Report

Anatomy of a Salesforce supply chain attack

How to prevent supply chain attack through third party integrations with Salesforce

Contents

1. Introduction
The state of play for digital supply chain risk

Every modern enterprise today sits at the center of a vast and complex network of digital suppliers. Affordable high-speed internet and the vast and fast-growing global cloud market mean that organizations can easily outsource anything they need to grow their business. Specialist software solutions can be accessed through SaaS models, or firms can acquire components and plugins to heavily customize their own infrastructure.

The digital supply chain offers unparalleled flexibility and freedom, enabling organizations to rapidly acquire new capabilities and seize opportunities. But it also comes at the cost of increased cyber risk exposure.

Introducing a web of thousands of moving parts makes it extremely challenging to maintain effective visibility of the IT estate and identify potential vulnerabilities.

However, threat actors are also actively seeking to exploit these connections. Attacking third party connections such as SaaS suppliers or software plugin developers enables cyber criminals to bypass security defenses and potentially strike at the heart of an organization's network. This connectivity can be exploited to deploy malware, including highly destructive targeted ransomware, within the target business, exfiltrate high-value data, or establish command-and-control.

Gartner® has named digital supply chain risk as one of the leading security and risk management trends for 2022 and predicts that, "by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."[1]

Indeed, it has already been estimated that supply chain attacks have tripled in 2021 alone. Some of the biggest data breaches of the last year have centered on digital supply chains.

1. Gartner Press Release, "Top Trends in Cybersecurity 2022", Published 18 February 2022

Log4Shell

This high-profile exploit affected the popular Apache Log4j 2 java library used for logging error messages. The vulnerability, officially CVE-2021-44228, enabled an attacker to gain remote access to a device running certain versions of Log4j 2 through text messages. The flaw was discovered and quickly patched in December 2021 but may have been around since as early as 2013. It is thought that nearly half of all organizations may have bene targeted using the vulnerability at some point.

Okta

In March 2022, secure MFA provider Okta announced that it had suffered a major security breach in January that impacted hundreds of customers. The breach demonstrated how third-party connections are targeted and exploited, as it began with the compromise of a sub processor supplying Okta. The attackers, a hacking group known as Lapsus$, was then able to enter customer networks and access data using a remote desktop tool.

Office 365

Threat actors have increasingly targeted the extended Office 365 environment in targeted phishing attacks. The victims are first hit with an email prompting them to login into their 365 account and verify a new application. Rather than the usual imitation phishing site, the email links through to the user's genuine Office 365 login page. The threat is the application itself, which will provide the attacker with access to the user's files and emails. Because it is already within the environment, the rogue application can circumvent the need for multifactor authentication (MFA).

