Hospitality

Protecting Data *and* the Customer Experience: Data Surveillance Changes the Game for the Hospitality Industry

Customers—and Their Data—Are the Business

In the hospitality industry, the customer ***is*** the business. When data breaches or cyber attacks affect hospitality companies, customers lose trust and the company loses business. Cyber threats not only target hospitality companies themselves, they specifically target their customers. In the past, hacking for customers' credit card numbers was the goal. However, fraudsters and cyber criminals have moved to hacking for far more lucrative personally identifiable information (PII). Names, addresses, social media usernames, and other data elements give fraudsters tools to easily obtain other credentials, infiltrate networks, and perpetrate fraud.

> ***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.*

Many household-name hotel and restaurant organizations have fallen victim to significant data breaches in the past few years. But the hospitality industry also encompasses property management companies, military bases, alternative lodging companies, casinos, resorts, airlines, cruise ships, airports—even the payment processors serving these companies. When any of these organizations loses guest records, those individuals now become targets. It can get even worse. One property management group lost 85.4GB of security audit logs, giving hackers unprecedented visibility into its entire security infrastructure.

In an industry already hurt by the pandemic and strong competition, protecting data now means securing more than just the infrastructure that stores and carries it. 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.

Data is at Risk Everywhere

A few years ago, free Wi-Fi service was an exciting addition to the guest experience. Today, it's an expected amenity, along with a wide range of "smart" features. Hotels with smart televisions allow guests to log in to their existing streaming services. Keyless entry, biometric check-in, and smartphone-powered services expand the amenity list. The more smart services connecting to networks, the greater the attack surface.

The hospitality industry also relies on a wide range of IP-based Internet of Things (IoT) devices, such as security cameras and smart building controls. These devices are often unmanaged and invisible to security teams because they lack the bandwidth or processing power to support security agents. Cyber attackers prey on weak IoT security to gain access to other connected systems. As a result, systems from property management software to revenue management, booking, and business intelligence (and their data) are at risk.

Social media data is another attractive cyber target. Hospitality organizations rely on social media and big data to gain more insight into their customers' preferences, promote their properties, and attract guests. The social media data they collect is valuable to hackers. So is loyalty data, which typically contains personal information about each guest and is stored for long periods of time. Many organizations also rely on DevOps or continuous integration and delivery (CI/CD) pipelines to automate loyalty programs, develop new features, and accelerate delivery. These are typically cloud-based workloads vulnerable to cyberattack from unsecured containers and weak cloud security practices.

Hospitality employees can be individually targeted through phishing and malware attacks. Bad actors work hard to convince accounts payable teams to approve fraudulent money transfers, gaining access to systems through stolen credentials. Third-party vendors are another avenue of attack. Hospitality organizations rely on a host of companies to operate, and many of these vendors have access to critical systems. Some of the largest security breaches have occurred through third-party access to systems.

Organizations Lack Data Awareness

In spite of millions of dollars of security measures spent to protect infrastructure, data itself is not secured. Most organizations don't know:

Exactly the data they have: They broadly know the categories of data they have, but they don't know which data is retained, which is used for multiple purposes, or how much is associated with each customer, transaction, or asset.

How the data is accessed: Is data being accessed through company-owned devices on the network? Via mobile device from outside the company? During normal business hours or other times? By whom?

Who uses it: They know who has access privileges to the repository. They don't know who actually uses the data after it is accessed.

Where it goes: Data retrieved from a repository proliferates. Authorized users need—and share—data for legitimate business purposes. But previously secured data is often seen, used, and shared by people who were never authorized to access it in the first place.

How it is used: It might be added to presentations, edited, updated, or processed in other ways. 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

No Longer Living with Data Unknowns

Organizations can no longer live with these unknowns. One hospitality organization decided to implement a Zero Trust posture to better protect systems and data. Although there are segmentation and security policy solutions available to implement Zero Trust for networks, devices, users, and applications, there have been no solutions for applying Zero Trust policies to data itself.

Flying Cloud CrowsNest Data Surveillance for Zero Trust Data Security

The hospitality organization chose Flying Cloud to help it create a Zero Trust environment for its data. 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 customer PII, financial, IP, legal, IoT, or compliance information—CrowsNest fingerprints data, monitors and analyzes usage, and defends data against threats in real time.

The hospitality organization has a premises-based infrastructure using network access controllers (NACs) to implement role- and device-based secure access for devices, as well as for employees, contractors and guests using the organization's wired and wireless networks. CrowsNest integrates with existing security infrastructure, functioning as the NAC's data "brain." However, CrowsNest can be implemented on premises, in the cloud, or both, and it also integrates with firewalls as well as SIEM, DLP, IoT, and cloud security solutions.

Know Your Data

CrowsNest began by fingerprinting the organization's customer, booking, and rewards data from the repositories where it resides. 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 then catalogs data content and structures without modifying files in any way.

Monitor Your Data

When data is accessed, CrowsNest conducts data surveillance—following and monitoring the data everywhere it goes. Patented machine learning and automation quickly establish a baseline of normal data patterns. By continually analyzing incoming data, data in motion, and data leaving the environment, CrowsNest continuously updates the rolling baseline.

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 model, such as loyalty programs, analytics, customer communications, financial and payment systems. It knows when new data is added to original data, when original data is modified, and when it's deleted. It knows who uses the data, where the data is located, when it's used, and how it's used.

Data usage patterns reveal cyber threats that are not detected by other security measures. CrowsNest can see applications and monitor their behavior to identify and alert you to attacks launched through users.

Defend Your Data

Once data is known and a rolling baseline is established, CrowsNest identifies anomalies, breaches, and exfiltration in real time via dashboard. Patented machine learning techniques isolate threats including ransomware, botnets, malware, Bitcoin, back doors, and command-and-control software.

In the NAC implementation, CrowsNest identifies that a specific user, on a specific device, is performing a specific function with specific data. If this activity is unlawful or unwarranted, CrowsNest sends the information to the NAC via the Flying Cloud API. The NAC then notifies network systems, such as routers, access points, or other hardware—instructing them to take the appropriate action. Actions can include kicking the user off network or isolating him on a quarantine network for further analysis.

CrowsNest also 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

The Business Impact: It's All Good

For the hospitality organization, data awareness has been eye-opening. For the first time, they can fully understand where their data goes, how it proliferates, and the actual risk associated with its movements. Data awareness is also empowering. It's enabling this hospitality organization to fulfill its goal of applying Zero Trust policy to critical data of consequence. As a result, the company will also achieve other significant business benefits.

Establish Data Accountability

Surveillance of incoming data, data in motion, and data exiting the network delivers granular visibility into all data. For example, here is data set XYZ. Person A has authorized access to the data set. But why did Person A share it with person B? How did it get in the hands of Vendor C?

Data accountability also enables a company to identify data on the network that isn't theirs. For example, suppose an employee checks their bank account and downloads data to their desktop system. That data is now on the company's network—is the company responsible for protecting it? Knowing exactly where data goes, who uses it, and how it's used enables a company to better protect the business.

Apply Data-Level Policy

For the first time, organizations can create, apply, and enforce policy on data at the bit level. Data itself is monitored and protected wherever it goes. Unlike DLP solutions, CrowsNest protects any data—not just regulated data in specific formats. And unlike DLP, CrowsNest protects at the binary level. Regex can be imported to CrowsNest, giving data-level visibility to data currently monitored by DLP systems.

Easily Ensure Compliance Everywhere

As an international organization, the hospitality company must comply with the data standards of every country in which it has a presence. The initial deployment of Flying Cloud CrowsNest and the NAC includes securing data across multiple international locations—each with its own data standard. A data chain of custody enables the security team to easily verify data residency and prove that critical data remains within the country.

Protect Data in Any Business Model

Each organization determines the consequences it faces if specific types of data are compromised. Will it lose customers? Will it lose market value? Will employees have personal consequences associated with a data breach? CrowsNest fits easily with any business model to secure the data that matters most in the way that works best for the business.

It integrates easily into existing security infrastructure—NACs, firewalls, SIEMs, DLP solutions, IoT solutions, and cloud security—without impact on users or systems. It can be implemented per dataset, per site, or enterprise-wide. For example, in a hotel organization with multiple product brands and pricing tiers, CrowsNest can automatically surveil and defend data at any level and at any scale. One hospitality 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.

The ability to see and send detailed anomaly data in real time can streamline incident response and reporting. CrowsNest is already enabling customers to greatly simplify compliance analysis and reporting, freeing team members for other projects.

See Data in an Entirely New Way

Cybersecurity measures 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 IP, track data, ensure data safety and integrity across large ecosystems, prevent data harvesting, and accelerate threat response.

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