Securing Salesforce in 2023

Scoping out the threats and challenges

Introduction

2022 has been another fast-paced year for cyber security. Prolific threat groups like Lapsus$ and Conti have made waves with major attacks on leading companies and national infrastructure. Even less high-profile criminal gangs are posing a greater threat through tactics such as targeted ransomware.

Cyber attacks predominantly happen through traditional IT systems and end points. However, as more and more businesses are moving their infrastructure and operations to the cloud, threat actors quickly adopt and shift focus to cloud-based environments such as Salesforce.

More than 150,000 companies rely on the Salesforce platform for their critical customer relationship management (CRM) activity, and as such it contains large amounts of valuable and sensitive customer data. Salesforce is also highly collaborative and customizable, supporting a huge array of third-party plug-ins and options for connectivity.

These factors all combine to make Salesforce a tempting target for threat actors. While there have been no major reported cases yet, we believe it's a matter of when, not if.

Salesforce is a very secure platform that has a huge number of security controls designed to create a safe place to store your data. However, there are many controls that customers themselves need to configure appropriately to keep their data safe - this is the nature of the shared responsibility model.

In this report, three Salesforce security experts share their insights on where to focus on Salesforce security in the year ahead. Their experiences are backed up by the latest data produced by WithSecure™ market research on cloud and Salesforce security in 2022*.

Read on to discover the results of the research, and the greatest Salesforce security priorities of 2023 - and what you can do to get ahead of them and start reducing the risk.

Key security topics in 2022

- The biggest security concerns among IT professionals and Salesforce administrators
- The threat posed by misconfigurations and unmonitored assets
- The rise of malicious files and URLs in Salesforce
- Finding the right security controls
- Our top seven recommendations for securing Salesforce in 2023

*WithSecure™ Market Research: B2B market research across 3072 IT decision makers and influencers in 12 countries conducted during April-May 2022: UK, France, Germany, Belgium/Netherlands, Finland, Norway, Sweden, Denmark, US, Canada & Japan

Our experts

Dmitriy Viktorov
Head of Product and Technology, Cloud Protection, WithSecure™

Dmitriy is a seasoned product and security pro who is passionate about solving complex problems and helping customers keep their cloud and digital services secure and protected. He has held different roles in R&D, Product Management and Technology Office, and is currently leading product development of Cloud Protection for Salesforce.

Pankaj Paryani
Salesforce Technical Lead, WithSecure™

Pankaj is a skilled Salesforce Developer & Consultant with multiple projects developed for customers around US, UK and APAC regions. His recent role focuses on leading the CRM Development team at WithSecure™ to make sure Sales and Services are securely up and running with their customer needs.

Doug Merrett
Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

Doug is a passionate security advocate who worked at Salesforce for 13 years as a Platform and Security Specialist, in the UK and Australia. During that time, he helped many customers understand Salesforce's approach to security & infrastructure and guided them on maximising the security of their data stored on the Salesforce Platform. In June 2021, Doug started his own consultancy, Platinum7, just focusing on Salesforce Security, Compliance and Resilience.

The biggest security concerns among IT professionals and Salesforce administrators

Top 5 Security Challenges

1. Preventing data breaches.
2. Ensuring protection against malware and ransomware.
3. Preventing advanced e-mail based threats, such as phishing or business email compromise.
4. *Ensuring security of cloud-based collaboration applications, such as Office 365 and Salesforce.
5. Ensuring the security of an increasingly diverse pool of devices, services and software.

* Cloud and collaboration

Cloud platforms like Salesforce have become essential for maintaining remote and hybrid working strategies accelerated by the pandemic, as well as delivering advantages in terms of improved efficiency and agility, and reduced costs and resources. However, cloud environments create more gaps and moving parts, many of which are out of direct control.

"For decades, everything used to be in your direct control on-premise, with only a limited number of external connections to worry about. Now everything is in the cloud, many critical systems are out of direct control."

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

In the last 18 months, what have been your top three pain points in managing data security?

(From the Salesforce Top Security Trends for 2022 report)

* **59%** Third-party security management

** **53%** Keeping up with compliance regulations

49% Mobile device security

38% Resource constraints

37% Vulnerability management

28% Managing proactive hacking prevention measures

15% Auditing

5% User behaviour

* Third-party security management

Salesforce is designed to be highly customizable, making it easy to find and implement new capabilities as needed. There are more than 3,400 applications on the Salesforce AppExchange alone, and countless third-party APIs and plug-ins readily accessible online. While this is good for integration and accessibility, it also creates an extensive third-party supply chain that can quickly grow out of control. Each add-on increases the potential exposure to supply chain attacks. With supply chain attacks dominated the wider cyber security landscape over the last couple of years, it's no surprise this is a key concern for Salesforce security. Read more from our latest report on Salesforce third party management.

** Regulation and compliance

The regulatory landscape has continued to evolve, and complying with security and privacy regulations has become increasingly complex as digitalization and cloud migration accelerate. With various regions having their own laws and regulatory bodies, firms must be acutely aware of where their data is being transferred, stored and processed. Firms must also be mindful of industry-specific regulations such as those in healthcare and finance.

There are more changes ahead as new regulations are introduced and others updated. The European Commission is set to publish new directive NIS2 (Network and Information Systems), expected to come into law within the next 18 months.

What are your top three IT security concerns?

Ransomware and phishing

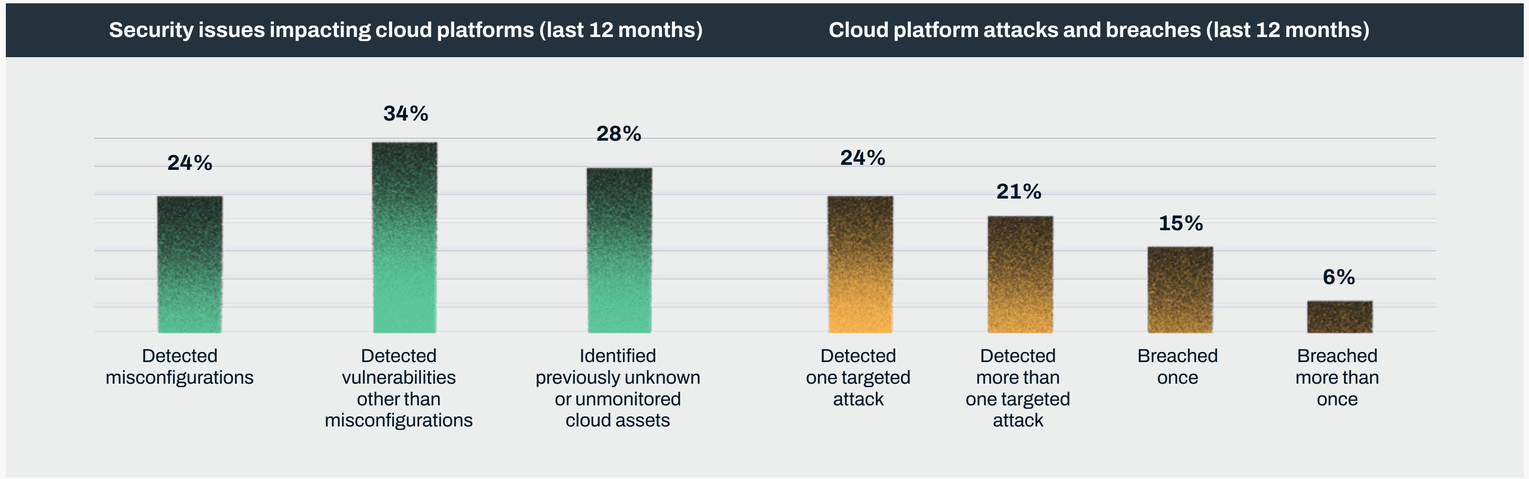
Phishing is traditionally considered an email-borne threat and adversaries continue using emails for phishing attacks. Unforunately, Salesforce is not immune to phishing attacks as the platform provides different email based flows such as email-to-case or email-to-Chatter. Moreover, with Slack, Chatter and other third-party options, Salesforce offers a number of communication and collaboration channels that can also be exploited in phishing attacks.

