PLUGGING THE GAPS IN SALESFORCE CLOUD SECURITY

F-Secure Whitepaper

F-Secure

INTRODUCTION

As cloud computing becomes the new normal for enterprise IT, threats to cloud platforms are growing in both volume and sophistication. And as the market-leading enterprise SaaS platform, Salesforce has become an attractive target for attackers.

Organizations that fail to protect their Salesforce clouds effectively face an increasing risk of data breaches, business disruption, financial loss and reputational damage – with no recourse to the cloud provider.

In this white paper, we give an overview of your responsibilities, outline the threats facing the platform and explain why F-Secure Cloud Protection for Salesforce is the strongest, simplest and least disruptive way of mitigating the risks to your organization.

> "Through 2022, at least 95% of cloud security failures will be the customer's fault." - Gartner.

UNDERSTANDING SHARED RESPONSIBILITY

One reason Salesforce has become such a fertile target for attackers is that many customers fail to understand the shared responsibility model they sign up to when engaging a particular cloud service or provider.

Securing the platform that underlies Salesforce – the data centers where it's hosted, the hardware, physical networks and storage, virtualization system, operating software, etc. – is part of Salesforce's responsibility. As such the company ensures it maintains a high level of security in these areas. This often leads users to presume that any data uploaded to that platform is similarly well-protected.

In fact, as the table below illustrates, irrespective of the type of cloud service deployed, customers always retain responsibility for securing at least three things:

- Content (i.e. all data uploaded to the platform);
- Devices accessing the platform;
- Accounts, identities and credentials of all authorized users.

In other words, you need to pay as much attention to protecting these aspects when you're using a largely hands-off SaaS platform like Salesforce as you would if you were deploying more hands-on flavors of cloud like PaaS, IaaS or on-prem (with each flavor respectively leaving your organization with increasingly more security responsibilities).

RESPONSIBILITY	SAAS	PAAS	IAAS	ON -PREM	
Information, content & data	🟦	🟦	🟦	🟦	**Responsibility always retained by customer**
Devices	🟦	🟦	🟦	🟦	
Accounts and identities	🟦	🟦	🟦	🟦	
Identity and directory infrastructure	⬜/🟦	⬜/🟦	🟦	🟦	**Responsibility varies by cloud service type**
Applications and runtime	⬜	⬜/🟦	🟦	🟦	
Network controls	⬜	⬜/🟦	🟦	🟦	
Operating system	⬜	⬜	🟦	🟦	
Virtualization	⬜	⬜	⬜	🟦	**Responsibility transfers to cloud provider**
Hardware	⬜	⬜	⬜	🟦	
Physical network and storage	⬜	⬜	⬜	🟦	
Data center	⬜	⬜	⬜	🟦	

⬜ Cloud provider responsibility   🟦 Customer responsibility

SECURITY RISKS AND THREATS IN SALESFORCE CLOUDS

Security researchers have seen an increased number of attacks that exploit inadequately secured Salesforce clouds to bypass wider system security. Below, we outline the most common threats facing organizations that use Salesforce Sales Cloud, Service Cloud and/or Experience Cloud.

Malware and ransomware

Malicious files and URLs can be uploaded to the platform via a community portal, Chatter, a web-based support request form, Web Chat conversation or attached to Email-to-Case or Email-to-Chatter messages. Since malware and ransomware stored in Salesforce could be accessed from unprotected or unmanaged user devices, they pose a significant security threat.

Zero-day exploits

Attackers can conduct fileless attacks using zero-day (previously unseen) exploits, typically by convincing end users to open either a ‘weaponized’ Office document, a specially crafted image file or a web link in Salesforce. Such exploits are often used in targeted attacks to gain control over an organization’s wider systems and can be extremely damaging and hard to detect.

Phishing

Web links (URLs) used for phishing attacks can be posted or shared in a community portal, Chatter messages/comments, Email-to-Case messages and Web Chat discussions. Traditional gateway or email security solutions will not block these attacks if malicious links are opened directly in Salesforce from unprotected or unmanaged user devices.

Unsolicited and inappropriate content

Without the right protections in place, Salesforce can be used to share spam and other unsolicited content that, for example, can break an organization’s compliance policies, hog system resources and even place them in legal jeopardy. Such content may include (but is not limited to): potentially dangerous files, large media files, illegal/offensive material, or URLs (web links) that point to adserving, gambling, adult, spam, hacking or other inappropriate sites.

Supply chain attacks

Salesforce allows other cloud services and external systems to connect to the platform via SOAP or REST APIs. This can allow attackers to place malicious files and URLs on Salesforce via compromised third-party services and applications in the supply chain, over which your organization may have no control or oversight.

Advanced persistent threats

Cybercriminals are increasingly abusing Salesforce and other cloud services to conduct multi-stage ‘stepping stone’ attacks known as APTs (advanced persistent threats). For instance, Salesforce can be used as a C&C (command and control) server that stores and distributes payloads for malware or spyware already installed on a compromised device inside an organization’s network. Traditional network and gateway security solutions often fail to differentiate these malicious connections from legitimate ones.

Malicious insider threats

Not all Salesforce attacks come from outside the organization. Insider threats are also a significant concern. For example, disgruntled employees with access to Salesforce can spread harmful or disallowed content that could damage the company’s reputation, particularly if it’s sent to external users. Malicious insiders can also steal or tamper with Salesforce data, either for their own benefit or to damage the organization.

HOW F-SECURE HELPS SALESFORCE CUSTOMERS

All the threats outlined above can be prevented by deploying F-Secure Cloud Protection for Salesforce, a cloud-based security solution designed to complement the native security capabilities of Salesforce platforms (see table below).

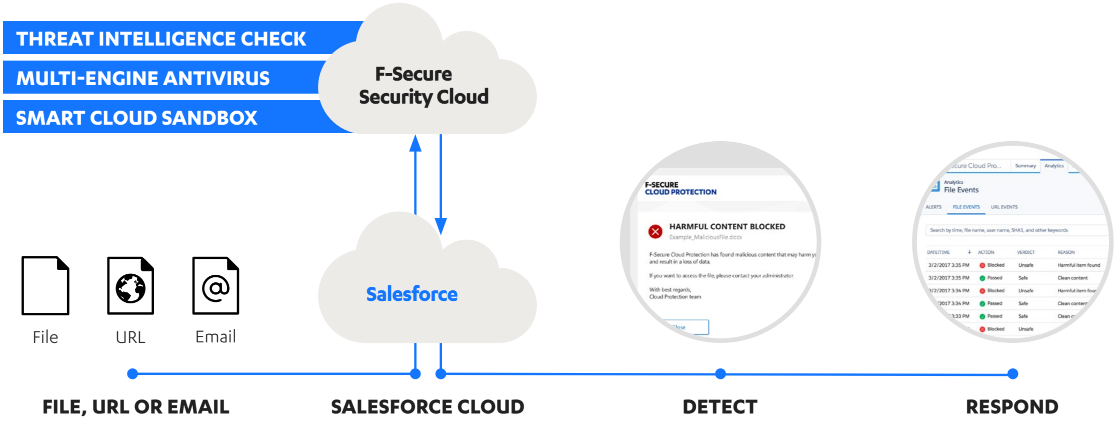
SALESFORCE CLOUD				
Application services				
Identity & Single Sign On	Password Policies	Two Factor Authentication	User Roles & Permissions	Field & Row Level Security
Network Services				
HTTPS Encryption	Penetration Testing	Advanced Threat Detection	Secure Firewalls	IP Login Restrictions
Infrastructure Services				
Secure Data Centers	Backup and Disaster Recovery	Real-Time Replication	Third Party Certifications	Customer Audits
+				
F-SECURE CLOUD PROTECTION				
Content: File and Link Protection				
Threat Intelligence Service	Multi-Engine Antivirus	Smart Cloud Sandboxing	Reporting and Auditing Service	Security Analytics Service

Multi-stage threat analysis

The solution provides dedicated security components that mitigate the risks posed by files and URLs uploaded by users.

Every time a user uploads or downloads a file or other content to one of the supported Salesforce clouds – including, but not limited to, Sales Cloud, Experience Cloud (previously Community Cloud) and Service Cloud – the system automatically scans it for threats (including malware, phishing links, inappropriate content and disallowed file types). This enables an organization to respond quickly and appropriately to any Salesforce-based attack.

If the system doesn't recognize a file, it is uploaded to the F-Secure Security Cloud where it is scanned for threats by multiple anti-malware engines. The system also uses advanced machine learning techniques to decide whether to send a file for further analysis to F-Secure's Smart Cloud Sandbox, where its behavior can be observed safely, facilitating detection of even zero-day and advanced threats.



HARMFUL CONTENT BLOCKED
Example_MaliciousFile.docx

F-Secure Cloud Protection has found malicious content that may harm y
and result in a loss of data.

If you want to access the file, please contact your administrator.

With best regards,
Cloud Protection team

DATE/TIME	ACTION	VERDICT	REASON
3/2/2017 3:35 PM	Blocked	Unsafe	Harmful item found
3/2/2017 3:35 PM	Passed	Safe	Clean content
3/2/2017 3:34 PM	Blocked	Unsafe	Harmful item four
2017 3:34 PM	Passed	Safe	Clean content
3:33 PM	Passed	Safe	Clean c
	Blocked	Unsafe	

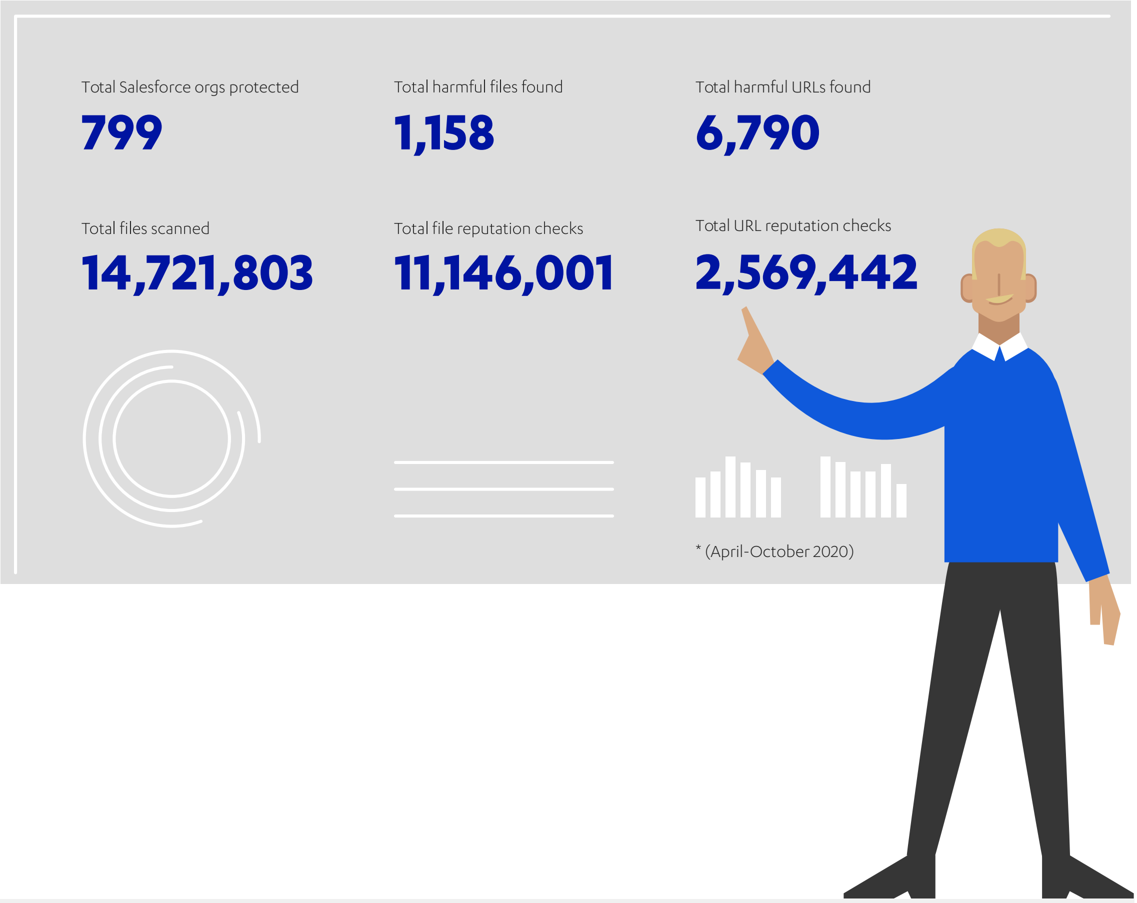
Easy to deploy, unobtrusive in operation

F-Secure Cloud Protection for Salesforce has been designed and developed in close cooperation with Salesforce in order to ensure maximum compatibility and reliability across the provider's various clouds. It supports the Professional, Enterprise, Unlimited and Developer editions of Salesforce.

Because the solution utilizes cloud-to-cloud architecture, there is no need to deploy or maintain middleware like proxies or implement additional network configurations. And the streamlined AppExchange deployment process makes set-up quick and easy.

Proven protection

Based on metrics collected over the last six months, F-Secure Cloud Protection has blocked thousands of threats in protected Salesforce organizations.



Total Salesforce orgs protected
799

Total harmful files found
1,158

Total harmful URLs found
6,790

Total files scanned
14,721,803

Total file reputation checks
11,146,001

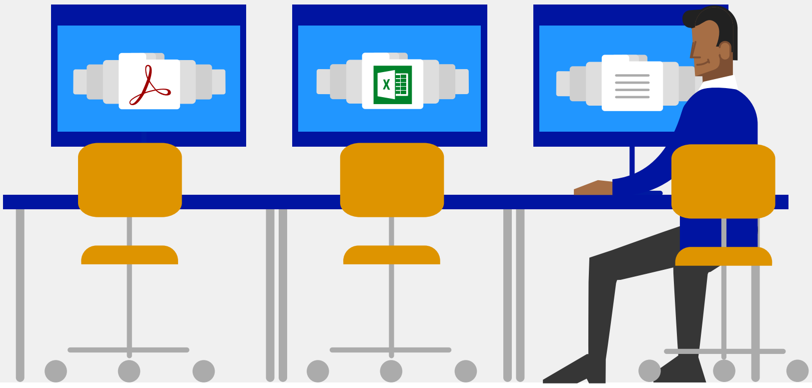
Total URL reputation checks
2,569,442

* (April-October 2020)

Total number of harmful files/urls found: 7,948
85% of malicious code was from url scans

Most common file types scanned:

Adobe PDFM | **Microsoft Excel** | **Text/Plain text files**



WANT TO KNOW MORE?

You can learn more about the product by clicking on the links below, or contact us and we will be happy to answer any of your questions.

- F-Secure Cloud Protection for Salesforce home page
- F-Secure Cloud Protection for Salesforce solution overview
- F-Secure Security Cloud whitepaper
- Salesforce Help – Platform Security FAQ
- Gartner’s Research - Assessing the Security Capabilities of Salesforce

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure