

Protect your Agentforce workflows from file and link-based cyber threats

WithSecure™ Cloud Protection for Salesforce defends against malware and phishing threats hidden in files, URLs, and chats – now extended to AI agent workflows with Agentforce.

Agentforce moves fast, your security needs to move faster

Salesforce Agentforce is transforming how organizations engage with customers. AI agents now handle conversations, retrieve files, and automate workflows at machine speed, but that speed creates new blind spots for threats.

Files, links, and chat content shared through Agentforce are not scanned by default. That means phishing links and malware can slip through portals, forms, and integrations like Slack or WhatsApp – and spread before legacy tools react.

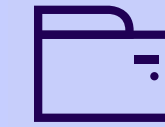
WithSecure™ Cloud Protection closes the gap.

It's the only real-time, Salesforce-native solution that scans files and URLs inside Agentforce workflows the moment they're uploaded, retrieved, or clicked. It stops threats before they reach your users or systems.

Agentforce helps you scale customer experiences. We make sure you scale them securely.



How securing autonomous AI works



Real-time protection at agent speed
AI agents act in seconds, and so must your defenses. Files and URLs are scanned instantly to stop threats before they spread.



Native to Salesforce, built for scale
100% Salesforce-native. No external routing, no portals, no tradeoffs. The Agentforce extension comes at no extra cost.

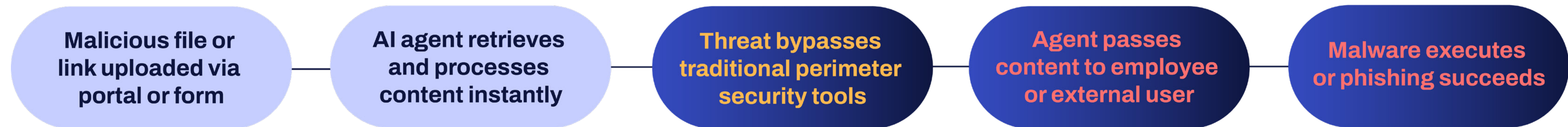


Visibility and control for security teams
Get audit trails, alerts, and custom dashboards to monitor threat activity and system use.



Keeps work moving, securely
We protect your workflows without slowing agents or disrupting collaboration.

Shared responsibility – and a new attack path



Agents move fast. So do threats.

Agentforce workflows introduce a new way for threats to slip through: content uploaded by a user, processed instantly by an agent, and passed to employees or customers without traditional defenses ever seeing it.

Agent workflows aren't scanned by default.

Files, links, and chat content aren't scanned by default. And AI agents don't recognize phishing, malware, or suspicious behaviors. That means malicious content can move at machine speed — and spread just as fast.

You're responsible for securing the data.

According to the Shared Responsibility Model, it's up to you — the cloud customer — to secure what flows in and out of Salesforce. Whether it's touched by a human or an agent, it's your job to make sure it's clean, safe, and under control.

Left unprotected, Agentforce can become a high-speed delivery system for threats.



What it protects – and when it kicks in

Agentforce moves fast. Malware hidden in an image, phishing links inside a shared form, or a legacy file loaded with threats – once processed by an agent, they can spread instantly across your Salesforce environment.

WithSecure™ Cloud Protection for Salesforce delivers immediate detection at the critical points where threats can enter, move, or exit the system without slowing you down:

- At upload: Files and URLs added via portals, forms, and connected apps
- At download: When content is downloaded by a user
- At click: URL protection triggered on access attempts
- At agent retrieval: Real-time scanning when agents fetch files or URLs
- At outbound use – Scanning before agents share content with customers
- At API and integration points: Includes tools like Slack, WhatsApp, and email-to-case

By making sure all data inside your Salesforce environment is clean – and by covering both human and agent workflows – we help you stay secure at agent speed.

Key capabilities

- ✓ Real-time scanning of files and URLs at upload, download, click, and agent retrieval
- ✓ Protection extended to Agentforce workflows – including forms, chats, and Slack integrations
- ✓ Advanced anti-malware powered by multi-engine analysis and global threat intelligence
- ✓ Sandboxing for zero-day detection using behavioral analysis
- ✓ Detection of phishing links, spoofed file types, and malicious QR codes
- ✓ Click-time URL protection with domain and shortlink analysis
- ✓ Deep scanning of password-protected archives and large files
- ✓ Full support for Salesforce standard and custom objects
- ✓ Automated and on-demand scanning of stored content across your environment
- ✓ Real-time dashboards, audit trails, and customizable alerts for security visibility
- ✓ Out-of-box and custom Salesforce-native reports for threat tracking
- ✓ 24-month event and detection log retention
- ✓ SIEM integration with structured log export
- ✓ Deployed entirely within Salesforce – no external portals or traffic rerouting
- ✓ Included Agentforce extension – no additional cost or complexity
- ✓ Covers both sandbox and production environments
- ✓ Regional data residency control across EU, US, Japan, and more
- ✓ Auto-updates and maintenance-free operation inside Salesforce

Agentforce protection, built for how agentic AI works

Get it from AppExchange

Salesforce Agentforce accelerates work. But without real-time threat protection, it can also accelerate risk. WithSecure™ Cloud Protection is the only Salesforce-native solution that scans files, links, and agent-handled content the moment they move – from upload to retrieval to outbound use. No routing, no delays, no middleware. Just fast, frictionless protection for your fastest workflows.



Secure at agent speed

AI agents move in seconds — your security has to move faster.

- Real-time file and URL scanning at upload, download, click, and agent retrieval
- Detect threats before they reach users or spread across workflows
- Protect both human and autonomous workflows without slowing them down



Simple, scalable, and seamlessly native

Security that's frictionless, easy to manage, and built for governance.

- Click-and-go deployment with zero external routing or portals
- 100% Salesforce-native with automatic updates and configuration logging
- Audit-ready logs and real-time visibility for compliance and control



Trust what agents touch

Let agents work at full speed — on clean, trusted data only.

- Scan every file, link, and QR code before agent access or handoff
- Detect malware in images, archives, or shared content
- Ensure unstructured content doesn't become a blind spot in automation

WithSecure™ – your partner in cyber security

As an end-to-end cyber security house, we offer comprehensive cyber security services, and develop our award-winning security technologies with a deep understanding that our in-house research unit and hands on field experience provides.

Certified and audit-ready

WithSecure™ Cloud Protection for Salesforce is continuously subjected to Salesforce's thorough security reviews to ensure top-notch performance. We are also comprehensively certified with ISO 27001, ISAE 3000 Type 2 (SOC2 Type 2 equivalent) to meet your compliance requirements.

