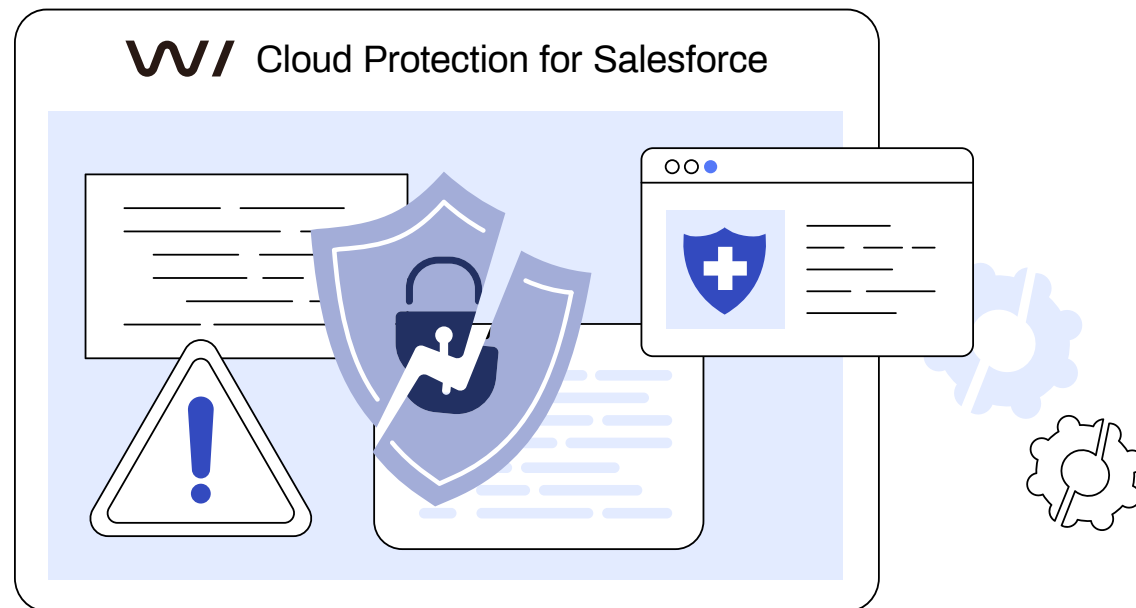


Ebook

W / T H<sup>®</sup>  
secure

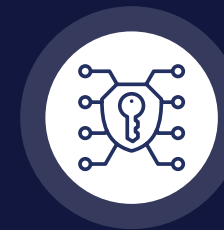
# Healthcare & Life Sciences **Industry Insider**



**See how our partner WithSecure tackles challenges in the healthcare and life sciences industry. From big-picture problems to the needs of a Salesforce administrator, WithSecure has it covered.**

WithSecure Cloud Protection is an ISO 27001 and ISAE 3000 Type 2 certified cybersecurity solution. It is designed to help shield Salesforce environments against malware, phishing, and zero-day threats that could reach users and disrupt operations.

**Here's how WithSecure** helps healthcare and life sciences organizations protect data, users, and customizations within Salesforce.



### **Shield Sensitive Data**

Safeguard your organization from malware and phishing. Detect threats to critical Salesforce data, patient records, and digital workflows the moment they appear.



### **Deploy Zero-Day Protection**

Prevent rapid exploitation. Stop both known and unknown malware before it spreads, using certified detection technologies.



### **Facilitate Business Continuity**

Instill operational continuity and trust by mitigating incidents that cause system downtime, investigation delays, or reputational damage.

Keep reading to see how WithSecure can help a Salesforce administrator strengthen their security posture with native, real-time threat detection.

# The Solution

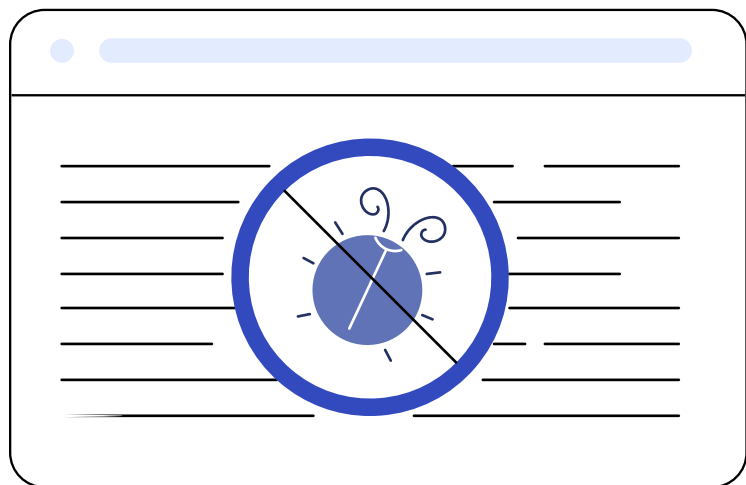
WithSecure Cloud Protection integrates natively into the Salesforce Platform for real-time protection where it's needed most. This means no rerouting, no added infrastructure, and no delays.



## Protect against file-borne malware.

**The Challenge:** Uploaded files may bypass traditional endpoint or email security and go directly into your CRM environment. This malware can remain dormant or activate on download.

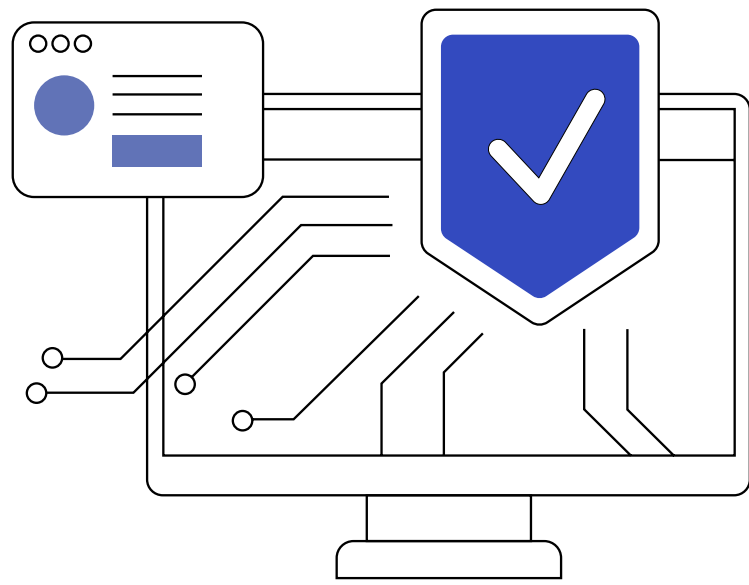
**The Solution:** WithSecure Cloud Protection performs real-time analysis of every file uploaded or downloaded via Salesforce. It detects and blocks commodity and zero-day malware using certified security engines. This allows organizations to confidently accept uploads and support the digital patient experience.



## Stop phishing attacks before they reach users.

**The Challenge:** Salesforce users can be tricked by malicious links embedded in fields, attachments, or custom objects.

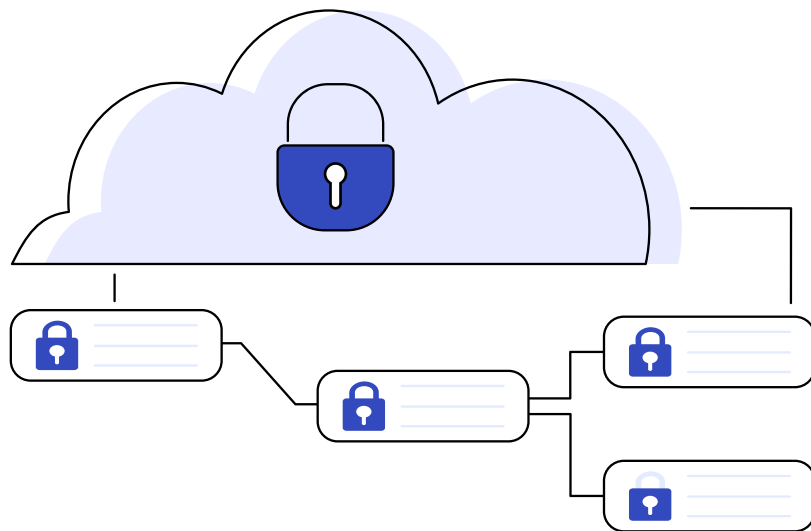
**The Solution:** WithSecure Cloud Protection inspects every URL and QR code uploaded to Salesforce in real time. It blocks access to malicious destinations and flags suspicious links, helping to prevent phishing attempts and credential theft at the point of interaction.



## Maintain critical system availability

**The Challenge:** Cyber incidents can cascade quickly across connected systems. Containment or investigation often requires halting integrations, workflows, or access.

**The Solution:** By preventing threats in real time, WithSecure Cloud Protection helps healthcare organizations avoid disruptions to Salesforce workflows. It stops threats before they enter or execute, reducing the need for post-incident investigation and isolation.



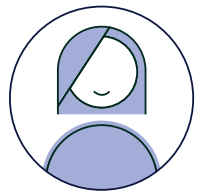
## Guard your growing attack surface.

**The Challenge:** More organizations are using AI-powered tools to automate workflows and digitize interactions. This can introduce more exposure points, allowing attackers to bypass existing defenses.

**The Solution:** WithSecure Cloud Protection helps secure traditional portals and new tools, including Agentforce. This helps to ensure that threats are blocked in real time across both human and AI-driven interactions.

# The Scenario

In this example, let's imagine how a Salesforce administrator can use WithSecure Cloud Protection to fulfill their part of the shared responsibility model for security and compliance.



**Emma Rice**

**Salesforce Administrator**

Emma manages her organization's Salesforce Platform, supporting internal workflows, such as case management and care coordination as well as external workflows, like patient intake and partner portals. She works closely with IT, compliance, and clinical teams. Her day-to-day responsibilities include maintaining system performance, enabling new features, and addressing risks raised by other teams.

Emma's priorities often align with CIO-level goals around uptime, innovation, and cost-effective risk reduction.

## Her Goals

- ✓ Maintain secure and stable Salesforce operations
- ✓ Protect sensitive patient data
- ✓ Enable innovation while mitigating risk
- ✓ Reduce time spent with external IT vendors

## Her Challenges

- ✓ Limited visibility into threats entering Salesforce via files, links, or forms
- ✓ Internal security controls that disrupt workflows
- ✓ Threat investigations that stall operations
- ✓ Balancing innovation with risk

# WithSecure solves Emma's challenges by helping her to:



## **Perform real-time malware scanning on patient uploads.**

Emma uses WithSecure Cloud Protection to scan every file uploaded by patients or labs through Experience Cloud portals. Malware is blocked instantly, before it can spread or be downloaded.



## **Respond to incidents faster and reduce disruptions.**

WithSecure blocks threats before they activate and provides alerts and logs that Emma and the security team can act on quickly.



## **Detect phishing links in Salesforce records.**

WithSecure's real-time URL and QR code analysis helps stop phishing attempts from targeting Emma's users. When attackers try to embed a phishing link in a message, record, or attachment, the system immediately blocks access.



## **Gain visibility and control across an expanding ecosystem.**

WithSecure Cloud Protection helps ensure innovations don't increase risk. Its native integration allows Emma and her team to minimize the addition of extra tools and complexity as they scale up with Agentforce for triage and patient routing.