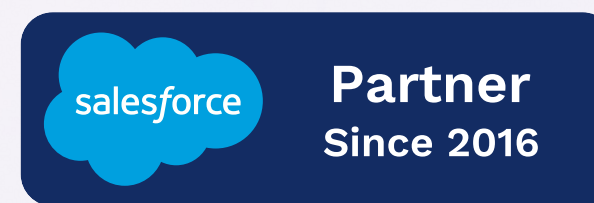




SOLUTION OVERVIEW

Cloud Protection for Salesforce



1. Executive overview



Cloud Protection for Salesforce is a cloud-based security solution designed to complement the native security capabilities of the Salesforce platform.

Salesforce and its customers share responsibility for security. Salesforce secures the platform itself, infrastructure, uptime, and core application controls, and provides basic native scanning for some content. Comprehensive protection for everything that moves through Salesforce, files, URLs, QR codes, emails, AI agent workflows, and user identities, remains the customer's responsibility.

Together with Salesforce, Cloud Protection for Salesforce makes it easier for companies to handle their part of security under the Shared Responsibility model used in cloud ecosystems. Cloud Protection for Salesforce is built to complement overall security capabilities and extend a company's security strategy into its cloud services.

Cloud Protection for Salesforce handles that part for you. It mitigates the risks posed by files, URLs, emails, AI agent workflows, and user identities across Salesforce, without hindering how people use it day to day, and provides rich reporting, security analytics, and full audit trails for fast incident response.

Native cloud-to-cloud integration between Salesforce and Cloud Protection for Salesforce makes our solution an efficient choice from both a security and a resourcing perspective:

- Easy Deployment: Deployment via Salesforce AgentExchange takes minutes, not the weeks of IT project work traditional security tooling requires.
- No new infrastructure to manage: Cloud Protection for Salesforce is a managed package, so there's no middleware, servers, or proxies for your team to run, and no network reconfiguration. All management, settings, and reporting take place natively within your own Salesforce environment.

Summary of benefits

Advanced threat protection

- Detection of known, emerging, and previously unseen malware
- Protection against malicious URLs, including embedded links in documents, QR-code-based phishing, and compromised user credentials
- Powered by multi-layered content analysis, real-time threat intelligence, machine learning, and sandboxing

Real-time protection and visibility

- Automated scanning on upload and download
- Flexible on-demand and scheduled scans
- Click-time URL protection against dormant and mutating threats
- Full forensic trail for threat hunting

Native security, built with Salesforce

- Purpose-built in close collaboration with Salesforce
- No additional middleware, connectors, configuration overhead, or hosting costs
- Up and running in minutes

2. Shared responsibility model



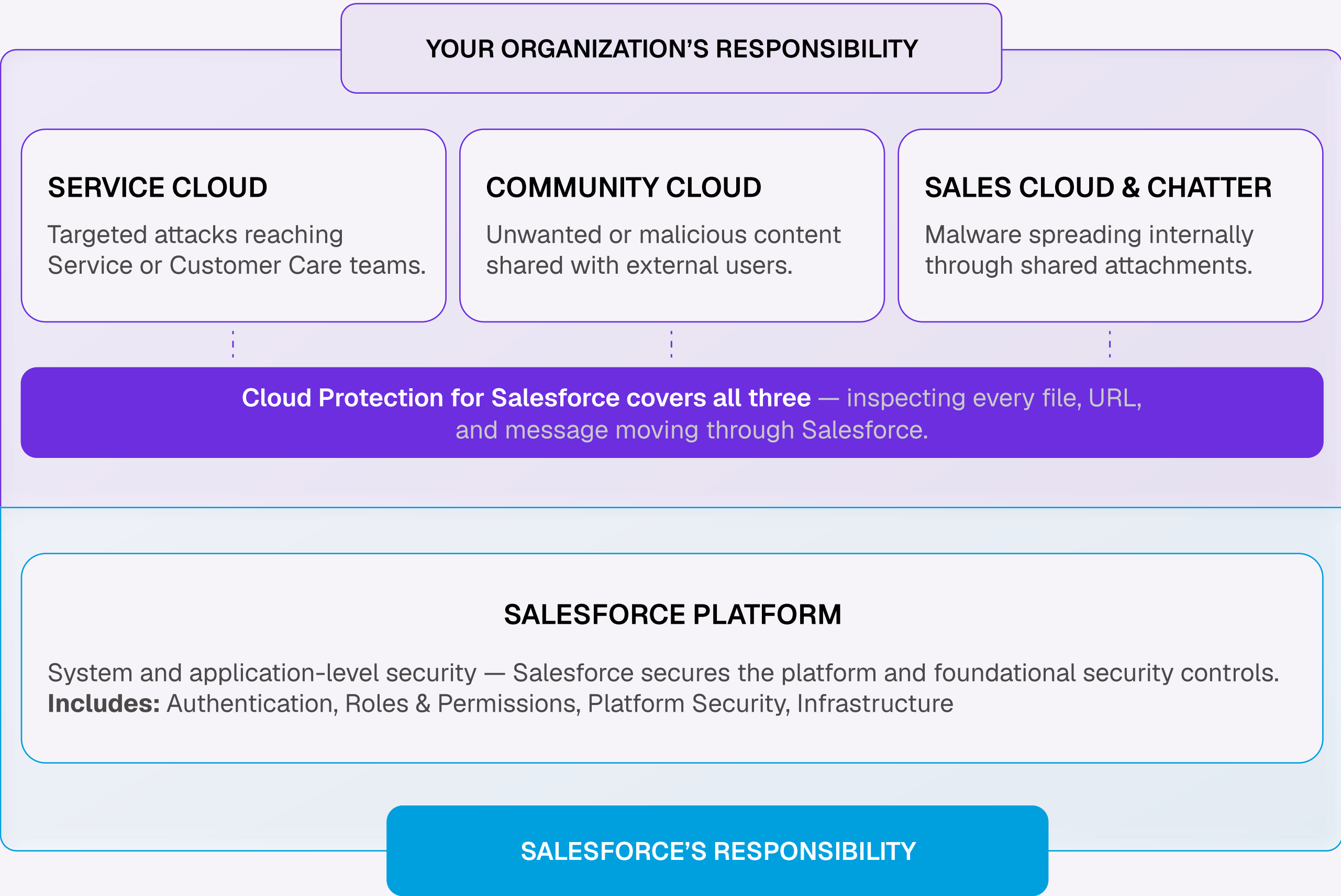
Under Salesforce's Shared Responsibility Model, Salesforce is responsible for the security of the underlying platform and infrastructure. Customers are responsible for securing how their Salesforce environment is configured and used, including authentication settings, sharing rules, permissions, and roles.

Comprehensive protection for the files and URLs your users upload to Salesforce is your organization's responsibility, alongside Salesforce's native security capabilities. No platform can guarantee the identity of every external user, or the safety of every file and URL shared by partners or customers on it. And because many organizations give cloud applications like Salesforce direct access through their firewalls, endpoint protection often never sees this activity at all; it happens natively inside Salesforce, not on a device endpoint tools can monitor.

In practice, this means organizations need to:

- Prevent malicious files from reaching Service or Customer Care teams through Service Cloud.
- Prevent unwanted or malicious content from being shared through Experience Cloud.
- Prevent malware from spreading internally through attachments shared in Sales Cloud or Chatter.

Cloud Protection for Salesforce extends Salesforce's native security with dedicated components that handle files, URLs, identities, and the other risks moving through Salesforce.

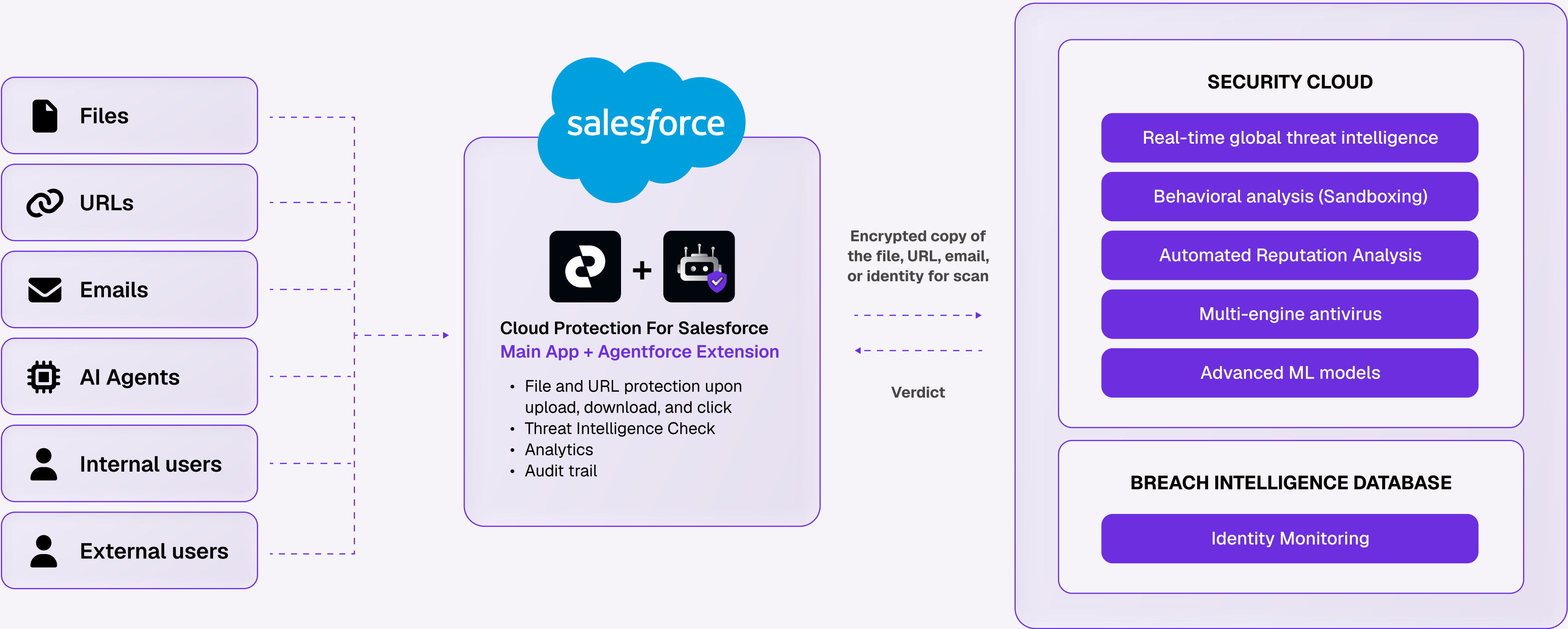


3. Solution overview



Every file, URL, and AI agent action that moves through Salesforce goes through the same process. Cloud Protection for Salesforce intercepts it and scans it in real time, using multi-layered malware detection, threat intelligence, and sandboxing to determine whether it's safe. If it's harmful, detected threats can be automatically blocked based on customer settings, the user is notified, and the admin is alerted, helping prevent malicious content from reaching users. Every scan and every action taken is logged, giving your security team full visibility and a complete audit trail to investigate or report on.

The diagram below shows the process behind every feature in this document.



3. Solution overview



The solution installs as a managed package directly from Salesforce AgentExchange, with no middleware or additional infrastructure required, and supports Sales Cloud, Service Cloud, and Experience Cloud across Professional, Enterprise, Unlimited, and Developer editions, and Marketing Cloud Growth and Advanced editions, which are built on the Salesforce core platform. Marketing Cloud Engagement and Marketing Cloud Account Engagement are not supported.



File Protection

Every attachment, content document, and Chatter file, scanned at upload and download, including files arriving via Email-to-Case.



URL Protection

Links scanned at post and again at click, wherever they appear in Salesforce, including links arriving via Email-to-Case.



Protection for Agentforce

Links and content handled by AI agents, scanned before an agent acts on them.



QR Code Protection

Malicious QR codes embedded in uploaded files, resolved before anyone scans them.



Identity Protection

User credentials and permissions monitored for breach exposure and excessive access.



Analytics & Visibility

Real-time dashboards and audit trails across all the above, in one place.

3. Solution overview



3.1. File protection

Files are one of the easiest ways for an attacker to get malware into Salesforce, through Chatter, Case attachments, community uploads, or web forms, since none of that traffic passes through an email gateway or endpoint protection. Cloud Protection for Salesforce scans every file the moment it's uploaded or downloaded, catching viruses, trojans, ransomware, and zero-day malware before anyone opens the file.

How a file gets checked

Every file is fingerprinted and checked against global threat intelligence and reputation data. If it hasn't been seen before, it's analyzed using multiple detection techniques, including heuristics, content analysis, and machine learning. Files that remain suspicious are run in an isolated cloud sandbox to observe their actual behavior, catching zero-day malware a simple signature check would miss entirely.

Beyond straightforward malware, the same process also catches the ways attackers try to slip past detection:

- Password-protected archives — blocked entirely at both upload and download, since attackers use them specifically to hide malware from scanners.
- Disallowed file types — administrators can block file types or extensions, for example executables or scripts.
- Macro-enabled files — configurable handling of documents containing macros, which are commonly used to deliver malware.

Analysis results are cached where appropriate to reduce unnecessary repeat analysis and accelerate threat detection, while still allowing files to be reassessed when required.

Download protection

The same checks apply on download as on upload. This closes the gap malware relies on content that looked clean at upload can still be caught at download, once newer threat intelligence becomes available, even if it slipped past the earlier scan.

Manual and scheduled scanning

Files already sitting in Salesforce before installation, or excluded from automatic scanning, can be scanned on demand or on a recurring schedule, running in the background with no impact on users.

Configurable handling for high-risk files

Administrators decide how password-protected or otherwise high-risk files are handled at both upload and download, choosing to allow and report, remove, or block, based on their own business and compliance requirements.

3. Solution overview



3.2. URL protection

Cloud Protection for Salesforce checks every URL the moment it's posted, and again the moment someone clicks it, since attackers often swap a link's destination after it's already been shared to slip past an initial scan. Malicious URLs can enter Salesforce through many channels, including Chatter posts, Case descriptions, Experience Cloud, custom objects, and Email-to-Case, places traditional email and endpoint security controls may not inspect once content is already inside Salesforce.

How a link gets checked

Every URL is looked up against Security Cloud in real time using reputation, threat intelligence, and URL metadata to determine its risk. The check draws on IP reputation, site patterns, known exploit and redirect behavior, and other URL metadata. Shortened links (bit.ly, tinyurl, and similar) are unwrapped to their true destination before being evaluated, so a masked link can't hide behind a shortener. Newly registered domains, a strong signal of phishing since attackers routinely stand-up fresh sites for each campaign, are also flagged, with administrators able to set blocking thresholds at 7, 14, 30, 60, or 90 days old.

Click-time protection

Posted URLs are replaced with protected redirect links so that the destination can be reassessed at the time of access. This allows the latest threat intelligence and URL reputation to be applied each time a user clicks a link, helping protect against destinations whose risk changes after they were originally shared.

Content and category controls

Administrators can block website categories according to organizational security and acceptable use policies. This helps ensure policies are enforced consistently across Salesforce.

3. Solution overview



3.3. Identity protection

A stolen password doesn't need to be stolen from Salesforce to become a Salesforce problem. Credentials get reused across services, and once one gets exposed in an unrelated breach, an attacker can walk into your Salesforce org as a legitimate user and stay there for months without triggering a single alert. Identity Protection continuously monitors Salesforce user accounts, including internal users, administrators, service accounts, and external Experience Cloud users, against continuously updated credential breach intelligence, helping organizations identify exposed credentials and respond appropriately. Up to 12 months of breach history is retained for each monitored identity.

It also looks beyond stolen credentials to excessive access: human and non-human identities holding high-risk permissions, such as ModifyAllData or ViewAllData, that go further than their role requires. When identity risks are identified, administrators can immediately take remediation actions such as freezing accounts, initiating password resets, or reviewing user permissions directly from the Cloud Protection for Salesforce dashboard, streamlining investigation and response.

Many organizations maintain large numbers of external identities for customers, partners, and suppliers. Identity Protection extends credential exposure monitoring to these accounts alongside internal users, helping administrators assess identity risk across their Salesforce environment from a single interface.

3.4. Protection for Agentforce

Agentforce agents automate business processes by processing content and executing actions on behalf of users using the Salesforce permissions of the user they represent. While this enables significant improvements in speed and scale, AI agents rely on the information provided to them and do not independently determine whether content is trustworthy. Protecting the content they process helps reduce the risk of malicious URLs influencing automated workflows.

Cloud Protection for Salesforce extends the same real-time protection to these workflows. URLs surfaced or shared within Agentforce-driven actions are scanned the moment they appear, and malicious or unwanted URLs are intercepted before an agent acts on them or passes them on to a user.

Every scan is logged in full, audit-ready detail alongside the rest of the solution event history, so teams get the same visibility into AI-driven activity as they already have into human activity.

3. Solution overview



3.5. QR code protection

Malicious actors increasingly hide phishing links behind QR codes embedded in uploaded files; a tactic often called "quishing." Because these links are only revealed once a device scans the code, frequently a personal mobile device outside the reach of traditional endpoint or email security; this attack path can bypass conventional security layers entirely.

Cloud Protection for Salesforce extracts and resolves QR codes embedded in uploaded files, including cases where a QR code points to a shortened URL masking its true destination. The resolved destination is then evaluated using the same URL inspection and threat intelligence capabilities applied to other URLs within Salesforce, helping identify phishing and other malicious destinations hidden within QR codes.

3.6. Analytics and reporting

Analytics

Most teams have no idea what's happening inside Salesforce, what files are moving through it, which URLs are being clicked, or which identities are at risk. Cloud Protection gives full visibility into all of it: every upload, download, URL click, and identity event is logged, so your team can confirm or rule out Salesforce as an attack vector, trace an incident back to its source, and see exactly who accessed what.

Each log entry captures the detail needed for real investigation, not just a record that something happened: timestamp, action and direction (upload, download, post, or click), verdict and file prevalence, reason, username, file details (name, type, version, size, SHA-256 checksum), URL and its category, location, and IP address.

Alerts

Administrators and security personnel are notified as events happen, not discovered after the fact: harmful content found or blocked, harmful or disallowed URLs found, a verdict flipping from safe to unsafe, or newly exposed user credentials.

Reporting

Built-in dashboards turn that raw log data into something usable day to day: a Summary Protection view, Protected Content Analytics, and detailed File and URL Protection dashboards, each with trend data over time. For anything the built-in views don't cover; custom reports are available directly through Salesforce Reports, using dedicated File and URL Protection data sets.

4. Data Handling and Compliance



4.1 Data Handling

Customers control how much data is processed to provide protection. Depending on the selected configuration, the solution can perform metadata-only scanning or submit file contents for deeper analysis. Data handling and retention follow the customer's configured privacy and data residency settings.

Customers choose where their data is processed: EU, US, Canada, Australia, Singapore, or Japan. For more information on how data is processed in the solution, please refer to the privacy policy available at <https://cloudprotection.com/legal/privacy-policy/>.

4.2 Compliance

Cloud Protection for Salesforce is independently audited and certified to ISO/IEC 27001, and holds an ISAE 3000 Type 2 assurance report, the international equivalent of a SOC 2 Type 2 report, covering both the core solution and Agentforce workflows.

Alongside ISO/IEC 27001 and ISAE 3000 Type 2, Cloud Protection for Salesforce is also independently rated by SecurityScorecard, which evaluates vendors across key security factors, and has passed Salesforce's own security review process as an AppExchange-listed solution.

Cloud Protection by Salesforce also supports organizations in meeting General Data Protection Regulation (GDPR) requirements for the secure handling of personal data belonging to European citizens.

5. Security Cloud



File, URL, QR code, and Agentforce protection are powered by WithSecure Security Cloud. Security Cloud is WithSecure's cloud-based threat intelligence and analysis platform, providing reputation services, automated analysis, and behavioral sandboxing to support the detection of malicious content across Salesforce.

How threats are identified

Security Cloud continuously incorporates new threat intelligence, allowing protection to evolve as new threats are identified and analyzed. It combines multiple detection technologies, including reputation analysis, threat intelligence, heuristics, machine learning, and behavioral analysis, to identify both known and previously unseen threats. Objects requiring additional inspection can be executed within an isolated cloud sandbox, where their behavior is analyzed to improve detection of threats that may not be identifiable through static analysis alone.

What data this involves

- Minimal by default. File data only reaches Security Cloud when it's essential to providing protection, and only where the customer has allowed it.
- No user-identifying information is transmitted. Information identifying who uploaded or accessed a file or URL, or the source of that activity, is not transmitted to Security Cloud.
- Always protected in transit. All communication with Security Cloud is encrypted in transit using strong encryption methods.

How Security Cloud itself is protected

Security Cloud is designed using security-by-design principles. Communications are encrypted, malware analysis is performed within isolated environments, access to critical systems is restricted to authorized personnel, and the platform is continuously monitored and maintained as part of security operations.

6. Summary of features



Core functionalities

- Multi-layered malware detection: reputation analysis, heuristics, machine learning, and behavioral sandboxing for known and previously unseen threats.
- Sandboxing threat analysis: detect zero-day threats with advanced behavioral analysis
- Global threat intelligence: continuously updated threat intelligence and reputation services.
- 100% Salesforce native architecture: deploy in minutes, no middleware or extra portals
- Automatic updates: stay current with no manual upkeep
- Data processing regional selection: control your data residency (EU, USA, Canada, Australia, Japan, Singapore)

File protection

- Detect malicious files on upload and download
- Detect and block macro-enabled files
- On-demand and scheduled scanning for existing files
- Detect malicious URLs and QR codes hidden inside files
- Detect file type spoofing: identify real file types, bypassing misleading extensions
- Detect and block password-protected archives
- Scan standard and custom Salesforce objects

URL protection

- Detect and block malicious URLs at the time of post and at the time of click
- Block unwanted website categories
- Detect newly registered domains
- Detect malicious short links: analyze the true destination behind shortened URLs
- Scan standard and custom Salesforce objects

Identity protection

- Detect breached credentials across internal and external (community, partner) users
- Flag over-privileged permissions, such as ModifyAllData or ViewAllData
- Respond directly from the dashboard: freeze an account, reset a password, or edit permissions
- 12 months of breach history retained per identity

Protection for Agentforce

- Real-time URL scanning inside Agentforce-driven workflows
- Full audit-ready event logging, alongside the rest of the solution's activity

Security visibility and analytics

- Real-time security visibility into risks and how to prioritize them
- Out-of-box and custom Salesforce reports and dashboards
- Customized alerts to your team and users
- Full forensic trails for threat hunting
- SIEM integration
- Configurable log retention: 12-month default, adjustable from 1 week to 24 months

Certifications

- ISO 27001
- ISAE 3000 Type 2 (international equivalent of SOC 2 Type 2)

7. Cloud Protection by WithSecure



Cloud Protection by WithSecure is the missing security layer for modern Salesforce threats. We secure Salesforce environments against malware, phishing, and malicious content. Our product, Cloud Protection for Salesforce, is a Salesforce-native managed package distributed through Salesforce AppExchange.

Cloud Protection by WithSecure started as an internal start-up within WithSecure and have been independent since September 2026. We build on more than 35 years of cyber security heritage dating back to 1988, and our detection draws on WithSecure's threat intelligence and research teams through the WithSecure Security Cloud analysis service.