Similarly, while the Salesforce environment itself is fairly inaccessible to standard ransomware, it can be exploited to deliver malicious files and links to target systems. It's also important to consider that ransomware and other malicious programs are evolving rapidly. The high-flex communication features of Salesforce could potentially create opportunities for such next-gen threats.

Access visibility and control

Based on their own experience, our experts also highlighted visibility and control of network connections as a major concern. Firms must both have a strong grasp of how critical data and systems can be accessed by internal and external users, and how their Salesforce platform connects and interacts with other systems.

The threat posed by misconfigurations and unmonitored assets



The fact that a quarter of respondents believed they were the victim of a targeted attack on the last 12 months demonstrates that adversaries have become more sophisticated and organized. However, many organizations are making the attackers' lives easy by failing to properly configure and monitor their cloud environments.

Misconfigurations are especially common because the options for the average cloud environment are immense. The most common Salesforce configuration issues we encounter relate to access. Both users and applications are often left with a default level of permissions which grant a high level of privileged access to the platform. This greatly increases the risk from both external threat actors and malicious insiders, as well as creating more chance for human error.

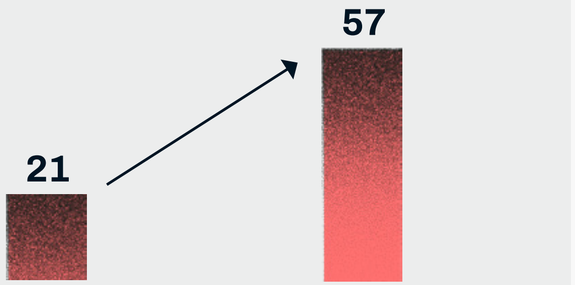
Alongside this, organizations often struggle with keeping track of their systems. The Software-as-a Service (SaaS) model means it's all too easy for employees to purchase and implement new add-ons and applications while leaving the IT department in the dark. As a result, Salesforce is often riddled with elements that have not been properly vetted and are not being monitored for vulnerabilities or suspicious activity.

"Complexity is the enemy of security. The more complex the environment, the more likely something will be overlooked and not configured correctly. As a highly customizable platform, Salesforce offers many opportunities for misconfiguration."

Dmitriy Viktorov, Head of Product and Technology, Cloud Protection, WithSecure™

Malicious files and URLs in Salesforce are on the rise

File / URL detections per customer per month



During the past 6 months detection volume of malicious files and URLs increased 171 %

Top 5 malicious detections and file types

1. HTML files 49 %
2. Archives rar/zip file 23 %
3. Microsoft Office files 10%
4. Exe/com files 4 %
5. PDF files 3%

*past 6 months

Top 5 malware types:

1. Trojan 54%
2. Adware 15%
3. Exploit 12%
4. Other 12%
5. Downloader 2%

*past 6 months

It is widely accepted that the number of attack attempts has been steadily increasing, and this trend is clearly supported by WithSecure's own data from monitoring Salesforce environments. In the last six months, we detected an average of 57 malicious files or URLs per customer per month. This represents a 171 percent increase over the average in the previous six-month period.

Malicious HTML files are the most popular attack method, making up more than half of files we detected. Of the malware-based attacks we identified, the majority involved Trojan type malware.

We have also noticed several trends that seem to indicate threat actors specifically monitoring for Salesforce assets to attack. For example, if a customer implements Salesforce Experience Cloud and creates a portal for content uploads, the number of detected files and URLs quickly increases soon after.