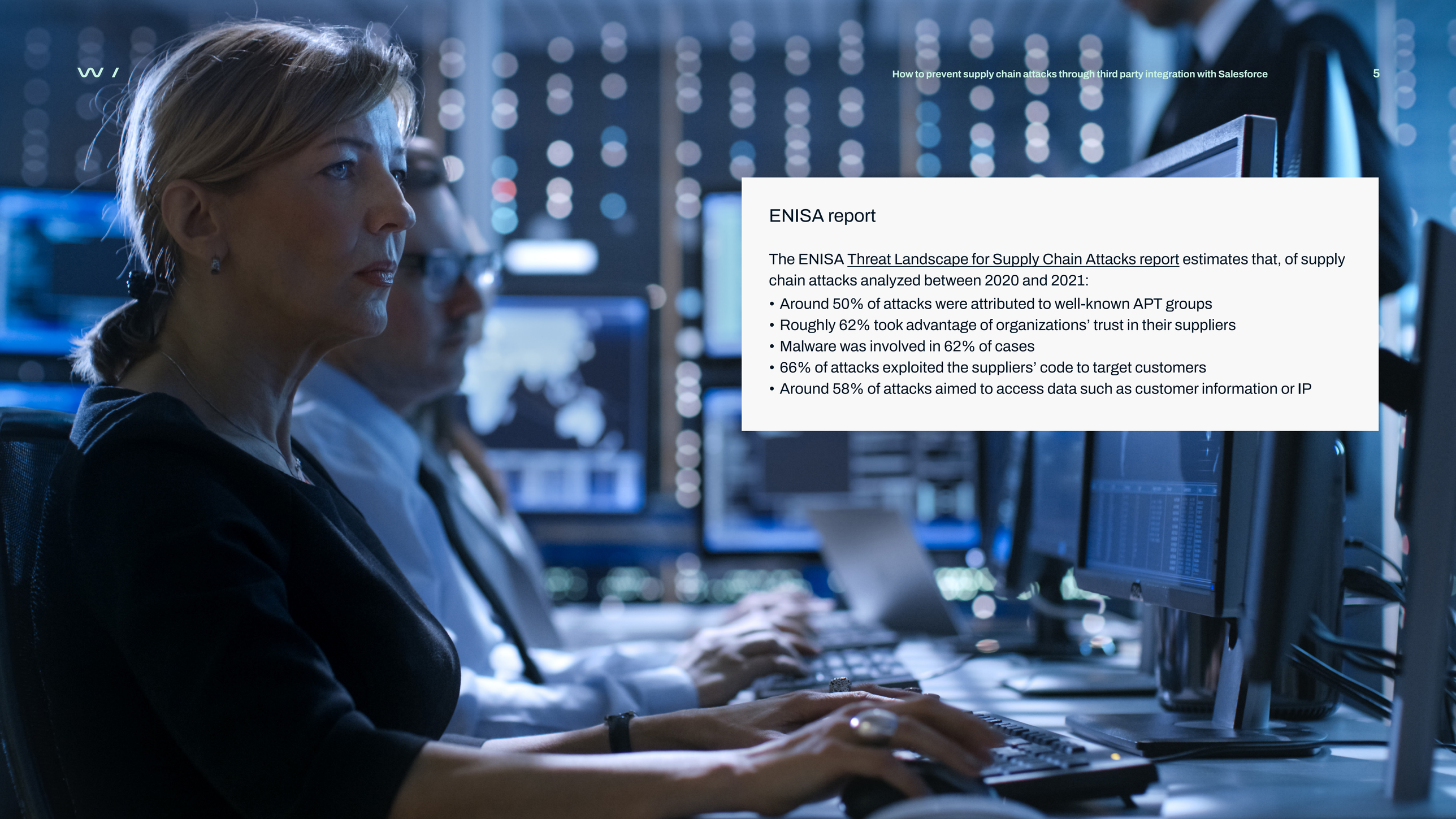
SolarWinds

Despite occurring in 2020, the SolarWinds attack remains the most notorious example of a high-end digital supply chain attack. Widely believed to be the work of Russian-backed operatives, the incident saw software vendor SolarWinds breached in a sophisticated multi-pronged attack that targeted its popular Orion solution. The perpetrators covertly injected malicious code into an update for the software, enabling them to access the networks of thousands of users, including governmental bodies such as the US Treasury and Justice department.

These attacks demonstrate why all organizations need to take digital supply chain risks seriously. A single compromised application can affect thousands of organizations around the world. Enterprises must ensure they understand the scale of the danger and move to update their security capabilities to keep pace as their digital connections continue to increase.

Supply chain risk is an issue for any area of the business that has undergone digital transformation and integrates third-party software. The more important the business function, the bigger the risk.

As such, Salesforce, as the CRM system relied upon by more than 150,000 organizations around the world, is one of the software environments most at risk of these attacks. While Salesforce infrastructure has not yet been involved in a major supply chain incident, successful attacks cannot be ruled out in the future.



ENISA report

The ENISA Threat Landscape for Supply Chain Attacks report estimates that, of supply chain attacks analyzed between 2020 and 2021:

- Around 50% of attacks were attributed to well-known APT groups
- Roughly 62% took advantage of organizations' trust in their suppliers
- Malware was involved in 62% of cases
- 66% of attacks exploited the suppliers' code to target customers
- Around 58% of attacks aimed to access data such as customer information or IP

2. How third-party integrations introduce new threats to Salesforce

Salesforce is an essential asset for many organizations, often playing a defining role in their entire customer management and digital experience strategy. As such, there is a huge market demand for the ability to customize and configure the environment to suit different operational needs.

