Flying Cloud
CrowsNest™

DATA SHEET

Defending Data with Real-Time Contextual Analysis and Rolling Baselines

In spite of organizations' large investments in security solutions, data is still compromised. Data loss happens all too frequently. Bad actors still steal Intellectual Property (IP), Personally Identifiable Information (PII), and other sensitive information. Security for perimeter and host systems is necessary—but so is a focus on securing the data that those systems are supposed to protect.

Flying Cloud CrowsNest does just that.

The first real-time data defense solution, CrowsNest™ delivers real-time visibility into your organization's data movement, usage, and changes. CrowsNest analyzes incoming data, data in motion across your network, and data leaving your environment to identify and help prevent data tampering, loss, and exfiltration. It creates a rolling baseline of normal data patterns, so that anomalous usage, unprivileged access, and threat actors become immediately visible. When anomalies appear, CrowsNest delivers real-time data forensics and analytics. Your security defenders receive a data "chain of custody" that identifies exactly who, where, when, and how content was accessed, modified, or distributed.

CrowsNest data defense capabilities complement existing security measures. They enable you to protect data without adding security experts, relying on users to decide what is sensitive and what is not, or adding complexity to your existing security environment.

Flying Cloud CrowsNest Use Cases

- **Protect** intellectual property designs
- **Tracking** data access across thousands of IoT devices
- **Preventing** data and process information from exfiltration
- **Documenting** data usage for compliance establishing chain of custody
- **Ensuring** data safety across a large ecosystem and third parties
- **Prevent** employees from harvesting data prior to resignation
- **Accelerating** contextual breach analysis

CrowsNest in Action

CrowsNest begins by scrutinizing network traffic to detect threats. Content and data are instantly and continuously analyzed looking for theft by means of: known threats, zero-day malware, unusual usage patterns, and other attributes.

CrowsNest uses real-time monitoring, active machine learning, and automation to determine normal data patterns. It continuously monitors data as it is delivered, used, stored, or sent via the network. Full packet capture and data payload inspection capabilities discover advanced threats and detect malicious data exfiltration. CrowsNest also identifies and catalogs data content and structures, without modifying files in any way. Anomalies are reported and advanced machine learning capabilities continuously update a Rolling Baseline™ of normal activity for your organization.

Detecting Anomalous Activity with High Accuracy

A Rolling Baseline of normal activity enables CrowsNest to instantly identify out-of-the-ordinary data usage without manually generated policies or historical analysis.

Patented machine learning techniques isolate known threats, against your data like: malware, botnets, Bitcoin, back doors, and command-and-control software. Because the CrowsNest Rolling Baseline knows what is normal, any suspicious data behavior immediately triggers an alert. When clusters of suspicious activity occur, CrowsNest contextual analysis identifies possible connections to "connect the dots" across attackers' tactics. Security teams don't have to guess whether activity is normal or not—they know.

Accelerating Incident Response

CrowsNest alerts security teams and their SIEMs when data anomalies occur. Because anomalies are immediately obvious, security teams can be confident that an alert represents a genuine threat. Real-time data forensics and analysis are delivered as the data is moving, enabling teams to respond quickly and accurately.

Rolling Baseline Technology™

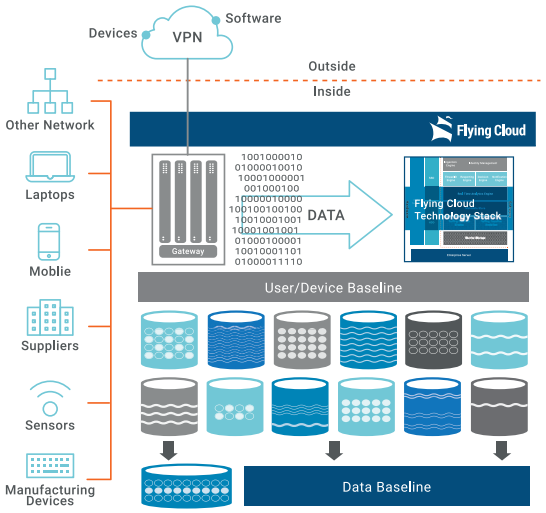

Figure 1: A copy of network traffic is delivered to CrowsNest for continuous monitoring and analysis.