It's also notable that there are more malicious URLs being detected than there are files. Adversaries are aware that more firms have strong strategies cantered around file scanning and have swapped to the more versatile and harder to detect URL approach.

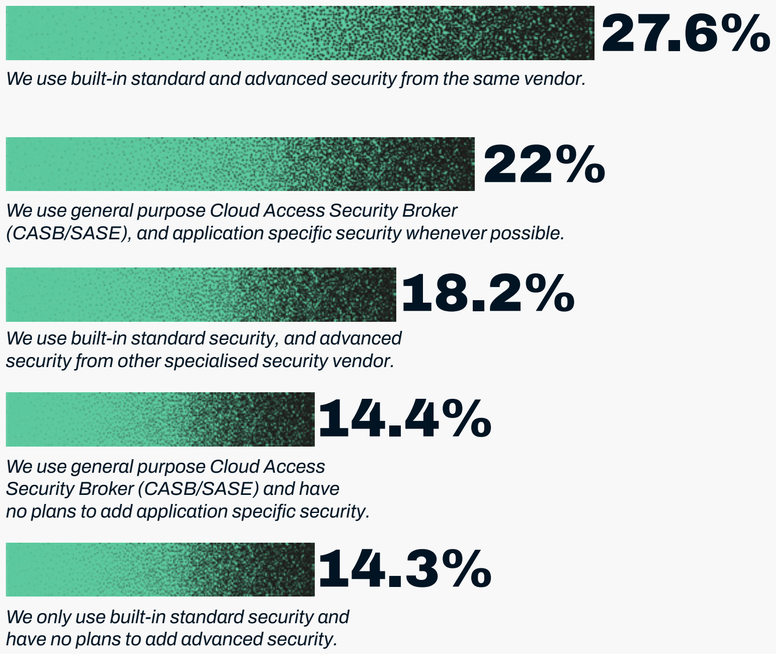
"Everyone knows to scan for malicious files, but scanning URLs still isn't always standard practice, especially outside of email."

Doug Merrett, Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

Finding the right security controls

Which of the following statements concerning Cloud Application security apply best to your company/organization?

(e.g.,Office 365, Google Workspace, Salesforce)



Our research discovered a wide variation in cloud security capabilities. While most respondents used a mixture of specialist security applications, a sizeable number are relying only on the native security capabilities of the application or platform.

These built-in tools are a good starting point, and often benefit from being built by the application's vendor. However, they also usually leave some important gaps. For instance, Salesforce does not provide security for unstructured data, and has no native functionality for scanning content uploads and downloads.

Ideally, firms should be combining native security functionality and in-house Salesforce services with specialist security tools from at least one vendor to fill in the gaps. Enterprises should also try and cover all their bases with solutions from a single vendor whenever possible. Using solutions from several different vendors can be difficult to manage as teams will have to contend with multiple disconnected data streams and threat alerts.

If selecting a Cloud Access Security Broker (CASB), those that function as proxies can be more difficult to implement as they must be configured specifically to each SaaS product, and can be very brittle. API-based CASBs or natively integrated solutions turn to be more versatile and useful.

"Built-in vendor tools rarely cover everything, but they can be very effective as the developers know the system so well. Having another specialist tool over the top will give balance and cover any gaps."

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

Our top eight recommendations for securing Salesforce in 2023

Reviewing the key data points of 2022 sets the scene for the biggest security priorities of the year ahead. Here is what our experts recommend focusing on for 2023 and beyond.

1. Manage identity and access

Focusing on managing system access is one of the most reliable quick wins. Multifactor authentication (MFA) will immediately and significantly reduce the risk of breaches, and with this now being included with Salesforce as standard, it can be deployed quickly and at no extra cost.

Alongside this, implementing a least privilege approach to system access for both users and API integration will greatly reduce the attack surface. While this is a slower process, it is extremely important.

