Securing Salesforce: Know Your Responsibilities, Protect Your Data

WITH secure

What is the problem with Salesforce security?

Salesforce helps over 150,000 organizations have better conversations with their customers. Since its launch in 1999, Salesforce has evolved from an online CRM solution into a popular cloud-based platform relied on by enterprises and high-profile businesses to provide a company-wide view on its customer-facing operations.

The platform helps sales and marketing departments to manage communications with their target audience by allowing non-technical users to easily create websites and forms that collect data and automatically transfer that information. This information can include text, media files, and links to business applications and cloud-based 'community' shared storage areas.

Salesforce customers are increasingly falling victim to cyber attacks, with confidential commercial and customer data put at risk due to security vulnerabilities

Salesforce customers are increasingly falling victim to cyber attacks, with confidential commercial and customer data put at risk due to security vulnerabilities created by misuse and misunderstanding of the platform. It's important to understand that these security issues are not because of vulnerabilities in the Salesforce platform itself—they occur as a result of misconfigurations and naive security practices regarding the shared responsibility model, and a lack of clarity about the security roles and responsibilities of Salesforce stakeholders in organizations.

By its nature, Salesforce is designed to be highly customizable. There isn't a standard configuration that works for all companies, so every organization uses the platform in a different way. There are more than 3,400 applications on the Salesforce AppExchange alone, and countless third-party APIs and plugins readily accessible online.

So while one advantage of using Salesforce is that it allows organizations to enable integrations and encourages user accessibility, its flexibility creates an automated third-party supply chain that can quickly grow out of control. If your organization doesn't properly protect itself, the sharing and automation features of the platform could lead you to you being responsible for infecting one or more of your partners' internal networks with malware, ransomware, or phishing attacks.

It can also result in sophisticated infiltration by criminals in search of valuable corporate and customer data. This could lead to irreparable damage to not only all the affected parties' IT systems, but also their reputations.

The balance between flexibility and security

Each time Salesforce is extended to provide additional business insights, the connectivity and automation used in the extension increases the surface area vulnerable to attack, and potentially provides more opportunities for cyber criminals. Supply chain attacks have dominated the cyber security landscape over the last couple of years, so it's no surprise that security is becoming a greater concern for Salesforce users.

A recurring issue is that Salesforce modules are usually created by non-technical staff from sales and marketing divisions, who have little knowledge and experience of managing security threats. Meanwhile, CISOs may be well versed in security practices, but how many understand the whole picture about how Salesforce is being used in the organization? Do they fully understand the power that Salesforce administrators and users have to unintentionally open gaps in their organization's security posture?

For example, let's look at how email security is dealt with. Email is a mature corporate tool and both incoming and outgoing email messages, including all attachments and links, are subject to in-built scans for malware, spam and malicious links. Many organizations also perform security awareness training so staff know not to insert unknown USB drives into their computers, and they simulate phishing attacks to help users recognize potential phishing and other social engineering activities.

But Salesforce implementations are not often subject to the same stringent security checks and balances. As a result, websites and shared storage spaces created by Salesforce admins often lack even basic access controls, such as usernames and passwords. This results in data being received, and shared with partners, that has bypassed the usual corporate security interrogation procedures, allowing
phishing links and malware to slip through the system and potentially be opened by unsuspecting staff.

