Deloitte.

Deloitte Cyber Salesforce Alliance

Embedding Cyber into our digital DNA

August 2022

Understanding cyber risks

A trusted Salesforce platform can help businesses **innovate fast** and **scale with confidence** in their digital transformation journey

Proliferation of Sensitive Data

Moving sensitive data gave businesses the biggest pause to enable consumer trust: 65% cited it among their top concerns about moving to the cloud.[1]

Addressing Cloud Security Head On

Challenges exists not in the security of the cloud itself, but in the policies, configurations, and technologies managed by the customer. Through 2022, 95% of cloud security failures will be the customer's fault.[1]

Compliance Challenges

Regulation and compliance can lead to challenges within industry verticals and across national and international boundaries: 42 percent of IT professionals do not know which compliance frameworks their company uses.[2]

Disruption of Business Operations

Data migration times, re-architecting to cloud environments, and third-party solutions, among others, can be disruptive to business operations.[1]

Salesforce products process sensitive information and support business critical processes and applications, making strong cybersecurity measures to safeguard sensitive data and boost digital trust even more important.

57% of companies have experienced a cyber incident in the past two years.[1]

60% of cyber leaders say that cybersecurity is underfunded in their organizations.[1]

90% of customers are more likely to trust an organization that gives them control over information collected.[2]

7.5% drop in stock values of surveyed publicly traded companies after a significant breach.[3]

[1] Navin Sing, et al.., *The Future of Cyber Survey,* Deloitte, 2019
[2] Salesforce Research, *Trends in Customer Trust*, Salesforce, 6 September 2018
[3] Kacy Zurkas, *Companies' Stock Value Dropped 7.5% after Data Breach*, Info security Magazine, 15 May 2019

Copyright © 2022 Deloitte Development LLC. All rights reserved.

With organizations focused on speed and agility to enable the business, embedding cyber and regulatory considerations early on can help accelerate the journey

Business adoption of Salesforce can be **accelerated** with a well-architected Salesforce implementation framework that has security and privacy considerations **embedded from design**

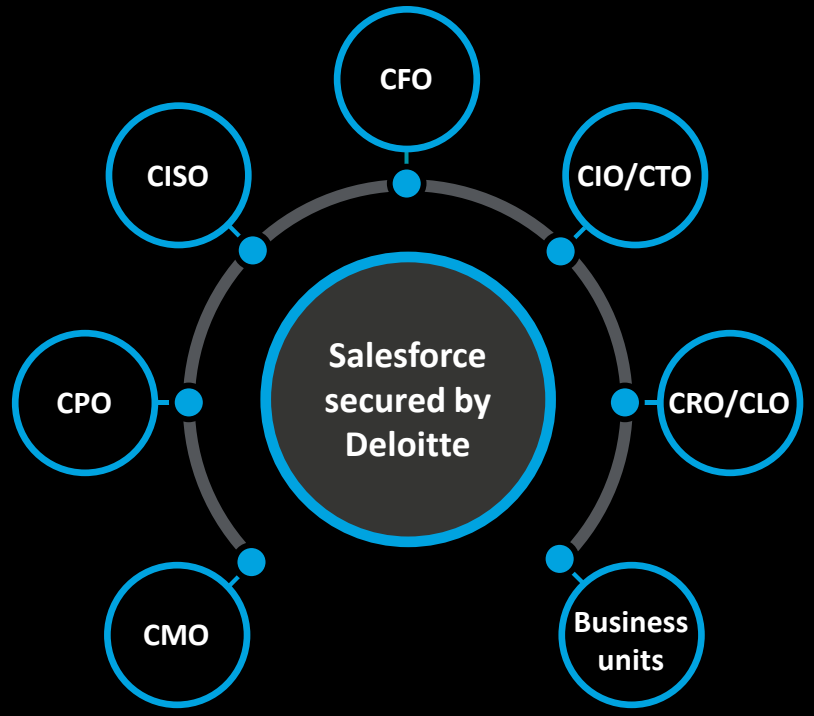
What questions are business leaders asking that can be addressed with a strong cybersecurity solution?

How do we drive top line **revenue growth**, reduce unplanned spend from breaches/cyber incidents and improve ROI ?

How do we reduce unnecessary friction from the client & customer journey while reducing **cyber and privacy risk**?

How do we create a **defensible position** for data and privacy regulations?

How do we enable **privacy at the center of our customer experiences** and provide more insightful services?



How do we **securely and safely** accelerate **digital** and drive operational improvements through technology innovation?

How do we determine our **risk management framework** is prepared for **cloud implementations** and **regulatory compliance obligations**?

How do we provide a unified client experience and **boost customer trust** in how we manage customer data?

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Navigating cyber risks early is critical in enabling trust

Deloitte Cyber helps organizations manage:

1. **Operational disruption**
2. **Customer trust**
3. **Reputational risk**
4. **Regulatory fines**
5. **Business performance**

Deloitte Cyber can help you embed cyber into your digital DNA to facilitate:

Trust at each touchpoint

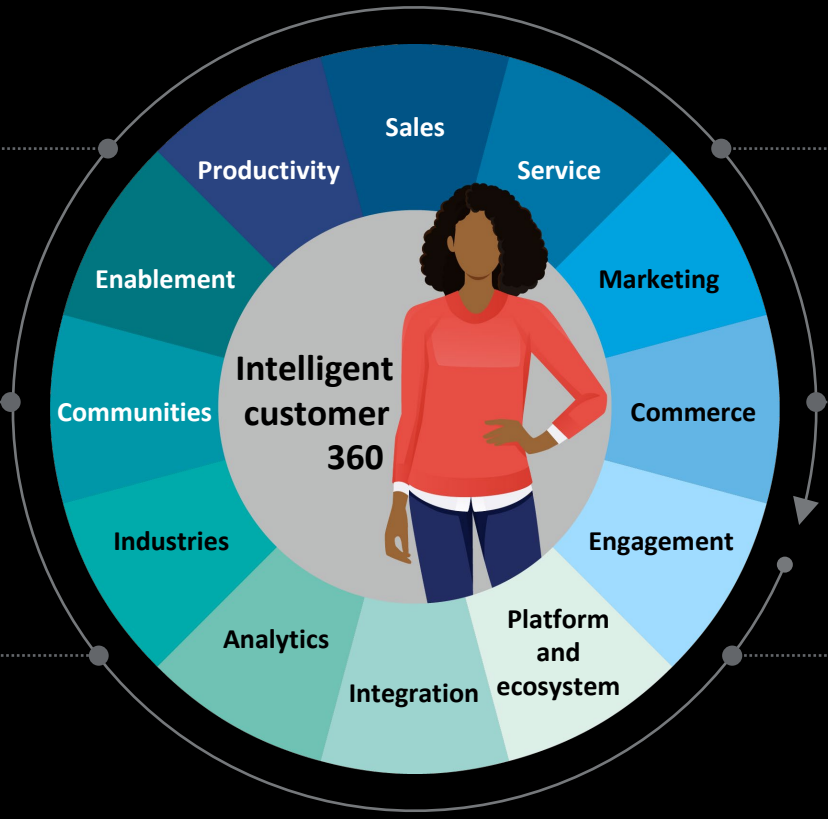
Demonstrating a competitive advantage by validating safety and security at each customer interaction.

Organizational alignment

Building connective tissue within your organization to embed cyber early in the digital transformation journey.

Intrinsic security

Enabling security to be embedded early and throughout many stage of the development lifecycle.



Improved customer experience

Engaging deeper with customers by empowering individuals to own their data and control how it can be used.

Improved cost optimization

Embedding basic security controls can help reduce the level of security incidents the organization will have to manage.

Security and resilience

Enabling security automation with stronger security monitoring can help improve cyber resiliency through orchestration.

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Security challenge – Trust platform used in untrusted ways

Salesforce products are offered as PaaS (platform as a service) or SaaS (software as a service) – each of which come with different levels of responsibility shared between the organization and the cloud service provider.

Responsibility	Salesforce PaaS	Salesforce SaaS
Identity and Access Management Controls	Customer	Customer
Data and Information Protection Controls	Customer	Customer
Application Security	Shared	Shared
Logging and Monitoring Controls	Shared	Shared
Platform Controls	Shared	Shared
Network Controls	Shared	Cloud Service Provider
Operating System Controls	Cloud Service Provider	Cloud Service Provider
Physical Host Controls	Cloud Service Provider	Cloud Service Provider
Physical Hosts and Network Controls (Hardware)	Cloud Service Provider	Cloud Service Provider

Customer Responsibility

Cloud Service Provider Responsibility

Shared Responsibility

Persistent mis-issue of the platform hampers security of Salesforce and clients

- Bypassing object and field-level access settings
- Using software that has known vulnerabilities (vulnerable third-party platforms)
- Bypassing sharing rules in Apex
- Storing sensitive data insecurely
- Using insecure TLS (Transport Layer Security)/SSL (Secure Sockets Layer) configurations
- Cross-site request forgery
- Insufficient escaping in Lightning components
- Loading JavaScript files from third-party endpoints
- SOQL (Salesforce Object Query Language) injection due to insecure database query construction

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Deloitte’s cyber services for Salesforce

Security measures go beyond out-of-the-box and “set it and forget it”. Our Cyber practice takes a **risk-based approach** to Salesforce implementations and provides **security, privacy offerings,** and **solutions** that can help carefully **secure Salesforce services** and **digital citizen identities**, so the business can focus on what matters and drive value by protecting business interests.

Security Assessments

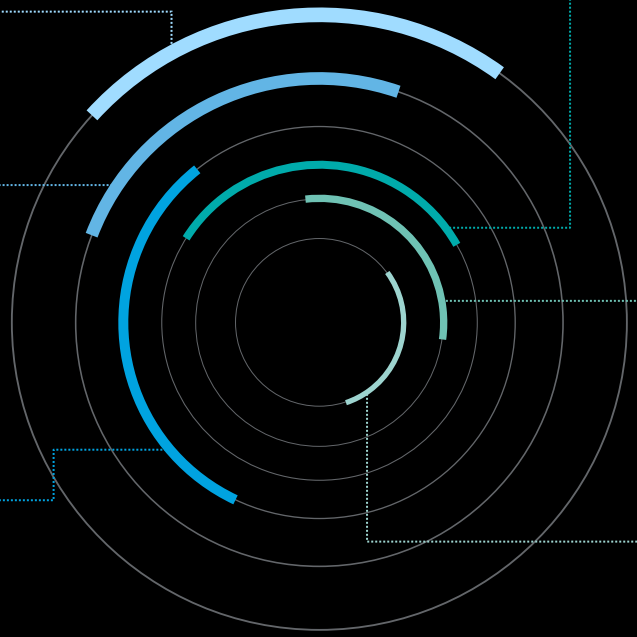
Deloitte performs a review of your Salesforce environments to determine the effectiveness of security controls and identify opportunities to further harden your Salesforce ecosystem

Core Platform Security

Deloitte provides assistance in identifying, designing, and implementing necessary security controls for a Salesforce implementation including role-based access control, secure code scanning, and Shield implementation

Privacy & Consent

Deloitte can help navigate data privacy and consent requirements according to the type and location of data collected, the capabilities to help meet regulatory requirements, and the related impacts on Salesforce solution design



Identity

Deloitte can help organizations protect customer and third-party identities both internally and externally, providing a secure experience throughout the security journey by implementing enterprise identity solutions such as single sign-on (SSO), multifactor authentication (MFA), and consumer identity access management (CIAM).

DevSecOps

Deloitte’s DevSecOps initiatives aim to break down silos between development teams, operational teams, and security to embed security throughout the product lifecycle and through our managed services capability, including threat modeling, streamlined application security testing, continuous security and compliance monitoring, and vulnerability remediation recommendations.

Advanced Salesforce Security

Deloitte can help you inspire customer confidence by enabling cyber measures that promote innovation, trust, and customer success by providing increased visibility to your Salesforce security posture and the ability to efficiently initiate investigations and responses to potential security events and compliance violations, while being able to manage elevated/privileged access to help prevent data breaches and unauthorized access to sensitive data.

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Managing cybersecurity challenges today to build digital trust for tomorrow

Deloitte Cyber differentiators for Salesforce allow for businesses to **take control** of securing their Salesforce solutions, **enabling and fostering trust** to boost sustainable and secure relationships with stakeholders.

Deloitte Cyber Differentiators for Salesforce

Core Salesforce Security

- Design security from the beginning to enable privacy and trust while meet business and compliance requirements
- Design access securely to prevent SOD risks and being exploited by misconfigurations
- Establish security testing to identify and remove security weaknesses to prevent malicious attacks
- Secure client data and digital authentication credentials to prevent data breaches, data and identity theft or manipulation

DevSecOps

- Identify possible threats across the platform and security measures to mitigate cyber risks
- Automate security testing to maintain fast flow and preserve trust of development practices
- Foster a culture of secure coding for development teams
- Enable fact-based security problem solving practices to improve resolution times

Advanced Salesforce Security

- Streamline login and authentication process to provide a secure experience for the customer during their journey
- Increase visibility to quickly initiate investigations and responses to potential security events and compliance violations
- Manage elevated/privileged access to prevent data breaches and unauthorized access to sensitive data

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Reach out to one or more of us

Niloo Bedrood
Lead
Alliance Partner
Deloitte & Touche LLP
nbedrood@deloitte.com

Chirag Patel
Advisory
Cyber Leader
Deloitte & Touche LLP
chirpatel@deloitte.com

Meer Hussain
Advisory
Cyber Leader
Deloitte & Touche LLP
mhussain@deloitte.com

Huy Vo
Advisory
Senior Manager
Deloitte & Touche LLP
huvo@deloitte.com

Andrew Haggen
Cyber Alliance
Sales Executive
Deloitte Services LP
ahaggen@deloitte.com

Kelli Wolfe
Cyber
Alliance Manager
Deloitte Services LP
kelwolfe@deloitte.com

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2022 Deloitte Development LLC. All rights reserved.