Salesforce Security: SALESFORCE'S APPROACH TO SECURITY

Target Audience: Chief Information Security Officers (CISOs), Senior Vice Presidents (SVPs), VPs, Senior Architects of Security

Success Is Built on Trust. Trust Starts with Transparency

TRUST IS SALESFORCE'S #1 value, and security is the cornerstone of trust. Salesforce relies on four key values to drive everything it does, especially security. Those values are trust, customer success, innovation, and equality.

At Salesforce, our highest priorities are to create and maintain trust with customers and to guard the security of customer data. Salesforce communicates transparently with every customer and engages intelligently with its technology to ensure that information is safe and secure. Salesforce has worked hard to build a foundation of trust with customers and to protect that trust at all times.

Salesforce views cybersecurity through a layered approach based on technology, process, and people. Every employee understands that they are responsible for the security of customer data. Salesforce invests in security by ensuring that security is built into their products through the Salesforce Secure Development Lifecycle (SSDL) and by evangelizing secure behaviors throughout the entire Salesforce ecosystem of customers, partners, and communities.

By aligning internal development and security, Salesforce has transformed its security process, empowering engineering teams to own security through improved education, tooling, documentation, and automation.

Salesforce delivers awareness, education, and communications programs that address the human element of security. By informing and educating their employees, Salesforce helps keep Salesforce and customer data secure. By employing innovative behavioral campaigns, comprehensive training, and educational opportunities, Salesforce has ensured that employees' default mode is to think of security first.

How Salesforce Embodies These Values and Puts Them into Practice

SALESFORCE'S VISION is to be the most trusted cloud platform as a service (PaaS) and software as a service (SaaS) provider. Salesforce's security strategy revolves around this vision and is based on the values of maintaining the confidentiality, integrity, and availability of customer data.

Salesforce has made an executive commitment to continuous improvement of infrastructure and services security by committing to these three fundamentals:

- **Defense-in-depth**: Security is designed to apply multiple controls and technologies whenever possible, to limit the possibility of any single point of failure.
- **Investment:** Salesforce invests in personnel, tools, and technologies to manage, analyze, and improve security effectiveness.
- **Transparency:** Trust cannot be maintained without open communications regarding service performance and reliability. Salesforce strives to lead the industry in transparency and provides real-time information on performance and security issues via their trust website.

Salesforce has one security team across all the Salesforce clouds, and security common controls are enforced centrally across all Salesforce products. From ensuring that security is built into their products through the SSDL to monitoring ongoing threats, members of the Salesforce Security team work to keep Salesforce and their customers' data safe.

Salesforce's Framework for Cybersecurity Risk

TAKING A RISK-BASED approach is of paramount importance when building a solid foundational framework for world-class security. Salesforce uses a threefold approach to gauging its security posture: the US National Institute of Standards and Technology (NIST) cybersecurity framework (CSF), a risk management program, and the implementation of a common security controls framework. This threefold approach provides Salesforce with a defense-in-depth approach toward security.

EXECUTIVE SUMMARY

Salesforce has built a foundational framework to ensure a world-class level of cybersecurity. This security foundation is built on metrics-based implementation of the NIST CSF, Salesforce's risk management system, and the application of common security controls across all clouds and products.

One way to put this into context is to think about how a vehicle is equipped with gauges to provide useful information on the vehicle's condition. The driver has the speedometer, the fuel gauge, and the engine temperature gauge at their disposal. Just as each of these gauges gives feedback on the most important metrics a driver needs to know, the Salesforce multi-pronged approach provides multiple insights into its security status.

Salesforce Implements the NIST CSF

SALESFORCE IMPLEMENTS the NIST CSF as the fundamental maturity measure of its security program. The NIST CSF provides a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks. The framework provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.

Implementation of the NIST CSF begins with a self-assessment of five key pillars:

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The NIST CSF tiers are used by an organization to clarify how it views cybersecurity risk and to assess the maturity of its cybersecurity program. Salesforce leverages the NIST CSF to ensure that it has a prescriptive mechanism to track the progress of building a stronger security posture for the Salesforce products. Implementation of the NIST CSF enables Salesforce to measure every security effort and project by tying it back to the five pillars of NIST CSF, from identify to recover.

By assessing current and target NIST CSF scores, Salesforce can quantify and track the overall progress of strengthening its security posture over time. Salesforce also engages with third-party assessors to perform biannual assessments of its progress. This ensures that Salesforce has an independent and unbiased view of the progress of its security program. Salesforce then leverages these NIST CSF scores to inform and update its board of directors on the state of security at Salesforce, as well as the progress and return on investment that Salesforce is achieving on the security front.

Implementation of the NIST CSF provides Salesforce with a standardized metric and prescriptive mechanism to assess the overall maturity of the program and to set and achieve security improvement milestones on an ongoing basis.

Salesforce Implements Its Risk Management Program

SALESFORCE HAS a risk management program that measures its security posture from a risk perspective. Salesforce maps all of its security initiatives to the risk that they are meant to address. Some of the key areas of the program include risk assessments and reporting, including the risks posed by third-party products (3PP), product infrastructure, and the data supply chain. The risk management team engages with risk owners and senior leadership to drive risk treatment.

Salesforce Implements Common Security Controls

FINALLY, SALESFORCE HAS a set of common security controls to ensure parity in the implementation of security controls across various Salesforce clouds and assets. This allows for a uniform and harmonized control view.

Once the risk management team has identified potential threats in common security risk areas such as 3PP, product infrastructure, and the data supply chain, Salesforce implements a common set of security controls to mitigate these threats. These common controls are reinforced throughout SSDL tools and training, and are fully integrated with its development cycle.

Three Pillars of Salesforce Security Strategy

AT SALESFORCE, cybersecurity is built into development processes across the board. This means that security is neither an afterthought nor a roadblock to development but rather an integrated element of the development process. Salesforce uses three guiding principles to keep everyone on task when it comes to cybersecurity: nail the basics, engineering and business agility, and raise the security bar.

EXECUTIVE SUMMARY

Security is a cornerstone of trust, which is a core value at Salesforce, and is integrated into all levels of operations. By emphasizing cyber hygiene as a key pillar, Salesforce ensures cybersecurity across all processes and products. Cybersecurity tools and protocols are built in as part of the Salesforce agile development process, which ensures that security is never an afterthought but always a core driver. Raising the bar for security is a key tenet that fuels continuous security innovation at Salesforce.

Nail the Basics

THIS FIRST PILLAR of Salesforce's security strategy is: Nail the basics. This concept keeps the overall health of Salesforce's security posture at the top of its engineers' minds.

An example of how Salesforce implements this pillar is in its emphasis on vulnerability management and software bug remediation strategy. Today's businesses, including those that collaborate with Salesforce, run on a heterogeneous infrastructure composed of numerous components. Any critical system or component that is out of date represents a major security risk. Every organization needs to ensure that all components through which data flows are patched regularly and within predefined service-level agreements (SLAs). Organizations need to keep up with patching status according to the criticality of the vulnerability. Salesforce implements patching strategies that include automated scans of all environments for vulnerabilities, automated patch deployments, and alerting capabilities.

Another "basic" that Salesforce concentrates on is building a robust single threat vulnerability management and detection system. Salesforce works with key stakeholders to develop inventory management systems that maintain a system of record for the following: all operational devices for both enterprise and IT, all sensitive data sets, and all applications in the organization's data supply chain. This system should include the monitoring capabilities, configurations, and statuses of these devices, data sets, and applications.

Identity and access management is another focus area. By implementing strong identity and access management systems, including multi-factor authentication everywhere, Salesforce helps organizations strengthen their security postures and mitigate cyber attacks stemming from compromised user credentials. Investments in technologies that enable strong password creation and seamless password management are proven to deliver high returns in building strong cyber hygiene.

Engineering and Business Agility

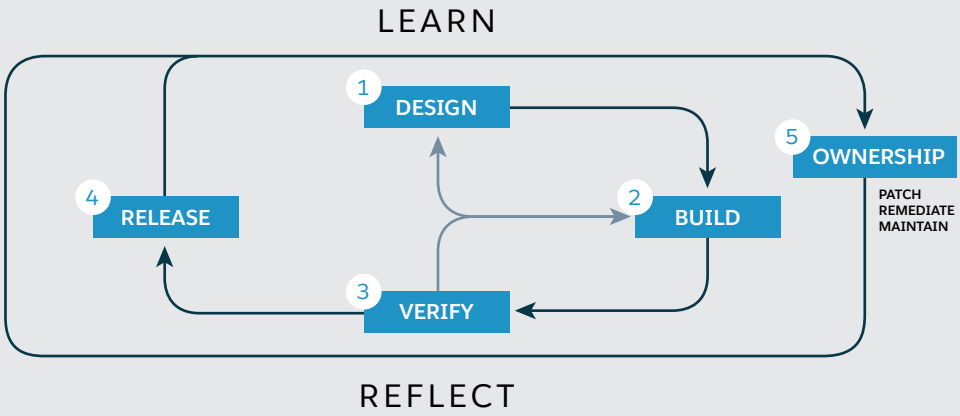
THE SECOND PILLAR of Salesforce security strategy is a key focus on agility. Business has an ever increasing need to go faster, and Salesforce's security strategy is to support innovation in a secure way. Salesforce has implemented a strategy to keep security from being an afterthought – or, even worse, a roadblock – to implementing a security mindset in every stage of development and involving security teams specifically to facilitate development work. Salesforce invests heavily in building scalable security models that support the pressures of business velocity and time to market in product development.

Salesforce has done this by implementing the SSDL model. The Salesforce Security team has implemented operations and technological optimizations that scale to support developers innovating secure code. This model moves security considerations to much earlier in the product development lifecycle to ensure that time to market and viability of the product are not thwarted because of security gaps or vulnerabilities.

Salesforce Secure Development Lifecycle

The seven stages of the SSDL are designed to sync up with agile methodology: learn, design, build, verify, release, own, and reflect. Security checkpoints are built in throughout the development cycle, as are easy ways for developers to partner with the security team throughout.

This process results in a dynamic and continuous application of security to all stages of development. This means that security concerns are handled across all Salesforce clouds and products in a consistent manner, one that does not impede time to market.



Raise the Security Bar

THE FINAL PILLAR of Salesforce's security strategy is a dedication to always raising the bar for security. The threat landscape is constantly changing. Today's defense does not protect us from the threats of tomorrow. Salesforce is a cloud security leader with a strong team of security professionals that continuously innovates to strengthen Salesforce's security posture and safeguard customer data while mitigating risk and deterring cybercrime. Some of the key areas where Salesforce innovates are PKI and Certificate Management, Platform integrity, and unified detection systems. Salesforce not only innovates but also contributes to open source projects that help the industry solve key security issues. An example of this is the JA3 project, a standard for creating SSL fingerprinting that can assist in producing higher fidelity identification of the encrypted communication between a specific client and its server.

Fostering a Culture of Security Awareness in the Salesforce Ecosystem

IF TRUST IS Salesforce's #1 value, then the means by which that value is expressed is by building a culture in which security is the responsibility of every single employee. The Salesforce Security Awareness team drives security education and assures that best practices are adopted across the Salesforce ecosystem, from employees to customers. These behavior engineers are charged with securing the human element of Salesforce – all the way from the product development stage to driving security control adoption with customers.

EXECUTIVE SUMMARY

Ongoing campaigns led by Salesforce's Security Awareness team ensure an ongoing stream of internal security training and education programs to keep cybersecurity and cyber hygiene at the top of employees' minds.

Many layers of Salesforce security work together to secure customer data. Organization-wide awareness and training campaigns are of paramount importance when creating a culture where cybersecurity is a universal responsibility. Throughout the employee lifecycle, Salesforce emphasizes how important it is to understand and assess the human role in the overall security posture of the organization.

While the Salesforce annual security training is required of every employee, contractor, and intern for compliance purposes, Salesforce goes beyond mere compliance. The Security Awareness team evangelizes secure behaviors by providing security awareness programs and technical education to employees and customers throughout the year. By requiring the active participation of all employees, Salesforce instills a security mindset in each and every one of them.

In order to fulfill this security promise, Salesforce provides programs, learning paths, and opportunities to create a security learning community for engineers and developers across products and clouds. Every developer has a training roadmap to complete, and managers can track progress across their teams. Furthermore, this training is not passive; it includes active participation and hands-on learning.

In addition to offering role-specific training opportunities and security campaigns on an ongoing basis, Salesforce constantly develops trainings using Trailhead and encourages developers to demonstrate a dedication to continuous learning by completing them. Salesforce also provides in-person seminars and webinars on security best practices on a regular basis.

Empowering Salesforce's Customers to Be Secure

PROTECTING DATA in the Salesforce ecosystem is a joint responsibility between Salesforce and their customers. Salesforce doesn't just leverage training and tools to ensure security best practices among its employees – it also provides them to other stakeholders, including their customers. The Salesforce Security team offers tools and educational resources to help customers configure and maintain secure Salesforce instances.

Protecting customers' data is paramount at Salesforce, which is why they work with customers to make them full partners in security. Salesforce empowers customers by providing proactive education on security controls and best practices that are critical to their data security. The security features in Salesforce enable customers to adapt their security models to their unique businesses and industries.

EXECUTIVE SUMMARY

Just as Salesforce employs internal training to ensure good cyber hygiene, so too does Salesforce partner with customers on proactive educational programs centered around security controls and best practices. These programs include a number of free and paid tools, applications, and sources of information to reinforce that security at Salesforce is a shared responsibility.

Security Health Check

Among the free security tools that Salesforce offers to its customers is Security Health Check. Health Check is a tool that shows the status of a customer's security settings in one convenient dashboard, and produces a score from 0-100 depending on how closely these settings align with Salesforce recommendations. A summary score shows how the customer organization measures against a default security baseline – the Salesforce baseline standard. The customer can also create and upload a customized baseline standard to measure against as well as enter weighting values to model their own risk. They can also view and rescore their historical reports as a way to measure improvement.

Salesforce Trust Site

The Trust.salesforce.com site is an important resource through which Salesforce communicates security issues to customers in a transparent manner. It is Salesforce ecosystem's home for real-time information on system performance and security. On the Trust site, you will find information about system status, security, and compliance issues.

Security Advisories

Salesforce is committed to setting the standard in SaaS as an effective partner in customer security. From time to time, it is important that Salesforce notifies customers with security advisories related to the Salesforce Platform or subsidiaries. Salesforce publishes security advisories on the Security Advisories page in the Security section of the Salesforce Trust site.

SCCS Compliance Site

The Security and Compliance Customer Success (SCCS) team is responsible for addressing customer questions and concerns related to security and compliance topics. The team represents Salesforce security controls to customer Chief Information Security Officers (CISOs) and compliance and audit organizations. The SCCS team hosts the Compliance site, where customers can access a comprehensive set of compliance certifications and attestations, as well as access most cloud and platform services.

Salesforce Authenticator

Salesforce Authenticator is a mobile application, developed by Salesforce, that customers can download to provide the "something you have" component of secure two-factor authentication. Salesforce Authenticator generates a time-based, one-time password, adding an extra layer of security to protect your Salesforce account and data. Version 3 includes the ability to intelligently save your trusted locations so that you can save time and stay secure when logging in to your accounts.

Salesforce Shield

Salesforce Shield is a trio of security tools that customers can purchase. These tools allow developers and admins to build trust, transparency, compliance, and governance right into business-critical apps. This product suite includes Platform Encryption, Event Monitoring, and Field Audit Trail.

Salesforce Security in Trailhead

Salesforce Trailhead provides developers and administrators with a guided learning path through the key features of Salesforce, using a set of interactive, online tutorials. There are a number of security-specific trails and trailmixes, each of which provide free training for Salesforce customers.

Journey to Build a Trusted Security Partnership

SALESFORCE USES MULTIPLE channels to build trusted security partnerships with all of its customers. Salesforce reaches out to CISO-level executives with a number of opportunities to meet, share feedback, and contribute to the direction that Salesforce cybersecurity will take. Salesforce also reaches out at the subject matter expert (SME) and developer levels. The Salesforce Security Awareness team proactively reaches out to customer communities who have a high amount of control over the security state of their Salesforce instance (administrators and developers) through conversations at Dreamforce, TrailheaDX, and World Tours. As well, Salesforce continually publishes Trailheads for self-learning and white papers like this one to communicate exactly what our security priorities and directions are.

EXECUTIVE SUMMARY

Salesforce has several means by which it builds partnerships with its customers. These include partnership events where CISO-level executives are invited to participate in Salesforce's security program development, events where SMEs are made available for consultation, and even self-directed learning opportunities such as Trailhead tutorials and white papers.

Building Trust Through Executive Channels

Salesforce and its customers understand that as the industry leverages the cloud in new ways, the potential impacts to customers' risk profiles increase. Business leaders understand the need to be proactive about ensuring that an appropriate security strategy is in place, and Salesforce understands the need to build a strong security partnership with its customers.

Salesforce CISO Forum

Salesforce hosts multiple CISOs from across the globe at its annual CISO Forum every year. This an invite-only day of information sharing and peer networking that brings together a community of C-level security experts to exchange concerns and best practices across the industry.

CISO Customer Advisory Board

The Salesforce CISO Customer Advisory Board (CAB) is an invited group of customers who are trusted influencers. Twice a year, Salesforce holds a security CAB meeting as a way to build thought leadership and relationships across the industry.

SME Channels

Salesforce maintains a force of security SMEs who are available when a customer has specific questions about a topic or wishes to do a deep dive. In this case, an SME session can be arranged to bring together customers and Salesforce security experts for a one-on-one on specific security topics.

Learning Channels

Salesforce maintains a suite of channels to inspire lifelong learning throughout your career. As part of Salesforce's dedication to building customer and employee skills, it offers Trailhead tutorials for users of varying skill levels. Trailhead tutorials are published on a regular basis, so there is always an opportunity to learn new skills.

- **Events:** Salesforce hosts a variety of educational events and content for administrators, developers, partners, and users. These events are key to ensuring that security controls are adopted throughout the Salesforce ecosystem. Salesforce events with a security customer presence include Salesforce World Tour events, Dreamforce, and TrailheaDX (US).
- **Trailhead: Trailhead** is Salesforce's signature online learning portal. Trailhead provides developers and administrators with a guided learning path on security topics, using a set of interactive, online tutorials.
- **Content:** Salesforce publishes blogs and whitepapers to keep partners and customers informed on the latest security innovations at Salesforce. Along with other useful information, security-related white papers can be found at the Salesforce **Security & Compliance Documentation Portal**.

STRONGER TOGETHER

Security is a partnership between Salesforce and its customers. Business leaders understand that as they look to leverage the cloud, the risk profiles of their companies can be impacted.

That's why Salesforce gives customers access to its security strategy of focusing on nailing the basics, engineering agility, and raising the bar, which Salesforce has built to protect its own infrastructure and products.

However, just as Salesforce expects its own employees to uphold security best practices, from blocking badge surfers to using the SSDL, Salesforce also expects its customers to leverage the recommended best practices and security tools made available to them. By leveraging these tools and best practices, Salesforce and its customers can collaborate to raise the security posture of all parties.

While Salesforce constantly invests in innovative solutions to strengthen its security profile, it truly believes security is the responsibility of the entire ecosystem. A strong security partnership with Salesforce means we can all be *stronger together!*