Flying Cloud CrowsNest Business Process

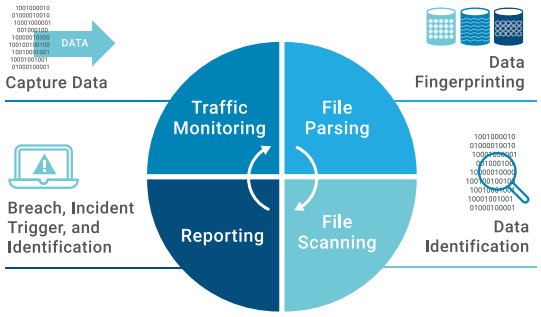

Figure 2: Flying Cloud CrowsNest performs continuous traffic monitoring, file parsing, file scanning, and reporting to build a Rolling Baseline of normal data, device, and user activity.

High-Accuracy Detection

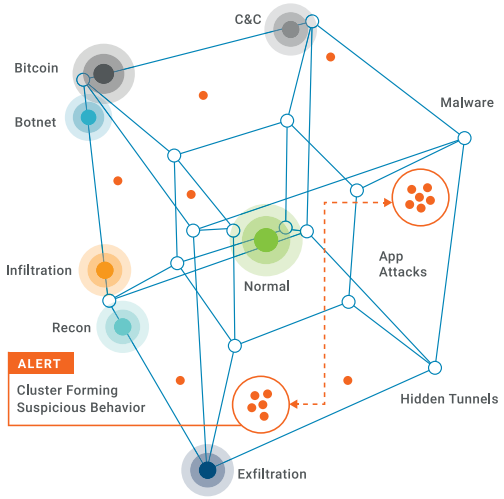

Figure 3: Machine learning and contextual analyses enable high confidence in alerts and virtually eliminate false positives.

Flying Cloud

CrowsNest Benefits

Detect—and Prevent—Breaches

By alerting you to unusual activities with data, CrowsNest enables you to detect suspicious activities as they are occurring. In addition to retaining historical information, CrowsNest enables you to replay all network traffic to discover and model breach patterns and prevent them from happening again.

Preempt Insider Data Exfiltration

With CrowsNest, you can monitor and ensure employee data policy compliance, because it documents normal data usage for employee groups and specific roles. Advanced machine learning and analytics quickly identify any anomalous activity that might indicate insider data theft. As employees move between projects, you can be sure that they only have access to data that's relevant to their current assignments. When employees leave the company, you can ensure that they are not abusing or exfiltrating data.

Achieve Fine-Grained Control over Data

Discover all data regardless of location, identify data creators and data consumers, list new files at creation, and detect exact and partial file matches. CrowsNest provides the power to know who, what, when, where, how, and even why data is used. With deep visibility into data, you can classify it to fine-tune encryption and DLP strategies.

Gain a Data Chain of Custody

CrowsNest provides a data "chain of custody" to support compliance, contractual, forensic, and legal requirements. You'll know where data resides on your network, as well as how, where, and by whom it was accessed across its entire lifecycle. Data tampering or possession by an unauthorized user is instantly reported.

Increase the Value of Existing Defenses

CrowsNest data defense complements existing perimeter and host-based security solutions. It can be deployed quickly—in hours, not weeks—without disrupting other solutions. Integrate CrowsNest with your SIEM or ticketing solutions through comprehensive CrowsNest APIs, and view results in your chosen management console.

CrowsNest Specifications

Capability	Specifications
Real-time Performance	• Threat ID • Notification • Reporting • Decision engine • Data ingestion
Data Tracking	• Incoming data • Data in motion • Data exiting the network • All files, including files that have been edited or changed
Scale	• Real-time • Petabyte + analytic capacity • On-demand elasticity
Flexible, Nondisruptive Implementation	• Implement per dataset • Implement per site • Implement enterprise-wide • Deploy without impact on users or existing infrastructure
Agentless Deployment	• On-premises VM • Public cloud • Private cloud
Integration	• TopMast™ open API
Compatibility	• ArcSight • Cisco • Juniper Networks • Palo Alto Networks • Splunk

Learn more about how CrowsNest from Flying Cloud Technology can protect your organization's data. Visit **flyingcloudtech.com**.

About Flying Cloud Technology

Flying Cloud Technology provides innovative data defense solutions that enable enterprises to protect IP, PII, and other essential or sensitive data. The company's CrowsNest platform uses advanced machine learning and big-data analysis, enabling customers to identify cyberthreats, prevent insider data exfiltration, refine security policy, and transform security effectiveness. Flying Cloud was founded in 2014. It is privately funded and headquartered in Polson, Montana.

Flying Cloud