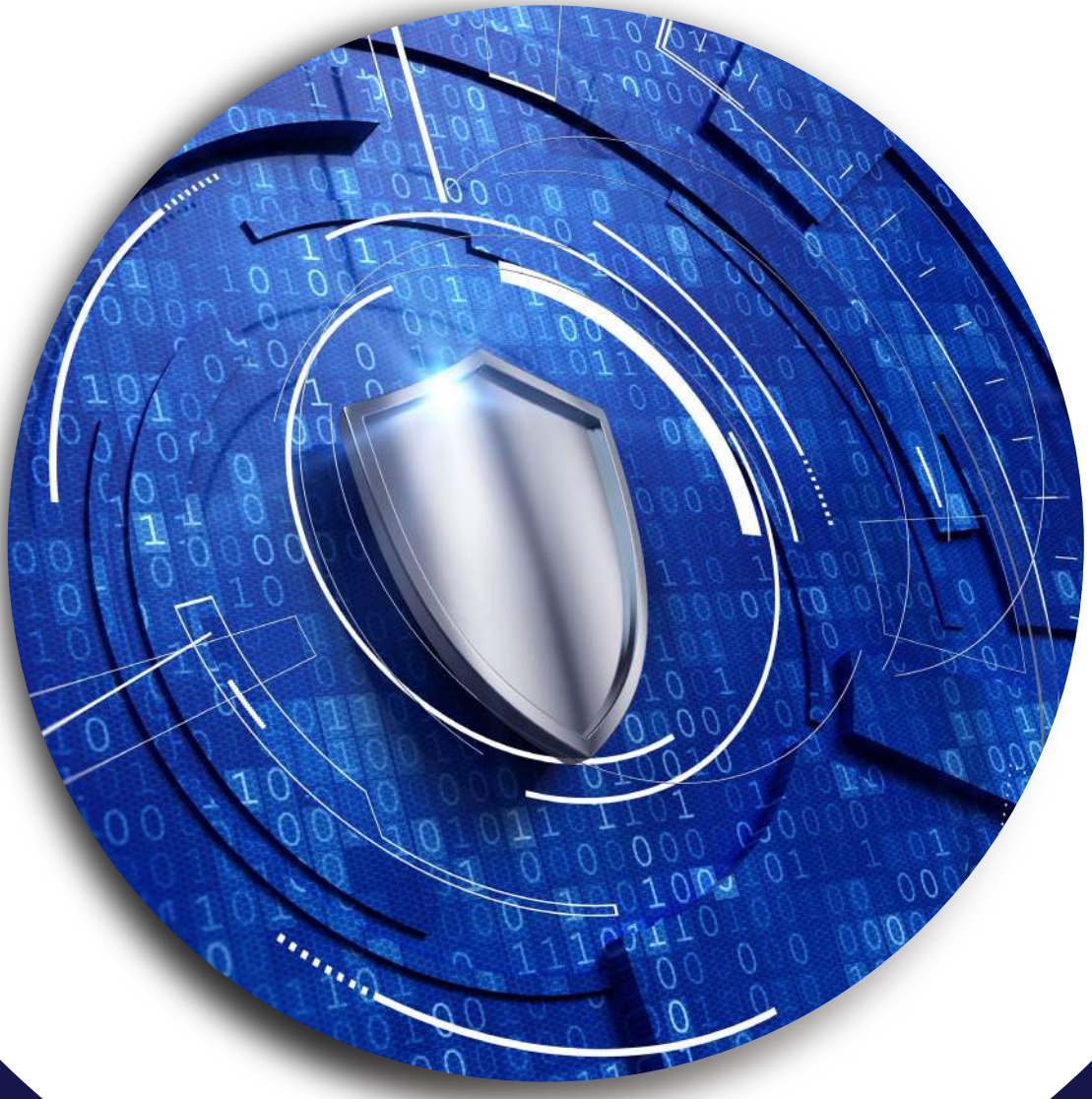