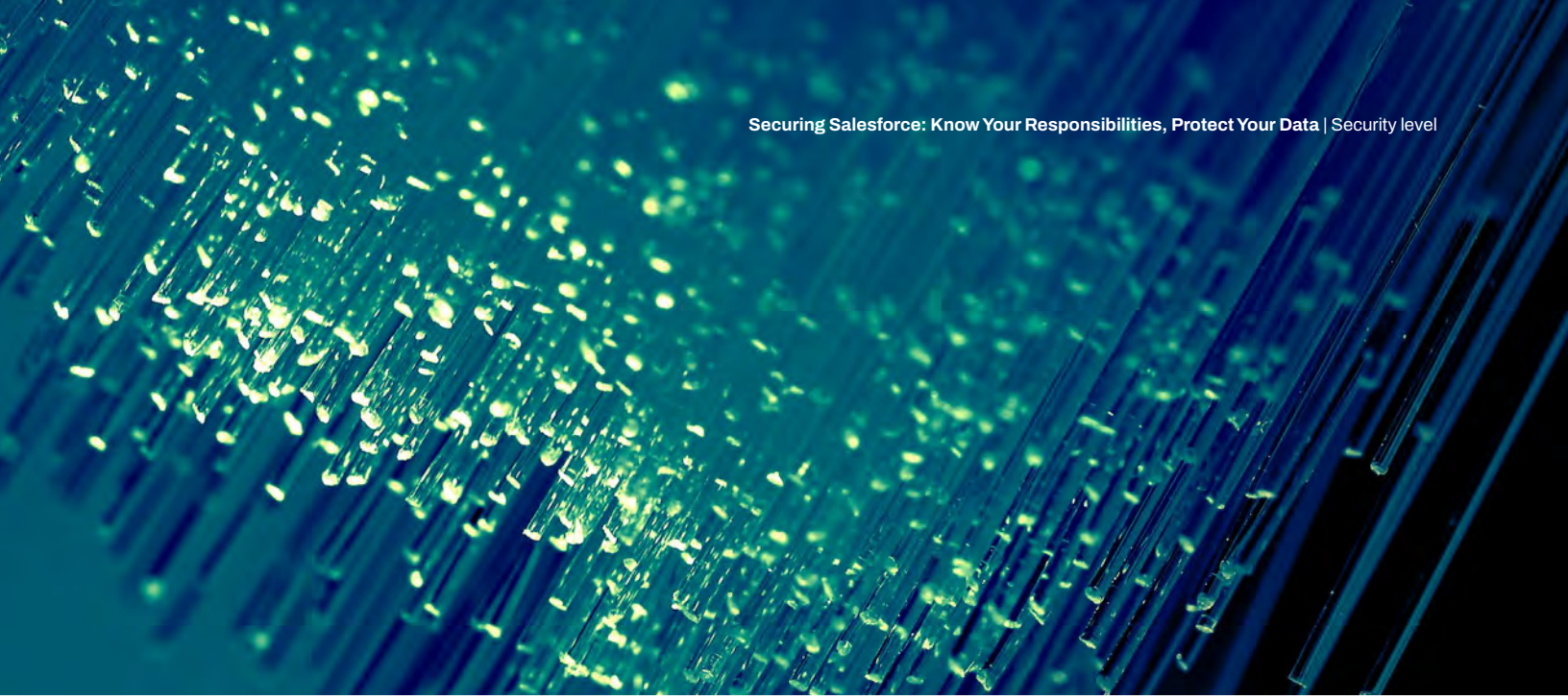
With more than 150,000 companies relying on Salesforce to run their business, and Salesforce installations constantly increasing in size and importance, a lack of communication between the security team and Salesforce managers and administrators is creating an avalanche of data exposures, putting at risk both sensitive corporate data, as well as personally identifiable customer data.

Salesforce and the shared responsibility model

In the shared responsibility model, the software-as-a-service (SaaS) supplier is responsible for security of the cloud, while the software user is responsible for security in the cloud. In other words, service providers are responsible for protecting the infrastructure, which includes the servers, compute, storage, and networks. You are responsible for securing the files, links, and content that they either create or collect from their customers and partners. SaaS contracts list in detail their own shared responsibility model, which highlights the exact boundaries of where their responsibility ends and your responsibility begins.

In itself, the Salesforce platform is extremely secure and the company is continually updating its security posture and helping its customers be more secure by default. However, its customers are ultimately responsible for ensuring they have the appropriate security policies, practices, tools, and culture in place to properly protect their data.

Many customers mistakenly assume that as the files and data being collected come through a form or microsite generated by Salesforce the information is secure or automatically checked for harmful links or files— it is not. It is the customers' responsibility to secure the information. This is one reason Salesforce is increasingly being used by cyber criminals to piggyback malicious files and links into corporate networks.



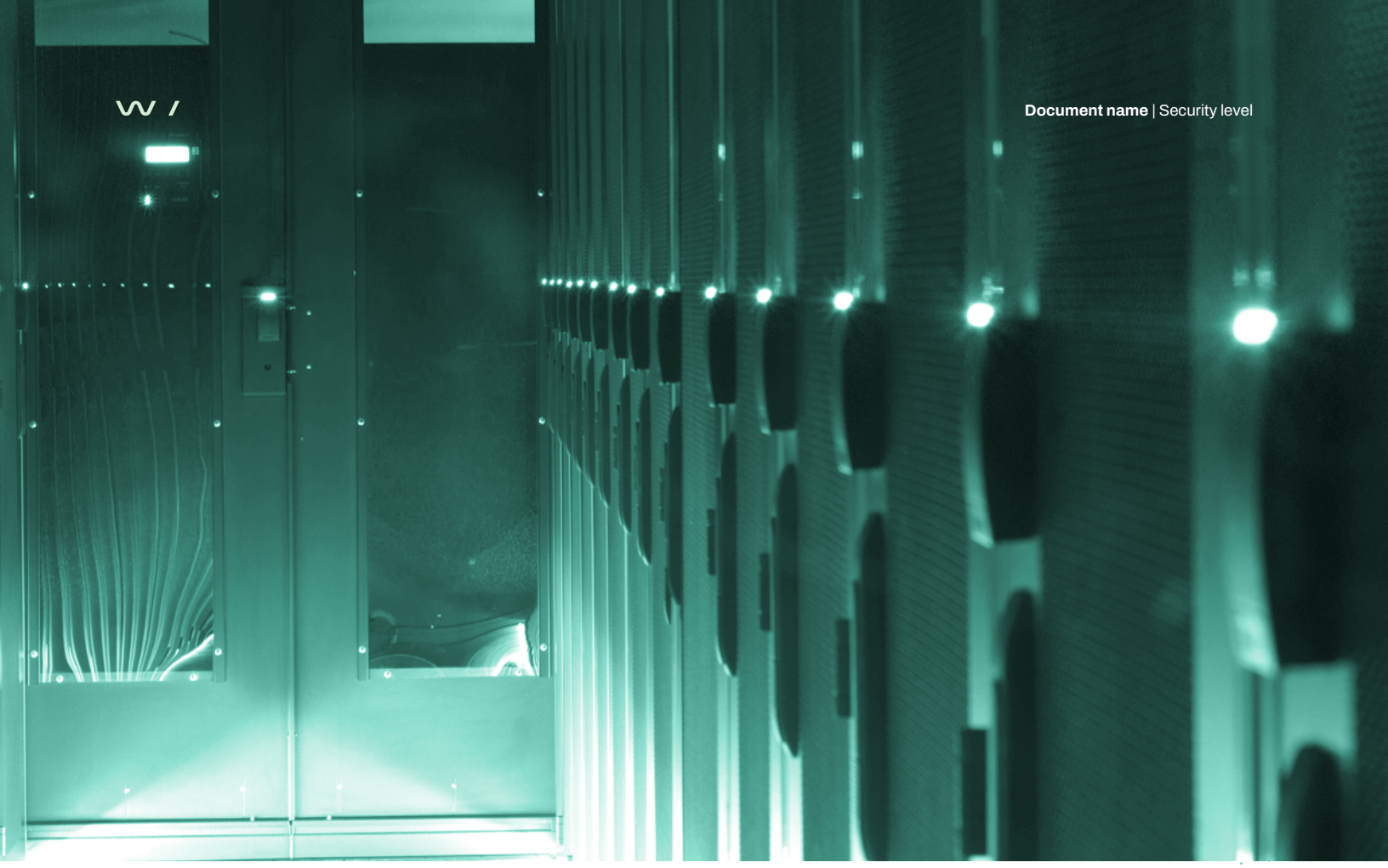
How flexibility, connectivity and automation create security vulnerabilities

Apart from being a CRM tool that helps sales teams to build customer relationships, Salesforce is used by marketers to quickly create forms and websites that allow customers to input data including files, URLs and plain text. We've discussed how many Salesforce misconfigurations result from a lack of access permissions. Users, files, and applications are commonly provided with a default set of access permissions, which increases the risk from both external threat actors and malicious insiders, as well as creating more chances for human error.

Alongside this, organizations are struggling to keep track of their ever-growing Salesforce ecosystem. The SaaS model means it's easy for employees to purchase and implement new add-ons and applications without any involvement from the IT department. As a result, Salesforce is often filled with integrations that have not been properly vetted and are not being monitored for vulnerabilities or suspicious activity.

For example, a consumer might apply for a loan using their bank's website but the online form is actually created using Salesforce. The bank's customers fill in a form that contains personal information and upload confidential documents such as bank statements, identification papers, and other related documentation. This data is stored in a location where, based on the shared responsibility model, the Salesforce users are responsible for security. This means that as bank staff go about their jobs and start to process these applications, unless the local storage systems are properly scanned, they have no idea if the application form is legitimate or contains malicious data. There is the risk that an attacker could pretend to be a client and send malicious files or URLs in an application form. When the unsuspecting staff open the file or link, they risk allowing the malware or ransomware to execute within the bank's internal systems or opening a door that allows a cyber criminal to start infiltrating the network.

Recruiters, health authorities, airlines, insurance companies, and any other organizations that require data and files to be uploaded by their Salesforce systems all face a similar problem. Unless they have adequate security controls in place, they are at constant risk of exposing their internal networks to cyber attacks.



How common are the attacks?

A simple online search for “Salesforce security” will return hundreds of news articles describing how the Salesforce platform has been exploited by cyber criminals using phishing attacks. Phishing is where malicious URLs purport to be innocent but if clicked on, these links can result in dangerous activities such as downloading ransomware, launching keyloggers, and taking screenshots that are sent back to the attacker.

The sophistication of these attacks has been increasing and recent high-profile cases have highlighted how URLs are morphing to avoid detection. For example, a URL might work as expected the first few times it is used but then, on the 5th, or even 30th click, it suddenly changes its behavior and redirects the link to a malicious payload. This highlights the need for a security system that checks the validity of links every time. But it’s not just phishing that’s a problem. Attackers can upload files containing malware or other content onto an unprotected Salesforce system.

WithSecure™ has hundreds of customers using its WithSecure™ Cloud Protection for Salesforce tool, and we found that the number of attacks are increasing at an alarming rate. We've seen a steady increase both in the volume of files and URLs uploaded into Salesforce and in the volume of malicious content. These attacks included malicious files, malicious URLs, phishing attacks, and trojans.

Our figures correspond with research from organizations such as the Anti-Phishing Working Group, of which Salesforce is a member, which reported that 2022 was a record year for phishing attacks, with more than 4.7m attacks worldwide. This is growth exceeding 150% year on year.

How to secure Salesforce

These days, an organization wouldn't consider deploying a new email system or customer-facing application without first considering how to ensure its security. Scanning for malware and rogue URLs would be part of the plan from its initial design. Additionally, both users and security teams understand email technology very well, as they have used similar systems for both work and personal use.

But while securing email is a standard protocol for organizations, securing Salesforce is not.

Security teams and Salesforce managers in organizations need to understand what the default security settings are, and the risks that they're open to. This common understanding should happen from day one, and lead to an ongoing, open dialogue to ensure the security of new Salesforce projects.

Salesforce administrators and business owners should be having conversations with their colleagues in the IT security team at a much earlier stage in their deployment timelines. Too often security is bypassed or seen as a blocker for business projects, but the need to protect their systems as well as customer and organizational data is paramount. Security and risk assessment teams need to firstly be involved to help design the architecture of the Salesforce workflows and storage areas to ensure that the platform's fine-tuned security options are properly configured and fit for purpose. They must then decide which additional layers of security to add to the IT stack to ensure all defence mechanisms are in place to keep rogue intruders and their harmful content out.

Security teams and Salesforce managers in organizations need to understand what the default security settings are, and the risks that they're open to. This common understanding should happen from day one

If the organization plans to make use of core Salesforce products, such as the Experience Cloud, Service Cloud, and Sales Cloud, these should be considered as part of the initial security planning. Make sure that it if these products are implemented, they follow the organization's security policy, as well as industry best practices for the shared responsibility model.

Integrate a security solution that secures your Salesforce implementations by scanning documents and links for malicious content, and automatically quarantines unsafe files and URLs.

WithSecure™ Cloud Protection for Salesforce was developed in close cooperation with Salesforce. We are their most integrated security partner, which is why Salesforce recommends us to secure your cloud activity.

2m+ Danish banking customers' data protected using WithSecure™ Cloud Protection for Salesforce

Several Danish banks have implemented Salesforce to reinforce their relationships and communications with their customers. The platform handles large amounts of data, including sensitive information about customers' personal finances, which is shared between banks. BEC Financial Technologies works with the banks to deliver secure IT services. It is crucial for BEC to protect this data and ensure the data remains clean from malicious code. BEC surveyed three providers of IT security solutions and in February 2021, selected WithSecure™ Cloud Protection for Salesforce.

"We chose WithSecure™ because they are a serious supplier that meets all our compliance requirements. In addition, they were recommended by Salesforce because their software can be implemented easily and quickly. It's almost a plug-and-play solution."
Tonny Rabjerg, Program Director at BEC.

Read the full case study.

SiriusXM uses WithSecure™ to plug unexpected CRM upload vulnerability

Sirius realized its Salesforce-based customer ID management system was vulnerable and was looking for a security solution that rapidly and reliably scans documents submitted to Salesforce before they are uploaded into the system.

“WithSecure™’s reliable plug-and-play approach was exactly what we needed—it was also a relief to know that WithSecure™ are specialists and would take care of any issues in getting it running smoothly, so our technical team could focus on the rest of the project.”
Naman Shah, Senior Director of Project Management at SiriusXM

Read the full case study.

Japanese city leaders secure COVID-19 patient registration on Salesforce with WithSecure™

At the start of the COVID-19 pandemic, the Osaka Prefectural Government in Japan began operating its own registration system to document people in the city who were suffering with the illness. As part of its approach, which involved citizens uploading formal identification to verify their identity to Salesforce, it chose WithSecure™ Cloud Protection for Salesforce to secure its operations and guard against cyber threats.

"We rate it highly because security is ensured and both citizens and personnel can use the system without being conscious of CPSF. It has been operated without any major problems"
Osaka Prefectural Government spokesperson.

Read the full case study.

Why WithSecure™

Why choose WithSecure™ Cloud Protection for Salesforce to protect your Salesforce ecosystem?

Here are four key reasons:

- You can exchange files and weblinks safely without the risk of malware or phishing attacks.
- WithSecure™ Cloud Protection for Salesforce is built as a module within the Salesforce ecosystem. It fully integrates with Salesforce workflows and customizations, so the job of monitoring and mitigating threats is done from inside the system—there are no external portals or complex integrations.
- It only takes a few minutes to install. Once done, your Salesforce data is monitored and secure.
- It was built with close cooperation from Salesforce. It's a tested and proven system that is already used by enterprises and by organizations in the public sector, and is recommended by Salesforce.

Using WithSecure™ Cloud Protection for Salesforce provides your organization with real-time visibility into all the uploads and downloads happening in your Salesforce environment. In addition, all URLs in the system are also checked and protected in real time. Our protection scales with your needs, detecting threats as they arise, and revealing new insights into how users interact with harmful files and URLs as they attempt to access your system. It's simple to use, with security scans available through your Salesforce portal.

Use WithSecure™ Cloud Protection for Salesforce to give you peace of mind that your data is clean and safe, and you can run your digital business undisrupted and with the reassurance you, your customers, and you partners require.

WithSecure™ has over 30 years of experience in cyber security and our technology meets the highest internationally recognized security certifications

Create a Salesforce security action plan now

If there's one thing to remember from this paper, it's to make sure you involve your IT security team as early as possible in your Salesforce project implementation. But if you're already up and running—don't worry—you can take our risk assessment to find out your Salesforce environment cyber risk score.

Below we've mapped out five simple steps to ensure your data is protected.

1. Seek the advice of Salesforce security experts to find out if your CRM is already at risk.

Our experts are ready to advise you on how to get started securing your data. Book a call with one of our advisers now.

2. Find out where you are today.

What are the risks of your current and upcoming Salesforce project(s)? What data will be uploaded—and how? What are the potential fallouts - from a business risk and operational standpoint? Don't forget our risk assessment tool can help.