The Salesforce platform can be heavily customized and extended with third party applications, components and cloud services. Salesforce AppExchange, the platform's official app store, offers more than 3,400 apps, and organizations can also connect their Salesforce environments with external systems or applications via SOAP or REST APIs. Those systems may be hosted in different cloud environments and use a variety of proprietary or open-source software. In addition, Salesforce platform supports traditional email or web-form based integration

With so many options, enterprises are guaranteed to find third-party support for any adaptions and extensions they want to apply to their Salesforce environment. However, each new addition also increases the organization’s exposure to digital supply chain risk.

There are multiple potential threats here:

Malicious imposters

In the worst-case scenario, third-party assets may have been created specifically as attack vectors. Organized criminal groups download legitimate applications and reverse-engineer corrupted clones that hide malicious code before re-publishing them for download. While there have been no reported cases in Salesforce’s App Exchange, the issue has become increasingly common in Android, Google and other sources. Salesforce’s strict security vetting requirements render the App Exchange a reasonably safe source, but this doesn’t extend to the many other online software resources. It is also difficult to control what an application does after installation, leaving a window for previously vetted apps to be used for malicious purposes.

Compromised software

As aptly demonstrated by the SolarWinds and Kaseya breaches, cyber criminals can also seek to exploit the digital supply chain by first targeting the software vendor. This enables them to use legitimate, previously vetted applications as an effective attack vector that will bypass many traditional security defenses. Such attacks are resource intensive and so usually reserved for organized groups targeting high-value organizations or seeking to hit a large number of victims with sophisticated attacks like ransomware. As such, individual Salesforce users may not be the most lucrative targets, but Salesforce and its higher-profile integrators will be.

Vulnerable code

Any digital asset can naturally introduce cyber risks without the intervention of a threat actor. Software vulnerabilities are an ever-present risk of doing business in the digital age, and a record-breaking 19,733 were reported in 2021. Even the most well-tested application from a vendor with an impeccable reputation will inevitably be found to contain at least some vulnerabilities.

Whatever the source, even a single unsecure third-party application or component can be enough to facilitate a serious security breach.

A complex environment with hundreds of additional apps and plugins quickly becomes extremely difficult to manage. With so many ants crawling around performing different tasks, even the best admins will struggle to see what's happening on the other side of the ant hill.

But there is a worrying tendency to assume the environment will remain secure simply because it is Salesforce. While system administrators and development and infrastructure management teams are increasingly aware of the challenges in securing other environments such as AWS, the more straight forward nature of Salesforce means it is often taken to be self-contained and self-securing. More complex infrastructure-as-a-service (IaaS) platforms like AWS will involve IT, network and security teams from the beginning, but Salesforce is unlikely to be afforded the same attention.

The threat within

Like any other digital environment, Salesforce can become highly vulnerable when it has not been correctly configured.

Misconfigured applications and ineffective identity management can quickly leave the environment exposed. Threat actors are adept at sniffing out poorly secured user accounts and applications that have been left with their default settings in place. Weak access controls make it far easier for cyber attackers to infiltrate the environment.

This is a serious issue even before the introduction of hundreds of new elements through third party applications and components. It can be particularly problematic for larger organizations, where a lack of coordination across branches and departments means the environment is bloated by redundant apps and plugins for the same tasks. Smaller firms meanwhile may be more streamlined but will be more likely to add new components on the fly without effective safeguards.

It should be noted that Salesforce has since taken steps to make poorly configured sharing rules more visible to help reduce the risk and has published release updates that change default settings to more secure ones. Salesforce Optimizer, a Lightning Experience application, can for example be used to conduct regular checks and highlight any potential issues around guest users.

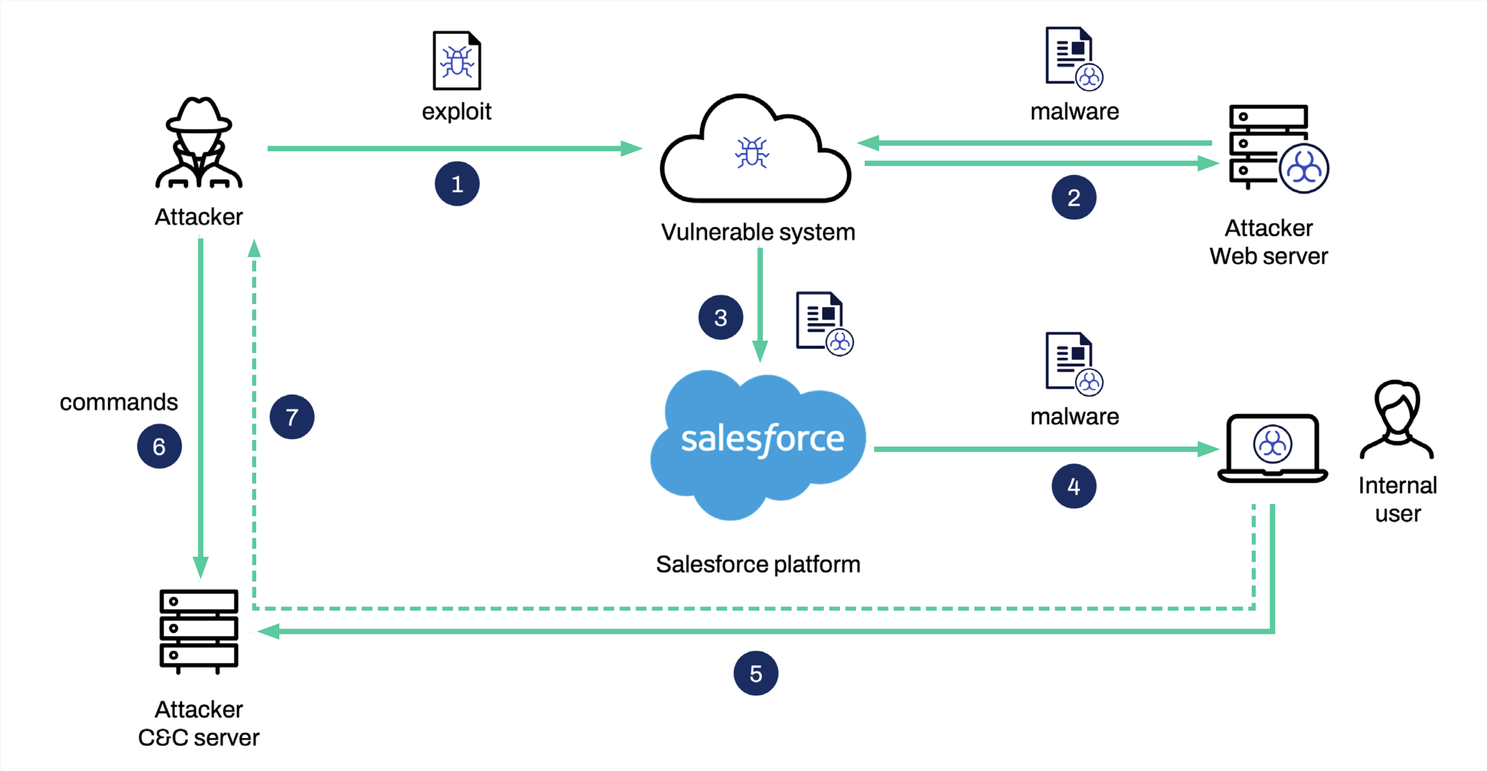
3. Anatomy of a Salesforce supply chain attack

The scope and complexity of the Salesforce environment means there are multiple ways it can be targeted and exploited as part of a digital supply chain attack. Here are two examples of attack scenarios.

Scenario 1: Vulnerable third-party system

Here, the attacker identifies a vulnerability in a software application integrated with Salesforce, such as a tool that retrieves data for analysis, and exploits it to achieve remote access of the system. The vulnerable application is connected to Salesforce via API, and since these usually have a higher trust level than a human user, the attacker is able to access the system with relative ease.

The attacker may seek to steal or damage data within Salesforce but can also use the platform's capabilities as part of their attack chain. For example, malicious documents and URLs can be seeded throughout the environment to be clicked and downloaded by unsuspecting users, including employees, customers, and other connections. These users can then be compromised, and their system access exploited to continue the attack on the rest of the company's IT infrastructure.



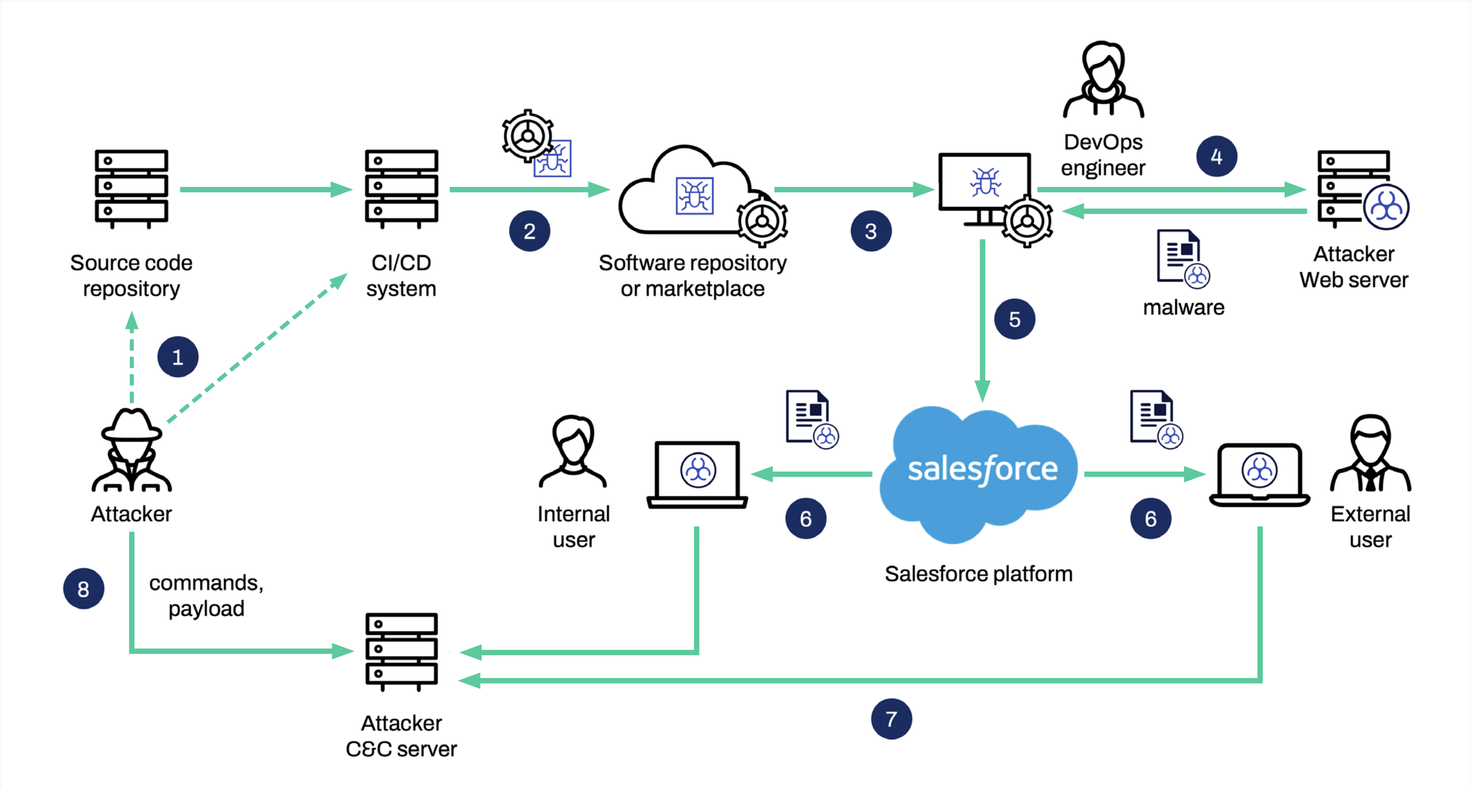
1. The attacker exploits the vulnerability in the 3rd party cloud (or on-prem) system connected to Salesforce.
2. The attacker executes the exploit code to gain access to the vulnerable system and download malware from the special web server.
3. The attacker "injects" malware to Salesforce platform. For example, malware is attached to a case, Chatter post or uploaded to the common file library.
4. The internal user downloads a file with malware and opens it on his/her device. The user doesn't notice anything abnormal.
5. The malware connects to the command-and-control (C&C) server hosted by the attacker.
6. The attacker finds out that malware is inside and has successfully connected to the C&C server. The attacker interacts with malware by sending additional commands or payload.
7. The attacker exfiltrates sensitive data from the internal user's computer and/or Salesforce.

Scenario 2: Compromised development tools

In this scenario, the threat actor first targets either a source code repository or the CI/CD system of a software vendor in order to introduce malicious code into its product. The initial system access can be achieved in multiple ways, with the use of phishing to acquire user credentials being one of the most common tactics, as demonstrated by SolarWinds.

The application or component is then integrated into the Salesforce environment, enabling the attacker to exploit its connectivity to compromise other users and endpoints. Again, from here they can achieve whatever malicious goals they have. The process may even repeat itself, with the targeted organization serving as yet another stepping-stone in an extended supply chain attack.

The attacker may access the Salesforce instance directly on the first pass or may implement a backdoor and wait until the integrator has production access later on. There is a tendency for developers to blindly trust in the security of their tools, particularly if they come from a known vendor. However, as SolarWinds demonstrates, even a well-established vendor can be a source of risk if they are compromised by organized attackers.



1. The attacker scans public source code repository and finds credentials for CI/CD system, which he eventually gains access to.
2. The attacker “injects” specially crafted payload to the software package built by CI/CD system and published to the official software repository or marketplace.
3. The DevOps engineer gets the package from the repository/marketplace with payload and runs it on his/her computer.
4. The payload downloads malware from the attacker’s web server.
5. As the DevOps engineer has access to Salesforce, malware is uploaded to Salesforce.
6. The internal and/or external user downloads malware and opens it on his/her computer.
7. Malware connects to the attacker’s command-and-control (C&C) server.
8. The attacker sends commands and additional malicious payload to the victim’s computer(s).

4. Best practice for mitigating digital supply chain risk

Cyber security is a complex issue that cannot be solved by a single magic bullet. This is especially true for a cloud environment as large and dense as Salesforce. As such, mitigating the risk of digital supply chain attacks on Salesforce requires a multi-layered approach that combines the right security solutions with the right processes and policies. Some of the most important elements to a Salesforce security strategy include:

Implementing Application Portfolio Management (APM)

All applications and components must be thoroughly vetted before they are introduced to the Salesforce environment. This includes researching any known vulnerabilities and previous incidents involving the asset and its vendor and verifying that these issues have been closed. Implementing an Application Portfolio Management (APM) process will coordinate vetting future applications and inventorying existing assets. Due diligence also extends to the vendor itself, and organizations should ensure that all third parties have an appropriate level of security in place to mitigate the risk of a supply chain attack. This also includes the risk of vulnerabilities accidently being implemented in updates

Companies with a particularly high-risk profile can introduce security requirements as part of their service level agreements (SLAs). Firms should also be particularly wary of the vendor's origin in today's geopolitical climate to minimize the risk of nation state-backed operatives.

Risk mapping potential breach impact

In addition to vetting the asset itself, organizations should conduct an in-depth review of its place within their Salesforce environment and consider the impact if it is involved in a breach. This means considering what capabilities the product has and how it connects with both Salesforce and other areas of the IT infrastructure.

Introducing risk is an unavoidable cost of doing business, but enterprises must be sure the risk level is acceptable against the benefits of the new component, and that they integrate this into their security strategy.

Gaining a centralized view of third-party assets

For larger Salesforce environments that include hundreds of third-party components, it can be all but impossible to keep track of everything. However, administrators need to focus on gaining as much visibility as possible to reduce the potential for blind spots that can lead to serious incidents.

Ideally, they should prioritize gaining effective control and visibility of the most important and high-risk third-party elements, and then gradually work their way from there. Establishing structured policies for how new assets are introduced will also help to ensure that visibility is maintained as the environment continues to grow and reduces the chances of redundant applications being added.

Eliminate misconfiguration and access issues

Alongside looking outward at their digital supply chain, firms must also focus on their own internal processes. Misconfigured applications and poorly handled access management can leave the door wide open for cyber attackers, even before the introduction of third parties.

Admins should look to audit their Salesforce environment to ensure that applications have been correctly configured with the appropriate level of access rights. Ideally, all assets should be set to the minimum level of access required and have any sharing capabilities disabled unless specifically necessary.

This extends to the organization's users. Both human user profiles and automated systems should be configured to a least privilege approach that only equips them with the access rights needed for their job role. This is particularly important when it comes to system admins, as firms often tend to default to giving admin rights to any user connected to the system.

Following best practice around system access will reduce the chances of a threat actor exploiting the environment and mitigate the impact of what can be achieved if a user or application is compromised.

It's important to remember this isn't a one-and-done action. All new features on Salesforce should be periodically reviewed through the provided release notes.

Organizations with particularly extensive environments should ideally conduct regular in-depth reviews of their system configurations. WithSecure's cloud consulting service can provide specialist expertise to ensure nothing is missed.

Block malicious content on Salesforce

Threat actors will use a wide variety of methods to begin their supply chain attack, with the use of stolen credentials being among the most common approaches. In order to prevent supply chain attacks involving phishing, stolen user credentials, and malware, organizations need a holistic approach to security that includes endpoint, network and cloud-based protection.

WithSecure offers a range of solutions to help customers prevent, detect and respond to modern attacks.

However, they must also account for the fact that Salesforce itself can be exploited as an attack vector. Its support for uploading and downloading content is a critical feature for many organizations, for example enabling insurance customers to upload their claims documents and proof of identity, or recruitment firms to send and receive job specs.

This core function can also be exploited to upload malicious files and URLs into Salesforce as an effective alternative to email-based phishing. A compromised Salesforce environment can likewise be used to share malicious content with users and customers.

While Salesforce is responsible for securing data within its environment, it does not vet content being uploaded or downloaded – this responsibility falls on the organization.

WithSecure Cloud Protection for Salesforce is one of the most effective ways of closing this attack path. The solution is a market leader designed to prevent attacks from being conducted via malicious files and URLs uploaded to Salesforce by sophisticated criminal groups and users outside of an organization's cyber security perimeter.

The solution scans all content being uploaded and downloaded in real time to identify and block any malicious content, informed by the latest threat intelligence from WithSecure. Cloud Protection for Salesforce was developed in cooperation with Salesforce to provide powerful protection without impacting employee or user experience.

Implementing an effective response plan

Finally, it is important to realize that the threat of a data breach has become a case of when, not if. Even organizations with mature security strategies supported by large budgets can be breached eventually be a sufficiently skilled and determined attacker.

As such, all firms should prepare for the worst-case scenario of a digital supply chain attack impacting their Salesforce environment. The priority here is to implement an effective incident response and remediation plan to quickly identify and close threats and restore normal business operations as quickly as possible.

The Salesforce Shield service offering provides access to capabilities such as detailed logging and per-field encryption. This can bolster key needs such as activity monitoring that are useful in detecting and analyzing incidents.

Organizations also need ready access to the specialized skills and tools needed to hunt down the source of the breach and remove any lingering threats within the environment such as hidden malware droppers and command and control programs. Working with a specialist partner is one of the most cost-effective ways of acquiring these capabilities.

Firms also need to plan for mitigating the impact of a compromised Salesforce environment, which could result in their entire CRM process grinding to a halt. Implementing regular system back-ups and alternative communication methods can help keep the business moving while the crisis is resolved.

5. Getting ahead of digital supply chain risk in 2022

- Supply chain risk is growing rapidly as threat actors seek new attack paths to evade defenses
- The extended Salesforce environment is vulnerable as an attack path unless organizations take precautions
- Businesses should prepare now before they fall victim

Supply chain risk is an unavoidable part of doing business in the digital era. Enterprises must be aware that the threat is increasing as both their own supply chains expand, and threat actors continue to look for new opportunities to evade security defenses.

As their digital footprints expand and connect with more third parties, organizations must ensure that their ability to monitor and control the extended supply chain keeps pace.

Salesforce must factor prominently in these security plans as both a crucial CRM system, and as an environment that can be home to hundreds of different third-party elements.

While Salesforce has accountability for securing its own infra-structure, users are liable for the third-party components and content that enters the environment – an approach known as the shared responsibility model.

High-profile incidents like SolarWinds, Kaseya and Log4J have continued to dominate the headlines and raise awareness of supply chain risk. However, Salesforce is not yet part of this conversation. Get in touch with our team now to find out how WithSecure can help you to secure this critical attack path before it is discovered and exploited in a serious cyber-attack.

Who We Are

WithSecure™ 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 & response is 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™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure