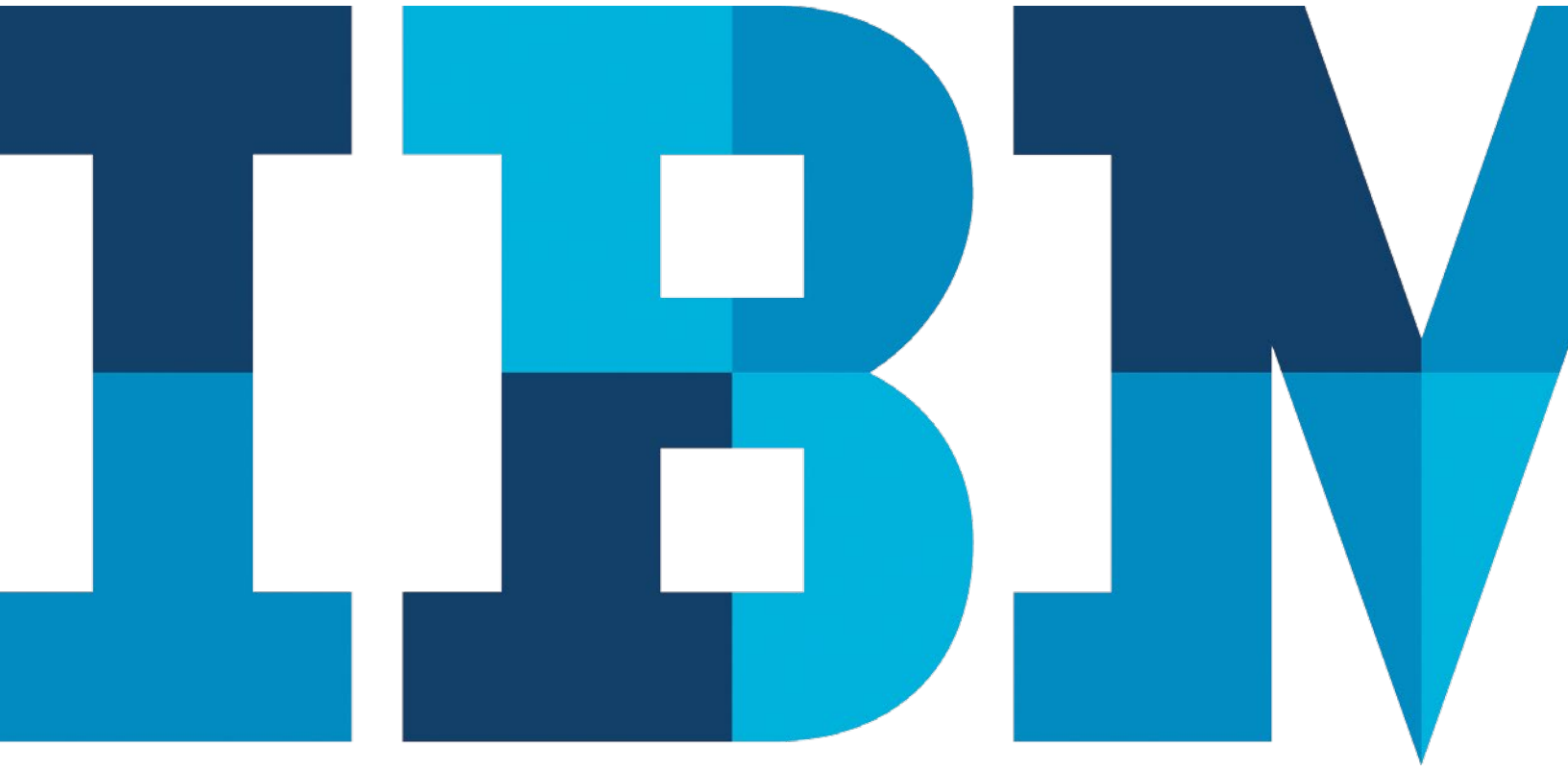
IBM
White Paper

Enhance the online user experience without jeopardizing sensitive data

Maintain strict security and privacy with IBM Tealeaf Customer Experience on Cloud



IBM

Introduction

Online transactions and interactions make up a large part of many organizations' businesses, so ignoring these channels can be a risky choice. Successful organizations are continuously searching for ways to optimize the online user experience to better serve customers and retain their competitive edge.

By capturing data about the user experience, organizations get behavior information that helps them understand what works and what doesn't work. Replaying the experiences can help organizations eliminate issues that might lead users to walk away from transactions, switch to another business or vent their frustrations through social media.

As organizations analyze more and more customer data, they face a fundamental challenge: maintaining strict data security and protecting user privacy throughout the life of the data. Collecting customer data creates opportunities for data loss or theft that might expose the organization to fraud, lawsuits, damaged client relationships and a tarnished reputation. Using cloud-based solutions that interact with private, personal customer data can amplify those concerns: Will sensitive user data escape secure on-premises environments and be transmitted to the cloud? And if it does, how will it remain fully protected?

IBM® Tealeaf® Customer Experience on Cloud (IBM Tealeaf CX on Cloud) is a software-as-a-service (SaaS) multi-tenant solution that answers these questions. It provides the advanced analytic capabilities organizations need to optimize the online experience while protecting user data, maintaining privacy and sustaining compliance. Tealeaf helps you avoid capturing sensitive user data and transmitting it to the cloud, but is also equipped with additional security capabilities to deal with a breakdown in these procedures.

IBM Tealeaf: A history of excellence

IBM Tealeaf has been a leader in the customer experience market for the past 15 years. It has earned a reputation for functionality and security, and is now applying that same expertise to the cloud space with Tealeaf CX on Cloud. Check out the impressive lineup of organizations that rely on Tealeaf to enhance and better understand their customer relationships:

- **7 of the top 10 online retailers**
- **8 of the top 10 bank holding companies**
- **9 of the 12 largest property and casualty insurance companies in North America**
- **50 percent of the top US airline carriers**
- **All major North American wireless providers**

Optimizing the online user experience while protecting sensitive customer data

Tealeaf CX on Cloud is designed to help organizations address usability issues with both websites and mobile sites, as well as maintain tight data security and user privacy. Organizations can capture and analyze each visitor interaction to provide clear visibility into the customer experience and users' behavior. Advanced reporting and dashboard capabilities within Tealeaf CX on Cloud enable organizations to quickly identify the root cause of issues and quantify the business impact of those issues while staying on top of long-term usage trends.

Tealeaf CX on Cloud data security and privacy protection capabilities are robust yet flexible—two must-have traits in constantly changing business environments. These capabilities enable organizations to capture only the data necessary for improving the customer experience and prevent any sensitive information from leaving the customer's browser (Figure 1). Even if sensitive data is inadvertently collected and sent to the cloud, Tealeaf CX on Cloud can apply additional privacy capabilities to protect that data within the secure IBM SoftLayer® infrastructure until it is permanently and irreversibly destroyed.

Because the IBM Tealeaf CX on Cloud solution can be configured to not collect or transmit sensitive data, your customers can feel confident they are engaging with a brand that secures their information, instead of questioning whether or not their personal information is safe.

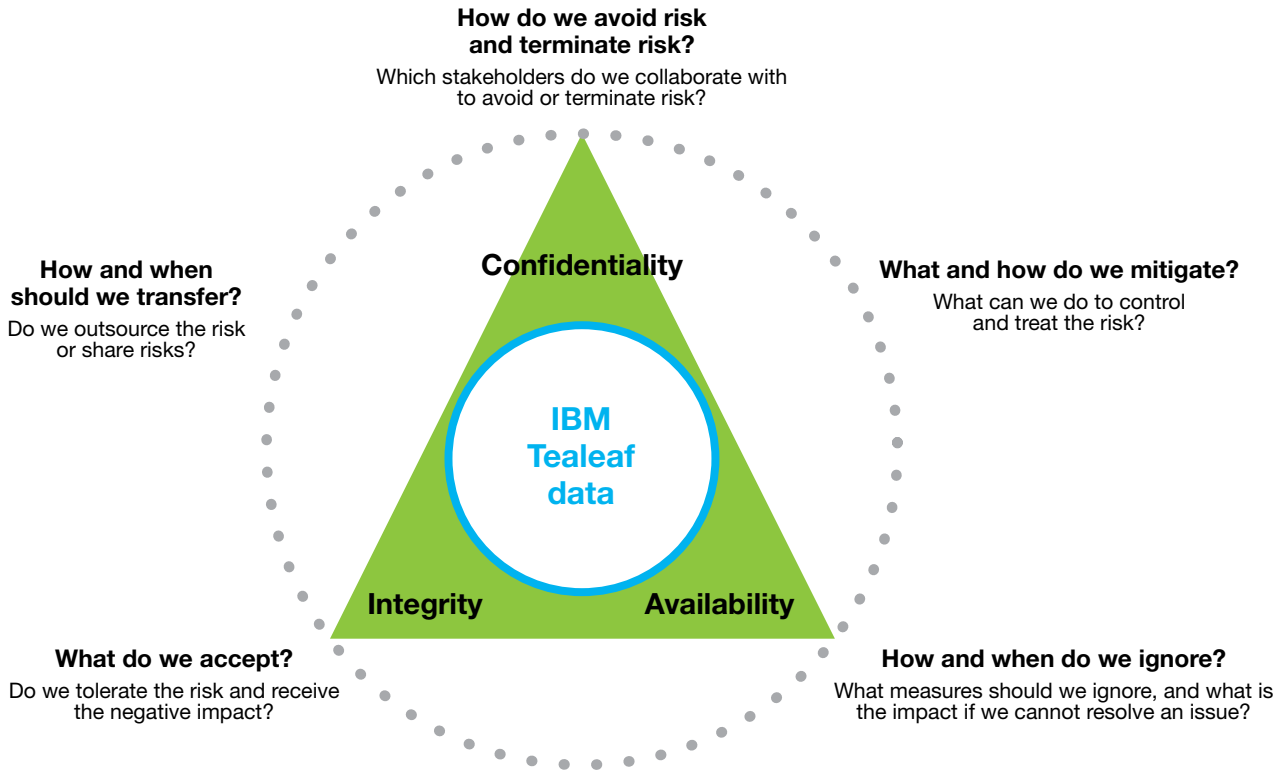


Figure 1. During the SaaS development process, Tealeaf CX on Cloud follows industry security guidelines including those governing data confidentiality, integrity and availability.

Maintaining tight security controls

Tealeaf CX on Cloud captures a wide range of data to help organizations optimize the online user experience: URLs, form fields, user login names, cookies, applications, client IP addresses and other raw data elements. Tealeaf CX on Cloud, however, is designed so that users can configure it to not capture personally identifiable information (PII) or sensitive personally identifiable information (SPII) such as user addresses, social security numbers, credit card numbers, health insurance account numbers or similar data as determined by an organization's security and risk controls.

The key lies in the software development kit (SDK) or UI capture method provided with Tealeaf CX on Cloud (Figure 2). When correctly configured, it enables organizations to automatically block data entered into certain form fields from being captured by the Tealeaf solution. If a social security number consisting of nine numerals and two dashes is blocked, it would undergo a one-to-one character replacement to completely remove the personal information, becoming "xxxxxxxxxx."