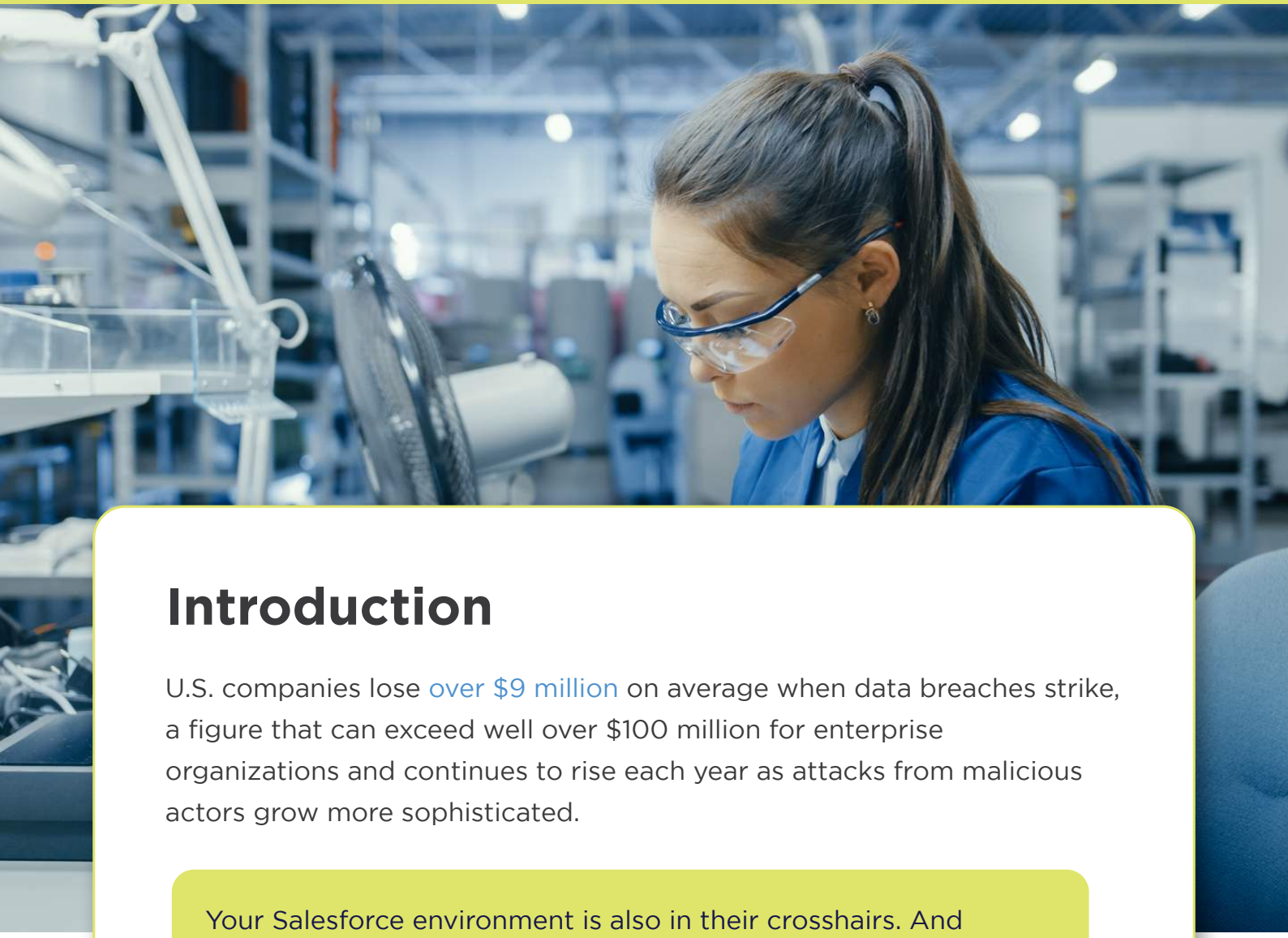
EzProtect

Salesforce Threat Protection

Are you actively choosing to put your Salesforce data at risk?





Introduction

U.S. companies lose over $9 million on average when data breaches strike, a figure that can exceed well over $100 million for enterprise organizations and continues to rise each year as attacks from malicious actors grow more sophisticated.

Your Salesforce environment is also in their crosshairs. And they are more than ready to turn your company into the next multi-million dollar mistake.

See what a breach could cost your organization with our EzProtect confidential calculator

Are you confident your current solution is protecting you? We recently discovered 298 active threats in a customer's Salesforce environment that went undetected by their previous security solution — they chose a general contractor when they needed a bridge engineering specialist.

These gaps are not random. They stem from five specific misconceptions about Salesforce security that continue to leave organizations exposed.

These five fallacies could cost you millions

1. Salesforce provides built-in protection against security threats

The reality

Salesforce is an excellent CRM platform that emphasizes security and customer trust, but its default security features are designed for general data protection, not comprehensive threat detection. Salesforce itself does not scan uploaded files for malware.

The risk

Believing Salesforce's native security features are sufficient leaves critical vulnerabilities unaddressed. Without specialized security, malicious files, links, and code can enter your environment undetected through everyday business activity and lead to costly data breaches, legal fees, and lost customers.

2. A virus scanning company is the safer choice for Salesforce security

The reality

A virus scanning company focuses primarily on protecting desktops and servers, not Salesforce. That means they will consistently miss critical security gaps specific to Salesforce because they lack platform expertise.

The risk

Relying on a traditional antivirus vendor to secure Salesforce is like asking your email spam filter to protect your CRM. It is built for a different purpose and misses the unique risks in Salesforce — like misconfigured permissions, exposed data through Flows, or malicious Apex code. You need a solution that actually understands the platform.

3. Security generalists offer the same protection as Salesforce specialists

The reality

Security companies with broad product portfolios often lack deep expertise in specific platforms. They bury their Salesforce security within a vast portfolio of products. For these companies, Salesforce security is just one of dozens of offerings, not their core focus.

The risk

Would you trust a housing contractor to construct a bridge your family depends on, or demand a specialized bridge engineer? When Salesforce security is an afterthought rather than a priority, critical security gaps develop. Enterprise companies are like housing contractors — less personalized, less flexible, and spread too thin across multiple product lines. In short, you end up paying premium prices without receiving specialized Salesforce support when your business depends on it most.

4. The cheapest option is good enough to check the box

The reality

You can absolutely save a few thousand by choosing a cheaper solution that does not meet your security needs. But the savings will pale in comparison to the amount you could lose in the long term after one or multiple data breaches.

The risk

Disney's recent Salesforce data breach put its $91.36 billion in annual revenue at risk. Are you willing to gamble with your company's future to save $10,000? When the inevitable happens, you will face not only financial consequences but also potential legal fees, regulatory fines, and permanent loss of customer trust and revenue.

5. Foreign security vendors with a U.S. presence are still safe options

The reality

Foreign security vendors, even with a U.S. presence, remain subject to their home governments' data access laws. Russia grants the FSB direct access to companies' data anytime, while China's Data Security Law provides the government with extensive authority to access data for national security purposes. Organizations must comply with government requests for data access, including sharing information with state entities.

The risk

When foreign adversaries demand access, they exploit U.S. data to commit espionage, conduct surveillance, and develop competitive advantages. Cross-jurisdictional requests bypass your consent entirely, exposing critical Salesforce information to hostile entities. This is why U.S. companies with employees on U.S. soil should be your only option for storing American data — anything else fundamentally compromises security.

Choosing the wrong security solution will carry real costs

What would happen if your company lost $200 million tomorrow and it was your fault?

Fingers will be pointed when millions are lost.

We recently discovered 298 viruses in a single scan from a customer coming from our competitor, but what if a breach had occurred before they chose EzProtect as their trusted partner?

When a breach occurs, everyone looks for someone to blame. Your Salesforce team might deflect responsibility to the security team. Your security team will ask you why there was no adequate protection in place.

Just look at the costs of these breaches to truly understand the devastating losses you would be held accountable for:

1.1 terabyte

Disney had 1.1 terabytes of sensitive data (44 million messages) stolen due to a single employee downloading malware in 2024, including unreleased scripts and intellectual property worth billions in potential revenue.

350 million

T-Mobile paid $350 million in settlements after exposing the data of 76.6 million customers, then suffered another breach affecting 37 million more.

3.1 billion

UnitedHealth spent $3.1 billion responding to a 2024 ransomware attack that exposed the sensitive medical and financial data of 190 million Americans.

86.6 million

After exposing the data of 16.9 million customers in 2024, LoanDepot faced $86.6 million in settlement costs plus $27 million in direct expenses.

See the real cost of a Salesforce data breach to your organization

Your accountability does not end after sending a ticket

You identified the threat and found an affordable solution with a 1-hour implementation. Yet your company remains exposed month after month while the decision cycles through endless reviews.

While your protection request sits in a SecOps queue, malicious actors with AI-powered tools are actively exploiting the exact vulnerabilities you flagged.

When a breach occurs, no one will remember your diligence — only that you knew the risk and chose to wait.

EzProtect closes Salesforce security gaps competitors leave open

EzProtect's advanced AI security technology protects your Salesforce environment from these common attack vectors that competitors routinely miss. Our comprehensive approach identifies and neutralizes threats like:

1. Extension deception

Fake .png or .docx files with dangerous .exe payloads sail through surface-level security checks and signature-based scanners.

Why competitors miss it

Competitors skip virus scanning for specific file types like images, trusting extensions alone. Without scanning the entire file structure, they cannot detect the real file type, creating easy attack vectors. Solutions using only checksum or hash comparisons miss these threats entirely.

How EzProtect addresses it

Our proprietary file analysis examines the entire file structure and content, regardless of extension. We maintain a zero-trust scanning policy for all files, without exception. Be wary of solutions that do not scan complete files every time.

2. Size exploit

Files over 52 MB cause errors in standard scanners, creating perfect hiding spots for malware.

Why competitors miss it

When competitors' scanners encounter an error with large files, they simply let them through unscanned — a critical security failure.

How EzProtect addresses it

We can scan files up to Salesforce's full 2 GB limit without exception. If an error occurs during scanning, the file remains blocked until verification completes successfully. Competitors lack Salesforce expertise to build truly secure solutions within the platform.

3. Salesforce email bypass

Emails sent from within Salesforce can distribute malicious files externally while bypassing traditional email security gateways, and competitor security solutions lack the necessary protections to prevent this.

Why competitors miss it

Lack of Salesforce expertise means they do not understand how Salesforce handles outbound email communications.

How EzProtect addresses it

We provide complete protection for all communication channels, including outbound Salesforce emails, to prevent accidental distribution of threats.

4. Malicious URLs

Emails, support cases, and other text data within Salesforce often go unscanned for harmful URLs and threats like phishing attacks.

Why competitors miss it

Competitors have limited URL field scanning and cannot detect certain URL formats, such as direct IP addresses like “223.34.44.15.” Missing basic IP-based URLs reveals inadequate testing — what other critical vulnerabilities are competitors overlooking?

How EzProtect addresses it

We scan unlimited URL fields across all objects and detect URLs in any format, including directing IP addresses that competitors miss. We have tested thousands of URLs in all formats to ensure complete coverage.

EzProtect: The winning advantage

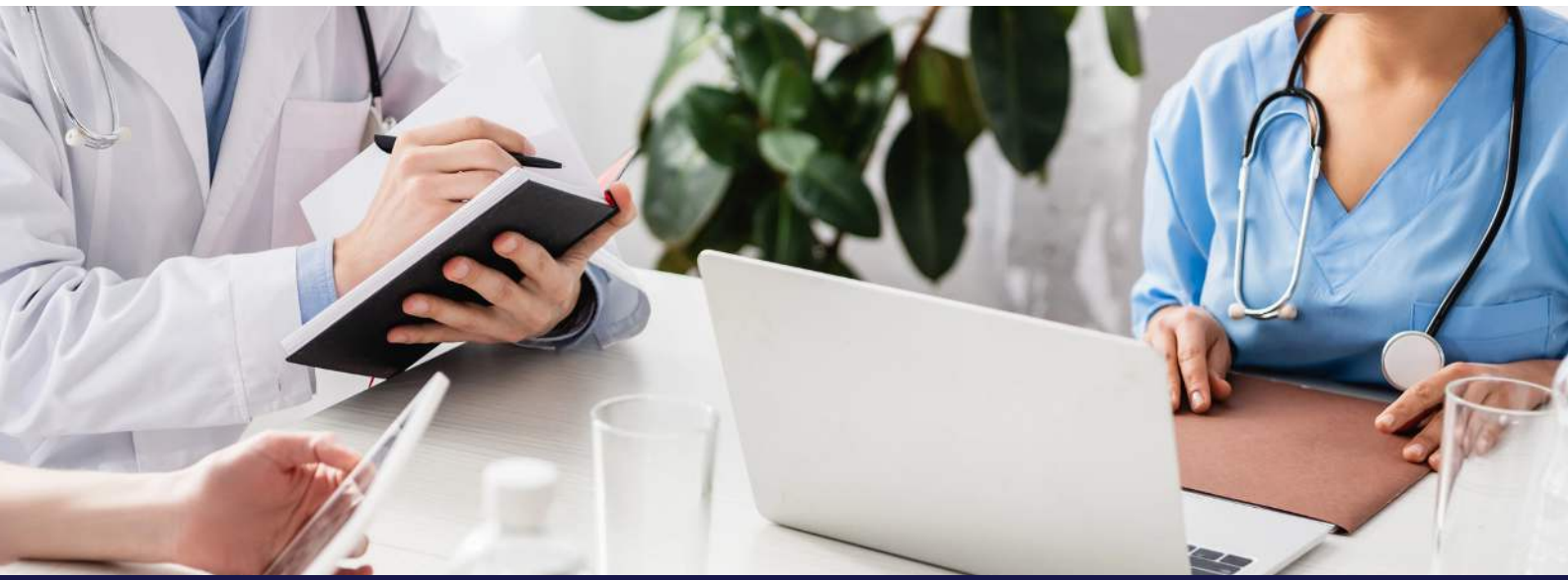
You should not entrust your mission-critical customer data to anyone but Salesforce security specialists. EzProtect delivers superior protection because it was built by Salesforce security engineers who understand the platform's unique architecture and take a proactive, multi-layered, zero-trust approach to keeping your data secure.

1. **Our only focus is protecting your Salesforce environment.**
2. We have 50+ years of combined Salesforce security and architecture expertise.
3. Our CEO and Co-Founder is a Certified Technical Architect (CTA) and the author of the #1 Amazon bestseller "Securing Salesforce Digital Experiences."
4. We are recognized cybersecurity experts, selected to speak on Salesforce data security at leading global conferences like Dreamforce, TDX, and London's Calling — events where competitors must pay for speaking opportunities.
5. We have been trusted Salesforce partners for 9 years and have been recommended by Salesforce themselves.

Complete protection, not just virus scanning

While competitors simply attach generic virus scanning to Salesforce, we provide comprehensive threat management tailored for your Salesforce environment.

	EzProtect	Generic security tools
Files scanned	All files up to 2 GB	Limited (under 52 MB)
True file type detection	Identifies the actual file type	Fooled by changed extensions
URL protection coverage	Unlimited fields & objects	Limited fields per target
Outbound email security	Prevents malware distribution	Files sent without scanning
Incident response	24/7 expert support	Limited support
Salesforce expertise	Dedicated specialists	Generic security focus



Here is what our multi-layered zero-trust approach looks like:

1. **Signature scanning**
   Initial screening of files against our extensive database of known threats

2. **Heuristic/DNA scanning**
   Advanced analysis that looks beyond simple signatures

3. **Dynamic scanning**
   Execution of suspicious files in a secure sandbox environment

4. **File type verification**
   Comprehensive examination of actual file content regardless of extension

5. **Malicious URL detection**
   Thorough scanning of all URL fields across your entire Salesforce

This proven approach uncovered 298 threats our competitors missed

We recently found 298 viruses in a customer's environment that a competitor's security tool completely missed. Our Salesforce security expertise and in-depth security approach detect threats that generic security tools overlook.

But we do not stop at detecting threats.

Complete incident response support

When threats emerge, our experts guide you through rapid containment, eradication, and recovery following NIST's proven seven-phase incident response lifecycle. Unlike competitors who only provide basic virus scanning and leave you to handle breaches alone, our 24/7 technical support team provides step-by-step assistance through the entire incident management process — from initial detection through post-incident analysis.

Weekly Salesforce security office hours

We don't just protect your environment — we empower your team with ongoing expertise. Our exclusive Weekly Salesforce Security Office Hours provide direct access to our Salesforce certified security specialists through weekly Zoom calls where your team can get immediate answers to any Salesforce security questions. While most competitors leave you to figure things out alone, we provide this ongoing support because we want to ensure our customers stay educated about the latest threats and have a lifeline when they need it most.

End-to-end Salesforce security ecosystem

Protection goes far beyond just scanning files for malware. We secure your entire Salesforce ecosystem, including custom objects, integrations, user access controls, and communication channels that competitors often overlook completely. During onboarding, we do not just set up virus scanning — we implement complete incident response processes following NIST guidelines, ensuring your team knows how to handle any security threat properly.

Trusted by industry leaders

Trusted across industries and regions — we are where you are, with data residency coverage in the U.S., U.S. Gov, Canada, EU, U.K., and Australia.

What our clients say

"We've been using EzProtect for several years now. It's imperative to protect your data and EzProtect scans our large volume of files quickly and seamlessly. The team is a pleasure to work with. This product was developed by a Salesforce CTA which says a lot about the expertise that went into the design. Can't recommend EzProtect and the peace of mind it brings enough."

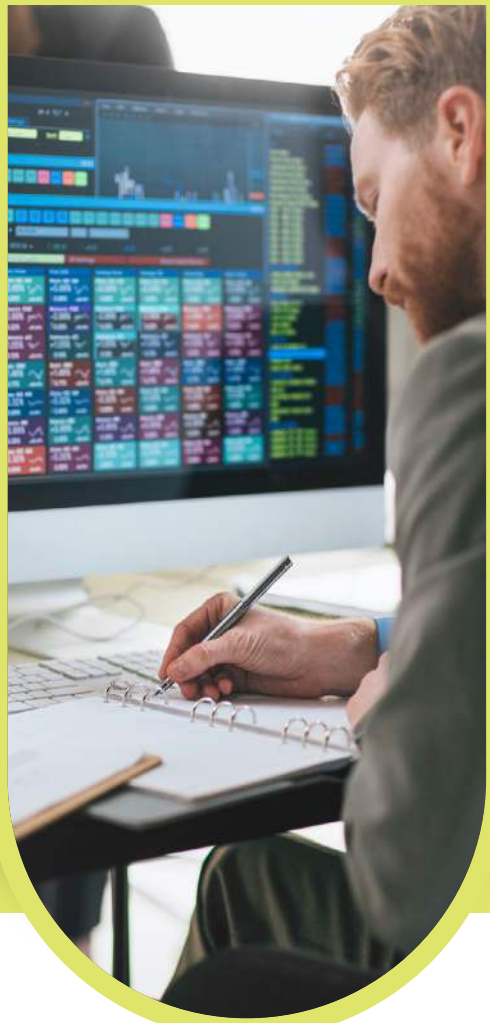
- Harold Lopez, Sr Mgr, Salesforce Platform Support at JH

"My org has used EzProtect for nearly two years now and I cannot be happier with the product. We are a fairly large volume user (> 100k scans per month) of the product, and it is very close to real time scanning of documents and attachments. The installation, administration and usage are very simple. The product also does exactly what is says it will and keeps infected documents and files quarantined to prevent downloading to other platforms."

- Director of IT, EzProtect Customer

EzProtect

Salesforce Threat Protection



Choose correctly:

Secure your Salesforce data with EzProtect

Schedule a free assessment for your Salesforce org to:

- Scan for malware and security threats in your Salesforce environment
- Receive custom mitigation strategies from Salesforce experts
- Get a comprehensive security assessment report to bring back to your team

Protect your Salesforce investment —

Click here to start your free Security Scan today