SRC CYBER SOLUTIONS LLP

The State of API Security For Companies Operating Businesses in China

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

srccybrsolutions.com

Digital transformation is accelerating for business operating in China at breakneck speeds. Over the last two decades Internet-first businesses have grown at an average of 300% year upon year! This massive pace of growth has been fueled by digital services being offered by various companies all talking to each other to share massive quantities of data. These interconnections have been fueled by a technology called APIs.

Whats are APIs - APIs stand for application programmable interfaces. APIs are used for connecting control and data transfer from one digital resource to another. APIs are now a primary source of data transfer between pieces of software. APIs are heavily used by enterprise organizations to transfer customer data to various third party services.

In this document we discuss the key findings, the trends and successful strategies that would help companies operating in China secure and comply with local laws related to data privacy and security, with a focus on APIs.

Key Highlights -

(1) The explosive growth in digital transformation projects in China has led to companies not paying enough attention to how they are sharing customer data with each other. These API interconnections run the risk of running orthogonal to the laws and regulations from China's government with respect to Privacy, Security and Data Localization.

(2) Chinese laws require special handling of data being transferred from one company to another , especially when it comes to sensitive financial, medical, user information.

(3) China is in the process of enacting laws that will restrict cross border data transfer, and will apply to all data exchanged via APIs.

Recommendations -

(1) Establish a comprehensive API security program based on Our Platform's Easy 4 step plan.

(2) Address China specific nuances by classifying data automatically, performing DLP on API data to identify violations in advance.

(3) Implement localization tracking and management for all data transfer via APIs to conform with China's legal guidelines.

Research

- By 2025 less than 50% of APIs are going to be managed. The tremendous growth in data interconnections via API is going to surpass the capabilities of existing tools to manage all these interconnections.

- By 2025 90% of organizations will be aware of only public facing API security, leaving huge gaps in 3rd party API communication which will cause major damages to companies from a regulatory fine perspective.

Details

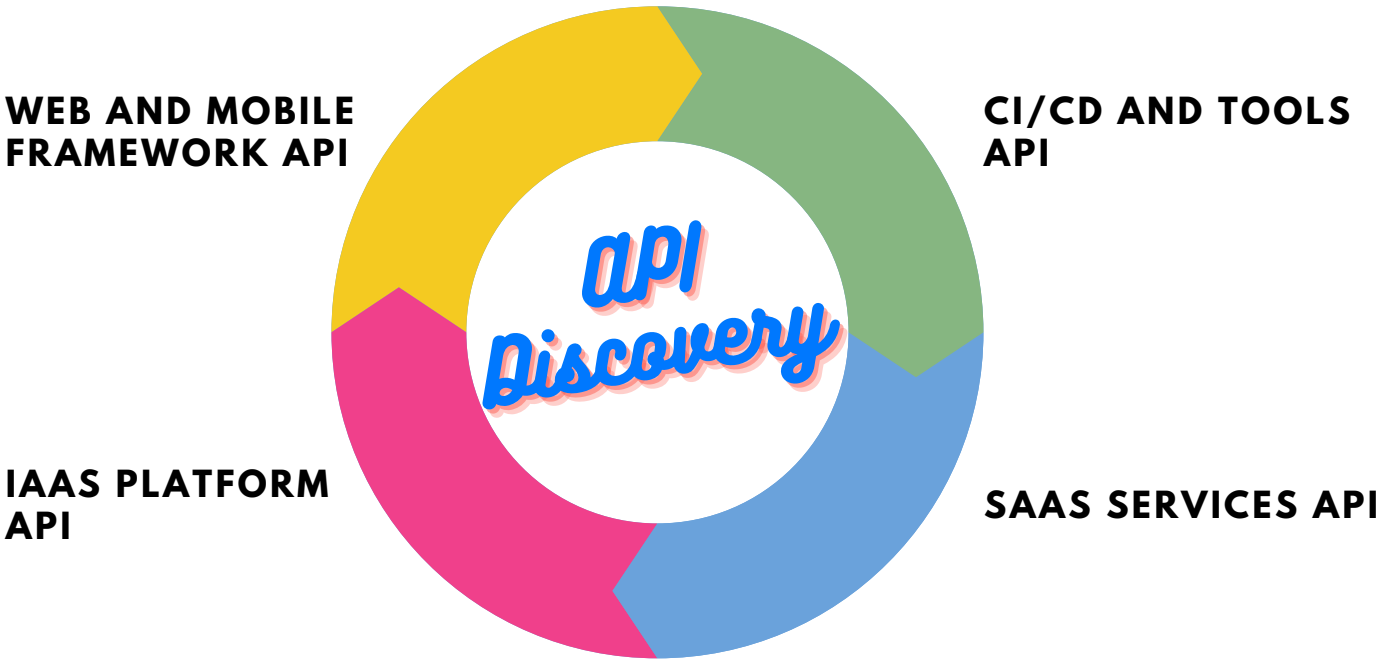
A well known publication, the 2021 IBM X-Force cloud security report found that two thirds of security incidents occurred due to insecure APIs. This is an amazingly large number. Knowing how to secure APIs, and more fundamentally cataloging, constantly monitoring and performing DLP (Data Loss Prevention) on the API traffic has become a leading concern for security thought leaders.

Additionally, China has introduced various restrictions and guidelines for different classes of data being transferred through APIs. These regulations also govern what type of data can cross geographical borders.

Types of APIs to Discover:

It is imperative to discover, catalog and monitor API calls within an organization. Given that there are many types of APIs, here are some examples that should fall within scope of our discussion.

- APIs built on web frameworks like Django, Laravel, Zend and more
- APIs built on top of IaaS vendors like AWS, GCP, Azure
- APIs built on top of CI/CD and deployment tools like Kubernetes, Kafka, Jenkins
- APIs built on top of SaaS services like Paypal, Shopify, Okta, Workday



It is important to understand the types of data that needs to be classified to comply with the law in China. The Data Security Law (DSL) puts in place guidelines like the PIPL - the Personal Information of the People's Republic Of China Law (PIPL) separates data in two buckets - personal information and user information. Both these need to be protected appropriately. Here are the controls being suggested as part of the laws:

- API security for transmission of data: This includes, authentication, authorization, desensitization, integrity protection, non repudiation, confidentiality protection and the validity of the duration of an API call.

- API Behavior control: This includes monitoring API calls to make sure that when transferring sensitive data if the behavior of the API deviates significantly from expected usage.

- API auditing and logging: This includes the capability to be able to audit the data being transferred during an API call and the ability to log any non standard events.

In order to be successful at implementing controls one needs to also follow some best practices that help with the classification of data into the following:

- Classify data as ordinary, personal, core and important. This can be a laborious process when performed manually, it is recommended ti use a automated solution that can help reduce the burden.

- Implement mechanisms to understand if the type of data passed through APIs violates any of the above classification standards, and stop the transmission of said data in flight.

Validation Phase: The portions of the validation phase which have to be accounted for in terms of the digital supply chain are listed below.

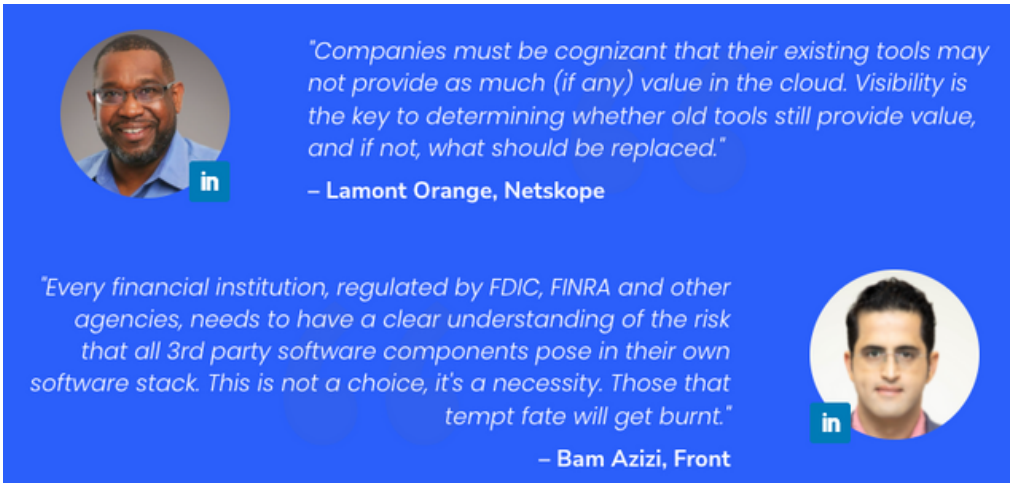
4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.
Actionable Insight - An automated system that tracks any changes in the risk posture of the software product accessing and processing sensitive information needs to be in place. The system should track changes in code libraries, associated vulnerabilities and risks. Highlighting the change in risk over a period of time is required.

4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.
Actionable Insight - An automated system that creates a catalog of all 3rd party and internal code libraries, used to compose the software as well as all the external and internal API calls needs to be in place.

4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.
Actionable Insight - An automated system should collect metadata about the software processing sensitive information, including but not limited to: Product owner, purpose of product, revenue from product, security and network posture fo the product.

4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.
Actionable Insight - An automated system should highlight and send alerts over email or any other mechanism to team members when the product or multiple products violate security policies for the the handling of sensitive information. As an example, software products that contain vulnerable components and API calls that can lead to the leak of sensitive data need to be highlighted.

4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.
Actionable Insight - An automated system that allows for comparison between products related to number of security issues, number of vulnerable components is required. The system needs to be automated without the need for human intervention to allow for accurate and unalterable statistics.



Ancillary Note - Managing risk for these API data transfer components is a very important part of the security and compliance processes in any enterprise. The challenges here though make it very difficult to make sure that the security and compliance teams can provide (1) sufficient coverage (2) sufficient reliability and (3) accuracy. The challenges stem from the fact that many development teams use 3rd party software in isolation from the security and compliance organizations. This is not for the lack of trying though. It is primarily the result of how organizational silos are built. The incentives for development teams are usually lined up with the need to ship better products, faster, with less bugs and more functionality. The chasm which exists between development and security and compliance is one of the primary reasons why we see that security and compliance organizations always find out later about which vendors and services are actually posing a risk to the business's revenue stream.

For more information please feel free to connect with SRC Cyber Solutions at sales@srccybersolutions.com .

Who Will Benefit

01

Sales and Revenue Generation Teams

Riscosity helps increase the bottom-line for companies. Lowering deal close times as well as allowing customers to do more with less – maintaining small governance, risk and compliance teams yet being able to respond faster and more completely to potential due diligence questions from buyers propels sales momentum.

02

C Level Execs and Company Boards

Riscosity provides effective and clear reporting that enables executives to understand the risk posture for the company and take appropriate recommended actions in line with fiduciary responsibilities.

03

CIO's Organization, Governance, Legal and Compliance Teams

Riscosity correlates the vendors and data being exchanged with various compliance standards. This helps CIOs present an accurate picture of the organization to the board. GRC teams can cut down compliance effort by 40% using auto cataloging of vendors and compliance mapping. General Counsels can get much more accurate information in real time, and hence can evaluate liability to the company appropriately.

Value for Multiple Groups

04

CISO and Security Teams

Riscosity accelerates security reviews and helps maintain control over the security posture of the organization. Gain total, and reliable (with low false positives) coverage when analyzing and cataloging all 3rd party interactions. Automated services, with intelligent policies cut down effort needed for security teams to act quickly and generate, audit reports .

05

Development and Ops Teams

Riscosity helps Development teams identify opportunities to improve 3rd party integration points in the native codebase. With automated failover switching (to secondary services) if the primary 3rd party service provider fails, ops teams can rest easy knowing that they will not have to perform middle of the night, manual configuration changes in production environments.

Financial Industry Risk Management Use Cases

FFIEC - FIL Aug 11 2021 [1]

Understand Risks
Inventory of Systems
MFA, Rate Limiting

23 NYCRR 500 [2,3]

Manage Risk
MFA, Rate Limiting

PCI DSS 2016v1.1 3rd Party Security Assurance[4]

Risk Assessment for 3rd Party, Nested providers - sec 3.3, 3.4
Monitor 3rd Party - sec 6.1
Network Diagrams

Specifically for APIs and 3rd Party Security

Quick Impact

Comply with Best Practices for Banking and Card Processing Industry

Free Up Cycles

Save significant manual effort on cataloging, tracking sensitive data flows

Real Time Reports

Get real time alerts if any changes occur in posture, one click report download

Technology Industry Compliance Use Cases

SOC2, Common Criteria 9.1 [1]	Manage Vendor Catalog Identify Inclusive or Carve Out - Provide Proof
FedRAMP StateRAMP [2]	Are all Cataloged Vendors ATO AC-2(g) - Logging, Monitoring and Throttling
NIST [3]	Manage API Labels, Version Log Everything Detect Data Leakage

Specifically for APIs and 3rd Party Security

GDPR, CPRA [4]	Data Processor Catalog Process Right to be Forgotten Identify Data Crossing EU boundaries to Data Processors
SLSA Level 4 [5]	Track and Report on Code and OS library Integrity
CISA [6]	Versioning, Input security, Encryption, Key and Secrets Management API Gateway Vendor Management

Healthcare Industry Security Use Cases

HHS.gov - API sec May 20 2021 [1]	Manage API Lifecycle Minimize Info Leakage Input Validation
NHS UK, CDS API Guidance 1.0.0 [2,3]	Bearer Token Management MFA, Rate Limiting
HL7 FHIR DevDays 2018 [4]	Manage API Labels, Version Log Everything Detect Data Leakage

Specifically for APIs and 3rd Party Security

ISMS, QMS	Vendor Catalog Vendor Risk Management
Get Visibility	Track and Report on Who are your 3rd Party Vendors and accessing your data
Interoperable	Exchange Data Securely and in Standard Formats