Tealeaf CX on Cloud also offers the ability to mask data, which is different than blocking it entirely. For example, an organization that wants to ensure end users adhere to password complexity

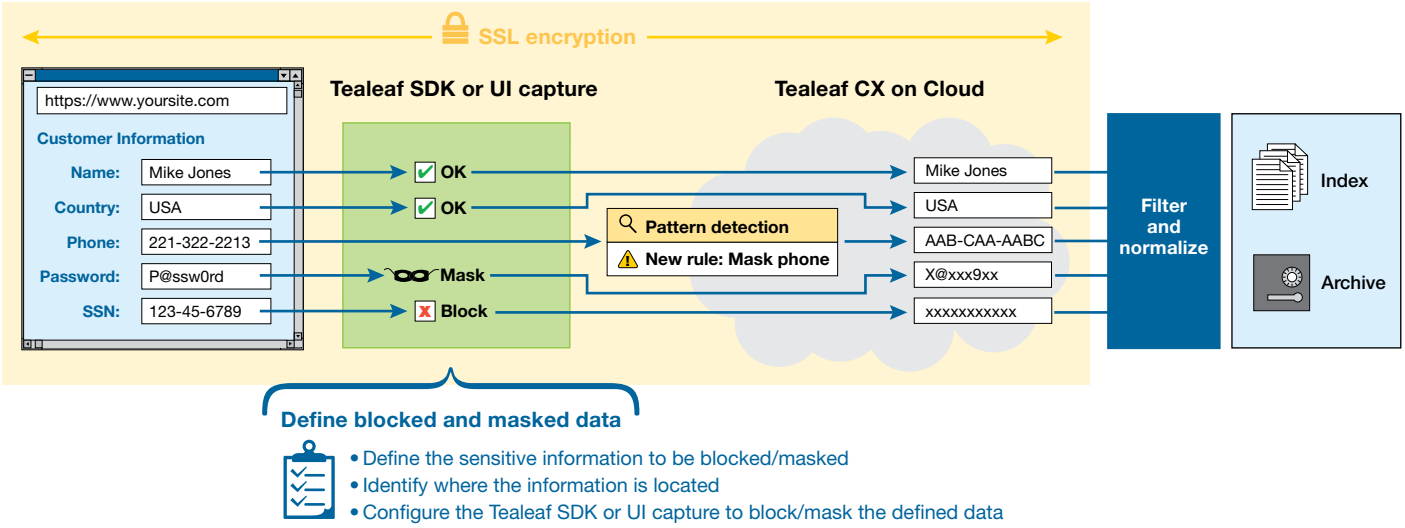


Figure 2. Defining which data should be masked or blocked and configuring the SDK or UI capture method accordingly is a critical element of the Tealeaf CX on Cloud solution. These guidelines and rules enable Tealeaf CX on Cloud to block or mask sensitive data before it is captured. If a privacy update is made that cannot be coded into the SDK, additional privacy capabilities can be applied in the cloud for an additional level of protection.

requirements but does not want to collect the actual password value can configure the SDK to mask the password field, replacing the password value of P@ssw0rd with X@xxx9xx.

Each organization must first define what data needs to be blocked or masked. Members of the organization's risk or security department review the appropriate corporate, industry and government regulations and identify data types that must not be captured or masked. Next, this team creates a requirements document that notes all pages of a site or app that contain data that should be blocked or masked. The IBM Tealeaf team then works with the organization's IT group to configure the Tealeaf SDK or UI capture, and to conduct any required testing.

All captured data remains secure with SSL encryption as it is transmitted from the customer's browser to Tealeaf CX on Cloud. When sensitive data is blocked or masked, it is done immediately at the browser level, and not analyzed by Tealeaf CX on Cloud. As a result, no one can see blocked or masked data when accessing Tealeaf session data. To minimize possible cases of unauthorized data access, Tealeaf CX on Cloud does not allow special access to sensitive data for any individual.

Applying privacy capabilities at the browser level via the UI SDK is ideal because sensitive data is blocked or encrypted before it reaches the cloud. However, there are circumstances where data collection rules change, putting sensitive information at risk of exposure until the SDK code can be updated. In these cases, Tealeaf CX on Cloud offers an important advantage: the solution can apply privacy capabilities at the cloud level for added layers of protection. For example, complex pattern detection enables organizations to identify and block any sensitive information that was not properly blocked during the capture process (for instance, if a new field was added without reconfiguring the SDK).

As data is received by Tealeaf CX on Cloud, it is streamed through a process that performs specific filtering and manipulation functions to normalize and protect the data. Once data is normalized, it is indexed, archived and made available for further access and analysis. (See Appendix A for additional FAQs about security topics.)

Reducing cloud risks with SoftLayer

IBM SoftLayer is a leader in the dedicated server, managed hosting and cloud-computing industry. Deployed on the SoftLayer cloud infrastructure—one of the highest-performing cloud infrastructures available—Tealeaf CX on Cloud benefits from additional security measures at the underlying infrastructure level that help protect user information.

IBM: Making deep security a top priority

At IBM, data privacy and security are not afterthoughts or considered simply part of "the cost of doing business." Managing and monitoring 15 billion security events every day for nearly 4,000 clients globally,[1] IBM maintains one of the largest single databases of known cybersecurity threats in the world. Emerging threats are continuously identified and analyzed, often before they are known to the world at large. IBM operates from a deep knowledge of privacy and security leadership, analyzing and using security database information to derive critical insights into the cyber threat landscape.

Physical and operational security

SoftLayer provides a wide range of physical security options and multiple, overlapping layers of protection customized to an organization's needs and interests. For example, the SoftLayer hosting location is hardened against physical intrusion, and server room access is limited to certified employees. Systems are fully accessible to administrative personnel but otherwise safely off-limits.

The SoftLayer infrastructure includes security measures down to the microchip level. It is certified for the ISO 27001 and Statement on Standards for Attestation Engagements No. 16 (SSAE 16) standards. ISO 27001 certification provides requirements for an information security management system (ISMS), a systematic approach to managing sensitive information by applying a risk management process that includes people, processes and IT systems. SSAE 16 is designed to update the US service organization standard to mirror and comply with the new ISAE 3402 reporting standard. SoftLayer offers additional hardware-assisted security options on demand, allowing organizations to customize security profiles as requirements change.

Network security

The innovative SoftLayer network architecture and commitment to using advanced hardware technologies dramatically minimize exposure to outside threats at the network level. The network integrates three distinct and redundant architectures into a multitiered network topology. Using SSL/HTTPS security, data is encrypted as it is captured and ingested into the SoftLayer cloud infrastructure. It is similarly encrypted when customers log into the application through HTTPS. Firewalls in the SoftLayer environment separate and protect the solution from the database to the application.

Protecting user data, promoting better online experiences

Tealeaf CX on Cloud provides unprecedented visibility into the online customer experience, allowing organizations to see how their websites, mobile sites and mobile applications work through the eyes of each individual user and enabling a proactive enhancement approach. Paired with industry-standard security capabilities, Tealeaf CX on Cloud helps deliver actionable insights while protecting sensitive data with industry-leading security technology. As a result, organizations can avoid costly data loss, fully comply with even the most rigorous regulations, protect brand reputation and give customers a better, more confident online experience.

IBM Tealeaf CX on Cloud has received certification to the ISO 27001 standard, an internationally recognized information security management standard that provides a framework for information security management best practices. Under ISO 27001, IBM Tealeaf CX on Cloud is required to continuously assess information security risks and implement appropriate controls and polices to address them. This certification reinforces IBM Tealeaf's commitment to keep our clients' information and data secure. View the ISO 27001 certification.

IBM Tealeaf CX on Cloud has also received certification to the EU-U.S Privacy Shield Framework, a framework designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. View the Privacy Shield Policy.

For more information

Learn more about IBM Tealeaf Customer Experience on Cloud: ibm.biz/tealeafcustomerexperience

Request a demo: ibm.biz/tealeafdemo

IBM
Route 100
Somers, NY 10589

Produced in the United States of America
November 2016

[1] "IBM Security Named a Leader in Gartner Magic Quadrant for Security Information and Event Management." July 29, 2015. **ibm.com**/press/us/en/pressrelease/47397.wss

Please Recycle

IMW14864-USEN-02