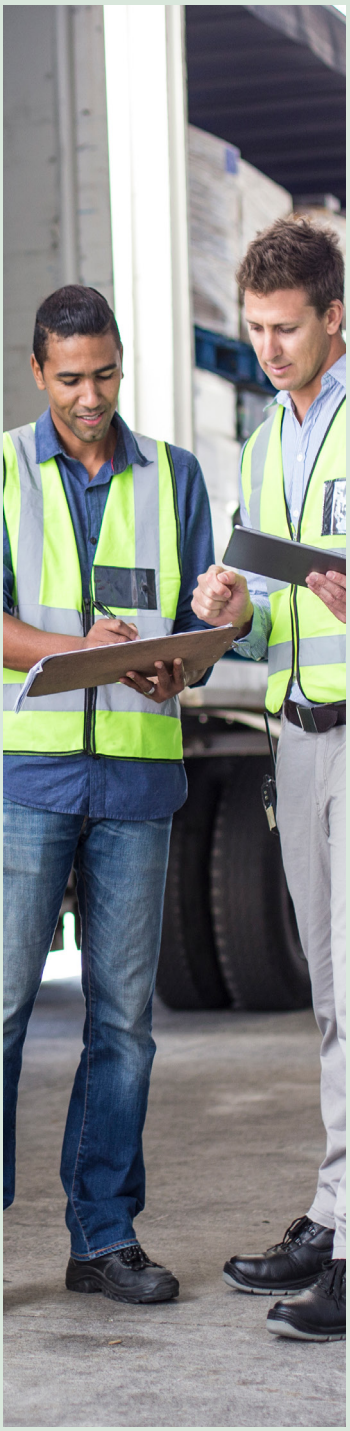
Infosys cobalt

WHITE PAPER



SALESFORCE SECURITY: GOING WELL BEYOND THE BASICS

Infosys®
Navigate your next

Is security essential for your Salesforce ecosystem?

In an increasingly digitized business environment, it is no surprise that cyberattacks have also risen exponentially. The Identity Theft Resource Center's (ITRC) research reveals that the number of data breaches was at an all-time high of 1862 in 2021, soaring 68% from the previous year[1]. Furthermore, experts are certain that the number and cost of cyberattacks will continue to grow. According to Cybersecurity Ventures, ransomware costs will hit a massive $265 Billion by 2031[2]. Quite naturally, cybersecurity comes under the spotlight as businesses scramble to plug vulnerabilities and fortify their operations else risk substantial damage to their business, brand and reputation.

The situation is no different in the Salesforce ecosystem. In fact, as the #1 ranked CRM provider by IDC[3], it becomes imperative to secure the ecosystem, given its market share and its position as a trustworthy platform[3]. In addition, there are several reasons why the Salesforce ecosystem must prioritize security.

To fully grasp the reasons, it is essential to trace the evolution of Salesforce the platform.

Salesforce Platform Architecture and Security

Starting as a multi-tenant SaaS, Salesforce gradually transformed itself into a platform on the public cloud today. The platform and the out-of-box applications come pre-built with security features. However, enterprises can get a pruned version of the platform at a lower cost and customize it. In addition, Salesforce made huge changes to how it manages its datacenters over the years. Initially, it managed its datacenters spread across various locations worldwide by itself. Now, most of the platform features are hosted on AWS public cloud as the company transitioned out of the non-core activity of datacenter management. But, again, data localization requirements in places like China and Europe posed a problem for Salesforce expansion. In response, the company launched Hyperforce[4], which allows the portability of services to other cloud computing service providers, like Alibaba, for instance.

Keeping this history as a backdrop, it's evident that security must be a priority to address these aspects:

1. Taking a broader view, in the age of accelerated digital transformation, effective cybersecurity is a critical success factor. Moreover, the Salesforce platform resides on a public cloud making it imperative to take adequate security measures. System integrators who implement and customize the platform can also introduce loopholes unwittingly.
2. A multi-tenant architecture's key appeal is its ability to serve a single software instance to multiple customers. At the same time, this aspect can cause security issues. However, Salesforce manages it by protecting customers' activities and data in partitioned storage, which can be accessed only using OrgID, a unique identifier.

The Salesforce way to better security

The Salesforce platform comes laden with numerous industry compliance certifications and attestations, satisfying requirements across many regions, such as ISO 27001, FedRAMP High, and CS Gold Mark[5]. That's not all. In addition, four more layers provide security –

- Out-of-the-box tools from Salesforce
- Add-on tools from Salesforce
- Custom solutions from the vendor ecosystem
- Support from the partner network

Out-of-the-box tools

Salesforce has rich pre-built capabilities to provide security at every layer. For instance, secured datacenters with strong backup and disaster recovery processes and real-time replication take care of the infrastructure layer, while built-in IP based login controls, real-time threat detection, HTTPS encryption for transactions boost network services security. Finally, strong identity and access management, password policies and multi-factor authentication ensure security at the application services level.

Add-on Tools

Salesforce has a host of add-on capabilities to enhance security. For instance, Shield, a trio of security tools, helps with event monitoring, data encryption at rest and field audit trail. In addition, the security center add-on delivers comprehensive insights on security, privacy and governance setup across Salesforce organizations. On the other hand, the privacy center manages data access insights and consent management.

For the developed custom solutions

Business requirements and practices are seldom satisfied with an "as-is" version of the Salesforce platform. System integrators resort to platform customization to bridge gaps in such cases. However, the downside of such customization is that it may introduce security loopholes.

Salesforce offers several ways to measure and enforce security. Security health check score is one such tool that compares the security settings against the baseline to provide a score and pointers to fix issues. In addition, there are features to promote secure programming practices, such as locker services for lightning component development, in any custom developed solutions. Lastly, comprehensive static code analysis and AppExchange security review measure the overall security health of the application and platform.

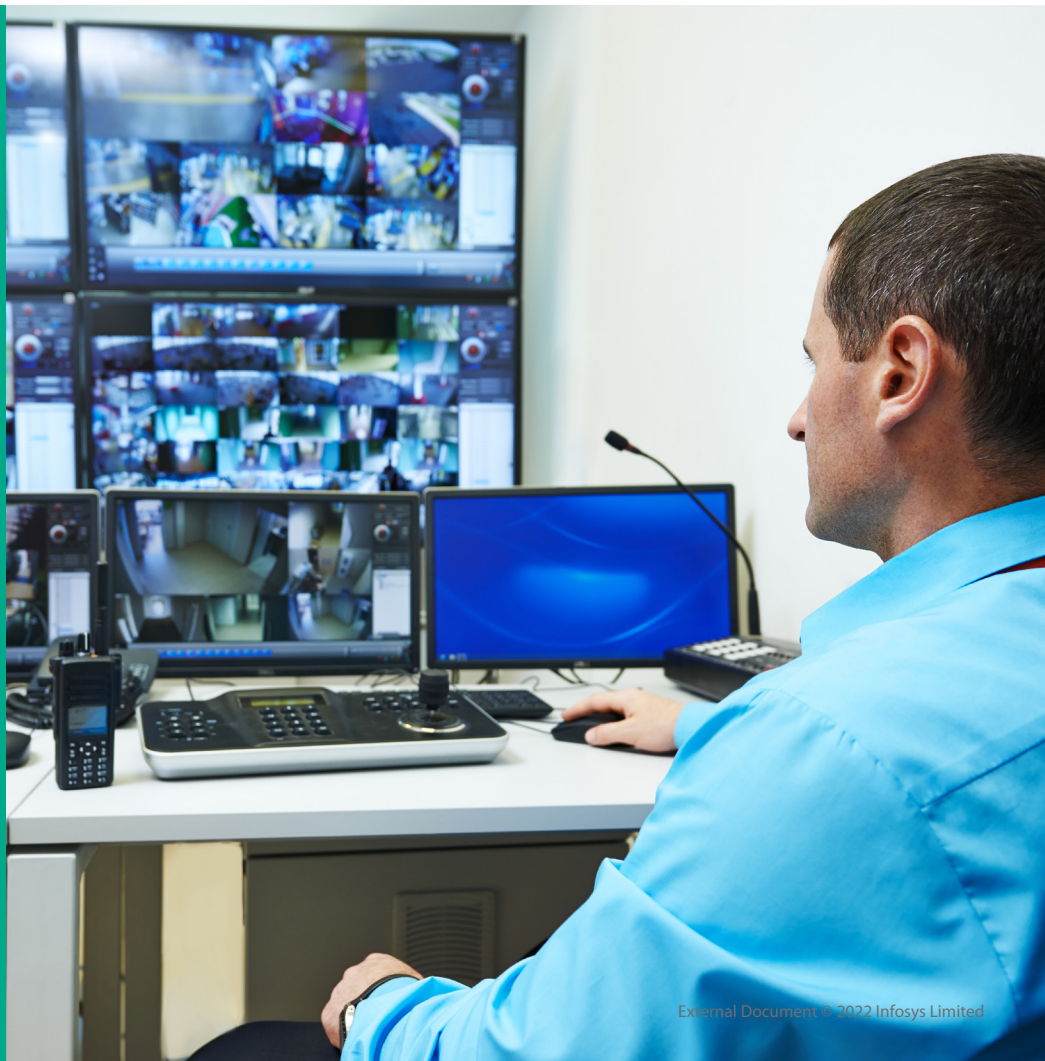
Support from Partner/ISV ecosystem

A key pillar supporting Salesforce is its partner ecosystem. Vendors have amplified Salesforce capabilities using the marketplace Salesforce AppExchange platform with their own solutions. In addition, various static code analysis tools, such as CheckMarx, SonarQube and PMD, have helped ensure secure, customized solutions.

Infosys' value-adding system integrator role

Thanks to its vast experience implementing Salesforce across several enterprises globally, Infosys has a solid knowledge of the intricacies of the Salesforce platform. As a result, the Infosys Salesforce practice follows a comprehensive set of tools, processes, and guidelines, as part of Infosys Cobalt, to ensure the security of the solutions. Some examples of the tools and processes we use in every engagement:

- Best Practices Enforcer, our version of a static code analysis tool, checks over twenty points to safeguard the solution's health.
- AgilePro, an AppExchange solution from Infosys, has a built-in code quality check.
- PMD is an open-source static code analyzer tool with enriched rule sets to spot common application code issues.
- Various best practices, secure coding guidelines and code review checklists documents.



Conclusion

As businesses globally embrace digitization, they inevitably become more exposed to cyberattacks. Unfortunately, the Salesforce ecosystem is no different and is susceptible to security vulnerabilities. But should security issues hinder users from benefiting from an enriched digital experience?

Salesforce's response is to load the platform with a rich set of security features and tools to ward off threats. In addition, the Salesforce ecosystem is suitably equipped to provide secure, customized solutions. At the same time, the role of seasoned and mature system integrators like Infosys cannot be underestimated. They bring in a wealth of knowledge and are armed with tools and best practices to ensure that security is always a priority. In addition, Infosys has helped several fortune 500 clients to deliver faster client value without compromising the overall system security. We have successfully achieved this with an optimal mix of tools, processes, and methodologies available in the Salesforce and partner ecosystem as well as Infosys' solution offerings.

It's safe to say that in a complex and interconnected digital world, a multi-pronged approach to security is the key to maintaining a secure environment.

About the Author

Kannan Narayanan

Is a seasoned Salesforce practitioner with 28 certifications, 12 accreditations and over ten years in the Salesforce ecosystem. Overall, he has spent more than 28 years in the IT industry. He is also a member of the Salesforce Partner Advisory Board (PAB) for platform solutions.

Kannan's primary expertise is providing advisory architectural services, delivery de-risking by bringing in design and arch best practices, and delivery automation via tools and accelerators. In addition, Kannan has delivered five AppExchange listings, right from ideation to solution development.

He also heads the CoE - Architecture practice and Technology Consulting Group within the current organization. Kannan is also a mentor volunteer at the NASSCOM Industry Mentoring Program (https://nasscom.in/) in cloud computing.

LinkedIn-> https://www.linkedin.com/in/kannan-narayanan-architect/

References

1 Data breaches break record in 2021 - CNET

2 MORE Alarming Cybersecurity Stats For 2021! (forbes.com)

3 Salesforce Ranked #1 in CRM Market Share for Eighth Consecutive Year - Salesforce News

4 Introducing Salesforce Hyperforce - Salesforce News

5 Certifications | Salesforce Compliance

For more information, contact askus@infosys.com

Infosys®
Navigate your next