3. Talk to your Salesforce co-workers and find an internal sponsor to highlight the issue.

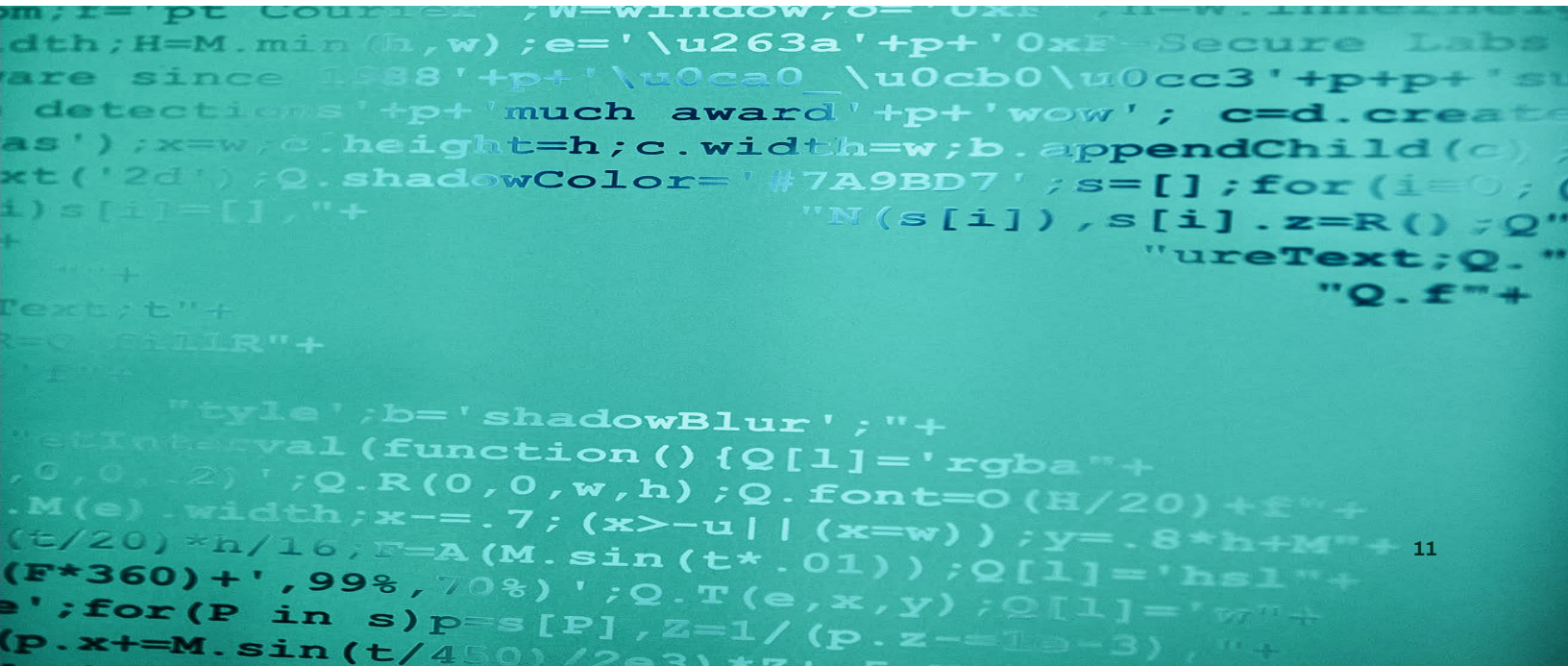
Who in the business is most likely to support you raising your security concerns with the necessary stakeholders—and help you implement a solution? Is the CISO aware of the security issues? Get them onboard, or create a small taskforce if necessary.

4. Find a technology solution that works around your workflow.

With WithSecure™ Cloud Protection for Salesforce, flexible scans run in the background in real-time or on demand with no disruption to Salesforce activities, and zero impact on customizations in your environment.

5. Enjoy peace of mind.

Get back to running business operations and growing your customer base with confidence using the full capabilities of Salesforce.



About WithSecure™

WithSecure™ is cyber security's reliable partner. Our experience and capability, developed over 30 years, protects critical businesses around the world. Businesses across industries trust us for outcome-based cyber security to protect and enable their operations. As an end-to-end cyber security house, we offer comprehensive threat hunting and consulting services, and develop our award-winning security technologies with a deep understanding that our in-house research unit and hands on field experience provides.

WITH® secure