Manufacturing

Protecting IP in the Most Challenging Compliance Environments

The Paradox of Protecting IP in China

Regulatory compliance is a fact of life for most businesses. Applicable regulations for each organization differ depending on industry, geography and other factors. Manufacturers and other companies that have presence in China are facing a new "compliance" problem. In essence, they must protect their intellectual property (IP) and trade secrets—from China's vigorous efforts to protect IP.

Wait…what?

Well aware of its global reputation for stealing IP and trade secrets, in 2018 China took the offensive to combat that perception and created the State Administration for Market Regulation (SAMR). This organization merged the responsibilities of many existing organizations related to market controls. The act also created a new State Intellectual Property Office. As part of a 35-point national plan[1] to combat IP infringement, the SAMR "makes special emphasis to protect the intellectual property of foreign-invested enterprises."

A foreign invested enterprise (FIE) is a legal structure under which a foreign company can participate in another country's economy. It's a common way for companies to access resources and markets in China and other Asian countries, but FIEs must operate under strict regulations. In China, some of these regulations include technology transfer requirements, restrictions on data flow, and compulsions to establish Party Committee or other political groups within their organizations.[2] FIEs are now subject to SAMR plans.

Specifically related to IP, SAMR's national plan to combat IP infringement includes:[3]

Deeper governance and product supervision: This particularly focuses on consumer goods, online sales of counterfeit goods, false advertising and fraudulent transactions.

__Flying Cloud__ is the first company to secure the data itself. Flying Cloud CrowsNest is the only patented solution that integrates data surveillance techniques with a Zero Trust architecture to secure data of consequence.

[1] China's SAMR Releases National Plan to Combat Intellectual Property Infringement, The National Law Review, June 15, 2020

[2] New Chinese Regulations Improving the Investment Environment, WilmerHale, October 29, 2019

[3] China's SAMR Releases National Plan to Combat Intellectual Property Infringement, The National Law Review, June 15, 2020

Strengthening IP protection: This includes trademarks, patents, and copyrights.

Severely punishing infringement: Increases criminal IP enforcement.

Promoting the promulgation of IP laws and regulations: Focuses on promoting legislation related to trademarks, patents, and copyrights, as well as improving civil and administrative enforcement.

Promoting business capacity: Strengthening propaganda and "telling a good story about protecting intellectual property rights and combating infringement and counterfeiting."

Trademarks, patents, and copyrights as IP are viewed somewhat differently than trade secrets. A trade secret in China is defined[4] as technical, operational and commercial information that (1) is unknown to the public, (2) has commercial value, and (3) is subject to confidentiality measures taken by its owner. In practice, China's definition of a trade secret covers a wide range of commercially valuable confidential information, including formulas, business plans, and manufacturing techniques. There is no requirement to register protection with Chinese authorities for a company's trade secrets.

Data Awareness Becomes Business-Critical

With SAMR, in all cases of IP and trade secrets, any hint of IP "infringement" triggers severe crackdown. "Infringement" can even include flows of data shared between FIEs and Chinese supply chain partners in the normal course of business. Enforcement officials are empowered to conduct broad investigations into cases of alleged infringement, including conducting raids, making copies of relevant documentation, seizing or freezing relevant assets, and interviewing individuals under investigation. FIEs that lack data awareness run the real risk of infringement investigation and seizure of their IP.

This presents a different security challenge. In addition to detecting and preventing "normal" kinds of cyber attacks on IT networks, devices, and users, companies operating in China must be able to identify, track, and control all data related to IP and trade secrets. However, most organizations don't know:

Exactly what this data looks like: They know the types and formats of data they have, but they don't know what it looks like at the bit level.

How the data moves: Is data accessed through company-owned devices on the network? Via mobile device from outside the company? Does it move automatically between systems?

Who uses it: They know who has access privileges to data repositories, and maybe even specific assets. Authorized users need—and share—data for legitimate business purposes. But previously secured data is often seen, used, and then shared with people who never had authorization to access it in the first place.

[4] China IPR Toolkit, United States Patent and Trademark Office, May 2021

Where it goes: Data retrieved from a repository proliferates. It might be added to presentations, edited, updated, or processed in other ways. Even with DLP solutions in place, unstructured data can easily leave the organization unnoticed.

How it's used: Organizations don't have a way to see how the data is used or how it changes, so they can't determine if those uses are benign or represent security vulnerabilities.

Solution

Creating Data Awareness

When an American electronics company acquired a manufacturing company with production facilities in China, the acquiring company's IP became subject to SAMR regulations. Essentially, data belonging to each company had to remain completely segregated. Data and IP created in China could not overlap with or migrate to data or systems owned by the American company. The American company had to be able to prove that data did not cross a digital "no-fly" zone. If it did, Chinese authorities could "conduct raids, make copies of relevant documentation, and seize or freeze assets."[5]

Flying Cloud CrowsNest Data Surveillance for Zero Trust Data Security

Facing new requirements, a compressed schedule, and mandatory compliance, the American company had to quickly find a solution. They already had turned to Flying Cloud to test its CrowsNest data surveillance solution for data security projects aimed at protecting unstructured data and data in unique formats. Flying Cloud CrowsNest is the only patented solution that integrates data surveillance with a Zero Trust architecture. CrowsNest protects any data of consequence, not just regulated data. Whether IP, trade secrets, PII, financial, or IoT data—CrowsNest fingerprints data, monitors and analyzes usage, and defends data against threats in real time.

SAMR compliance requirement presented a new challenge. The enterprise was faced with implementing a system that could scan, monitor, and directly prevent actions. CrowsNest had to:

- Prevent data from overlapping
- Prevent unauthorized data migration
- Stop data exfiltration
- Ensure no unauthorized data transits across or between corporate applications and tools
- Prevent unauthorized data movement between on-premises repositories and Microsoft's Cloud SharePoint instance
- Review, hash and store SharePoint audit and access logs

[5] China IPR Toolkit, United States Patent and Trademark Office, May 2021

Know the Data

Flying Cloud collaborated with all customer teams chartered with protecting their IP. They established stringent network boundaries, including a secure DMZ network between California and Shanghai.

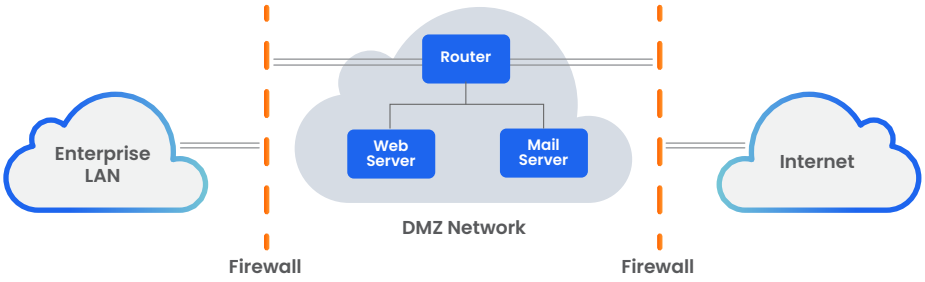

Fig. 1 Creating a No-Fly Zone to Maintain Data Separation

Next, the team used CrowsNest to scan all files and fingerprint the data. Fingerprints are a binary hash of all identified data. Working at the binary level, CrowsNest identifies where the data originates, as well as its purpose, level of sensitivity, movement and relationship to other data and users. CrowsNest catalogs data content and structures without modifying files in any way.

Monitor the Data

Next, CrowsNest conducts data surveillance—following and monitoring the data everywhere it goes. It analyzed decrypted, fingerprinted traffic on the company's network. This included scanning for unauthorized data movement between enterprise applications and tools, as well as scanning for unauthorized data movement between on-premises systems and SharePoint Cloud.

CrowsNest recognizes fingerprinted data at the bit level everywhere it appears on the network. It understands how data feeds into every area of the business—from enterprise applications and devices to factory floor systems. CrowsNest delivered advanced keyword analytics for content and attachments. The company's teams now know when new data is added to original data, when original data is modified, and when it's deleted. They know who uses the data, where the data is located, when it's used, and how it's used. Patented machine learning and automation quickly established a baseline of normal and acceptable data patterns.

Defend the Data

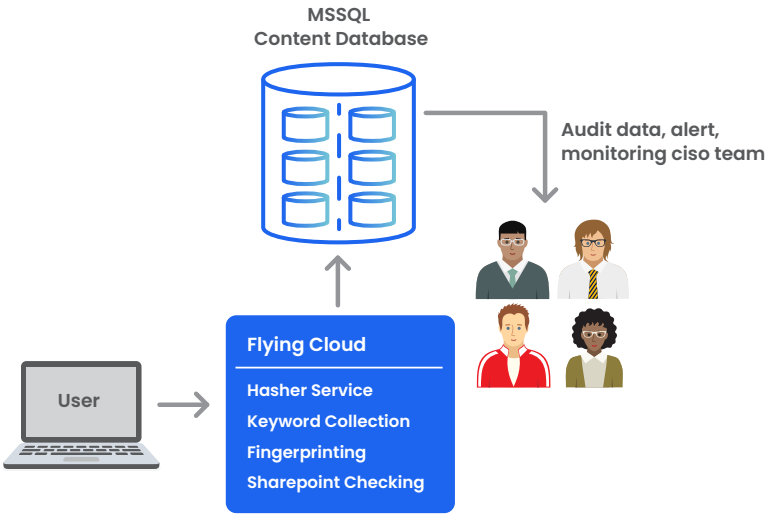

Fig. 2 CrowsNest IP Protection in Actionn

CrowsNest defends the company's data by identifying anomalies, breaches, and exfiltration in real time. Once data is known and a rolling baseline is established, CrowsNest enabled the company's teams to apply policies to data. In addition to access and usage policies, these included tunable data exfiltration parameters. Any attempt to exfiltrate data—whether on the network to an external location or any movement of data attempting to leave the DMZ—would trigger an alert to the team. Through API integration, CrowsNest delivers full digital forensics data to the customer's Splunk SIEM. The team also can trigger immediate action through Splunk to stop data from moving or leaving.

Patented machine learning techniques also isolate cyber threats such as ransomware, botnets, malware, Bitcoin, back doors, and command-and-control software. CrowsNest provides contextual analysis to connect the dots across attackers' tactics. It reconstructs events, extracts payloads, and provides play-by-play analysis of the activity. Teams will immediately know exactly what happened, where, and by whom—gaining a data "chain of custody" to support their response and remediation capabilities.

Benefits

Achieving Comprehensive Data Accountability

Collaboration between Flying Cloud and the company delivered new capabilities—as well as compliance benefits. The solution design enabled the company to also incorporate new proprietary applications and disparate repositories.

Compliance Challenge...Met

CrowsNest gives the company's team granular visibility into its data, usage, and activity through a detailed report that includes:

- Data on all fingerprinted files showing user, date, file name, file type, and file path
- Specific changes to files and updates on finger printing

- Audit logs showing who placed each file on SharePoint with all other required attributes exposed by Audit/Access logs from SharePoint
- Content analysis of files to gather insight on specific data types
- Data confidence match statistics and reduction of false positives
- Details of file monitoring and movement alarms, such as exfiltration and site-to-site movement, through PAN decrypted traffic flow

A comprehensive report was prepared for Chinese compliance reviewers and was met initially with…silence. Finally, the official responded saying that they'd never seen anyone comply before.

Easily Extend Data Accountability Everywhere

With international locations, the American company can now easily comply with the data standards of every country in which it has a presence. Data chain-of-custody reports enable the security team to easily verify data residency and prove that critical data remains within the country. Or in the case of an FIE environment, verify that no data overlaps or exfiltrates.

Any Business Model, Any Infrastructure

This American electronics company implemented CrowsNest in a hybrid on-premises/cloud environment. In the cloud, on premises, or in both environments, CrowsNest can be implemented per dataset, per site, or enterprise-wide. In organizations with multiple products, production models, and locations, CrowsNest can automatically surveil and defend data at any level and at any scale.

It also integrates easily into existing security infrastructure—NACs, firewalls, SIEMs, DLP solutions, IoT solutions, and cloud security—without impact on users or systems. One Flying Cloud customer has fingerprinted hundreds of petabytes of data, relying on CrowsNest to automatically scale and follow the data as it proliferates across the business.

Simplify Operations

Once a company knows what it's protecting and where it's going, it can make better decisions about how to protect it. For example, better insight and control over all data can allow organizations to reduce or eliminate the high costs associated with data encryption or the false positives associated with DLP. At the same time, CrowsNest enables far better protection against insider unauthorized access.

See Data in an Entirely New Way

Compliance requirements have always had the goal of protecting data. But this is the first time that organizations can actually protect the data itself—not just the systems and devices surrounding it. See your organization's actual data as it is accessed, moved, and used. Flying Cloud customers choose CrowsNest data surveillance to protect data safety and integrity across large ecosystems, prevent data harvesting, and accelerate threat response.

What next?
Go to www.flyingcloudtechnology.com/demo