2. Monitor for incoming threats to Salesforce

Threat actors are expanding their attack toolbox beyond email. Salesforce's content upload function and in-built communications channels like Chatter can be exploited in malware and phishing attacks – but the platform lacks native content monitoring capabilities. WithSecure™ Cloud Protection for Salesforce was designed in conjunction with Salesforce to scan all inbound and outbound content in real time to identify and block malicious files and URLs.

3. Keep up with privacy and compliance regulations

The regulatory landscape is continuing to shift, and with so many moving parts in the Salesforce environment, keeping track of compliance can be a complex task. Adhering to a strict least privilege approach with minimal access by default will go a long way to ensuring compliance. For regulations that extend to third parties, strict vetting should be implemented to cover connections and responsibilities.

4. Don't let built-in tools go to waste

Salesforce includes a number of very useful tools as standard, so make sure you're getting the best out of them before you start investing in third party solutions. Health Check and Optimizer are two tools that can go a long way to quickly highlighting possible misconfigurations or lose access controls.

"While Salesforce is working to keep its infrastructure secure, users must recognize their responsibilities in securing their instances. The days of Salesforce not being targeted are close to zero, so there is no time to waste"

Doug Merrett, Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

"Effective user monitoring is a must. It will not only help catch threat actors and malicious insiders, but also accidents and misconfigurations."

Doug Merrett, Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

5. Back up your backups

Reliable backups are one of your most valuable resources for improving resilience. Being able to restore your Salesforce instance will greatly reduce the impact of attacks like ransomware that seek to damage or destroy your CRM data. Backups also provide another layer of protection from human error, enabling you to hit the reset button when misconfigurations or a bad app integration start causing issues.

6. Do your due diligence

As your Salesforce environment continues to expand, it's more important than ever to be thorough with due diligence. When choosing to implement a new third party application or plug-in, ensure you investigate the vendor and check if they are reliable and trustworthy. The community is good at leaving accurate reports on the AppExchange store, so this is a good starting point. Reviews are updatable, so it's worth checking in to see if there have been any changes over time.

7. Enable event monitoring

Event monitoring is critical to understand what is going on within your Salesforce environment, allowing you to see how users and applications are accessing and interacting with your critical data. This visibility is critical to protecting your Salesforce platform from both external attack attempts and risks from within, whether from malice or by accident.

This forensic data is only useful if it can be properly absorbed and understood, so tools like Splunk and Imprivata FairWarning are a useful way of getting on top of things.

8. Safeguard sensitive data

Business data is vital and every bit and byte is worth protecting. However, pay special attention to customer and sensitive data. Use Salesforce Shield or other third-party solutions to find, encrypt, monitor and retain sensitive data.

"Salesforce is continually improving its capabilities against threats like phishing with new in-built features. But users need to do their part in properly implementing and utilising these tools."

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

"Supply chain attacks have been a big issue for the last two years, and they aren't going anywhere in the year ahead. Organizations need to prioritise understanding and securing their extended digital environments."

Dmitriy Viktorov, Head of Product and Technology, Cloud Protection, WithSecure™

WithSecure™ Cloud Protection for Salesforce complements Salesforce native security capabilities by mitigating the risks in uploaded files and URLs.

Get in touch

salesforce PARTNER SINCE 2016

Data sources

WithSecure™ 2022 B2B Market Research study reached 3072 respondents with an online survey conducted in May 2022 across 12 countries, including 9 European countries: UK, France, Germany, Belgium, Netherlands, Denmark, Finland, Norway, Sweden, as well as North America: US and Canada, and Japan. All respondents are IT/Network/Cloud Security decision makers and influencers for purchase of IT/Network/ Cloud Security Products and Services in their organizations.

The numbers and trends of malicious file and URL detections were collected by WithSecure™ from internal, anonymized data of threat analysis requests received from protected Salesforce environments.

Salesforce's Top Data Trends for 2022 – Based on a survey of 300 InfoSec and IT executives conducted by Salesforce and Pulse.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure