Data Surveillance in the PLM Digital Thread

Companies' digital transformation journeys are increasingly encompassing product design and manufacturing. In complex Product Lifecycle Management (PLM) environments, the digital thread encompasses hundreds of devices, tools, and applications. It includes thousands of users and dozens of third-party partners. And it supports petabytes of data, with IP as the crown jewel.

PLM security measures have traditionally focused on protecting IP. But today, role and department-based access control methods are no longer enough. Securing the systems and devices that store, transport, and process IP is no longer enough. First, they don't protect the data itself at the binary level. And second, **IP data isn't even the first place attackers target.**

40%
Percentage of breaches executed through stolen credentials[2]

112% increase
Access brokers selling stolen access credentials in 2022 over 2021

4th highest
Ranking of manufacturing sector credentials for sale[3]

New Protection Priorities

It's faster, easier, and more efficient for attackers to gain a foothold in a network through social engineering and email compromise than to try and attack a PLM system head-on. Industrial espionage is still an attack motivator, but in 2023, the data most targeted by cyber attackers is data surrounding the IP itself—personal data and user credentials.[1] Why? Personal data is financially lucrative, and user credentials allow bad actors to gain undetected entrance and persistence in the network. Attackers mine personal data and user credentials from common communication tools used across the organization and in the PLM:

- Email
- Collaboration channels
- Productivity applications
- Planning documents
- Images
- Internet searches
- SaaS and third-party connections

PLM systems were never designed to protect these types of data. That's why it's not enough to only focus on IP data itself. You must be able to see, track, and defend the data surrounding it to effectively prevent security incidents and breaches.

[1] Data Breach Investigations Report 2022, Verizon
[2] Data Breach Investigations Report 2022, Verizon
[3] 2023 Global Threat Report, Crowdstrike

Data Surveillance—Protecting Digital Thread Data

Flying Cloud CrowsNest patented data surveillance enables you to view data as it's created, moves, and is consumed across your environment. For the first time, you can see data analytically and forensically, as well as control where it goes.

See Data in Real Time

CrowsNest identifies and fingerprints both structured and unstructured data. Unlike digital rights management (DRM) solutions, CrowsNest fingerprints data without touching or altering it. Once data is fingerprinted, you gain complete visibility into data types, IP addresses, relationships, and content in real time.

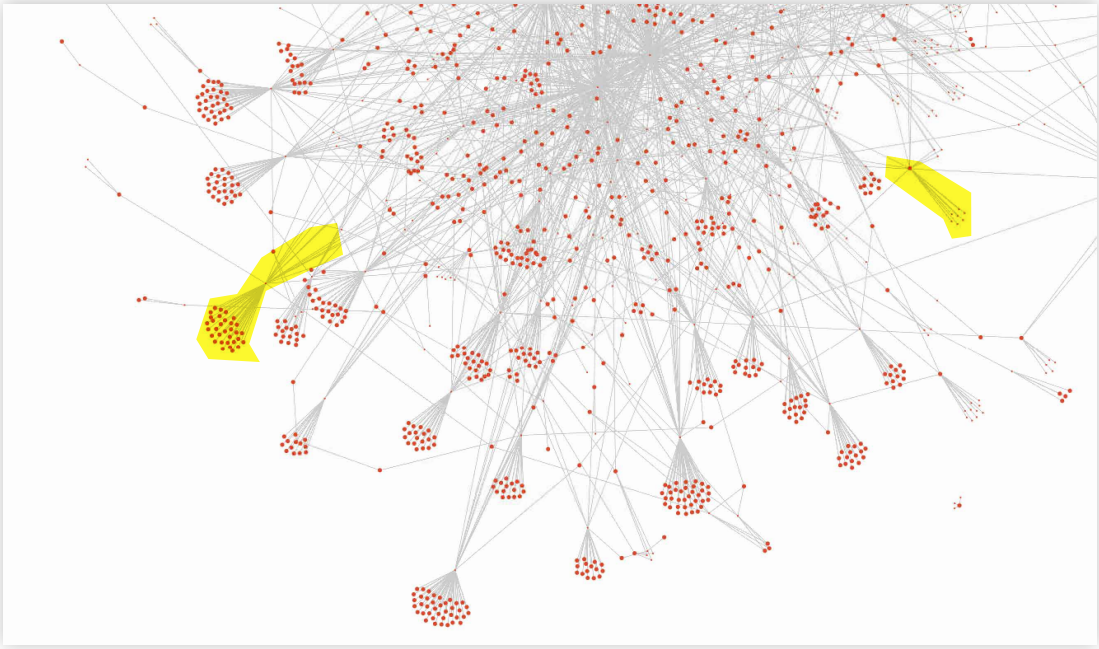

Figure 1. See where data originates, travels, and proliferates across the environment with the ability to drill down to packet-level detail.

Automatically classify data, eliminating manual methods of tagging data or relying on users. Use CrowsNest's out-of-the-box preconfigured rules. Import rules from other sources. Or, create your own rules. Unlike traditional IP address-based technologies, CrowsNest data fingerprinting allows you to even geo-fence data within physical spaces based on content.

Track Your Data

CrowsNest establishes a rolling baseline of normal activity for your data and follows fingerprinted data everywhere it goes. The rolling baseline is continually updated in real time as new content is added, infrastructure changes, and users come and go. When fingerprinted data behaves out of character with the rolling baseline, CrowsNest alerts you.

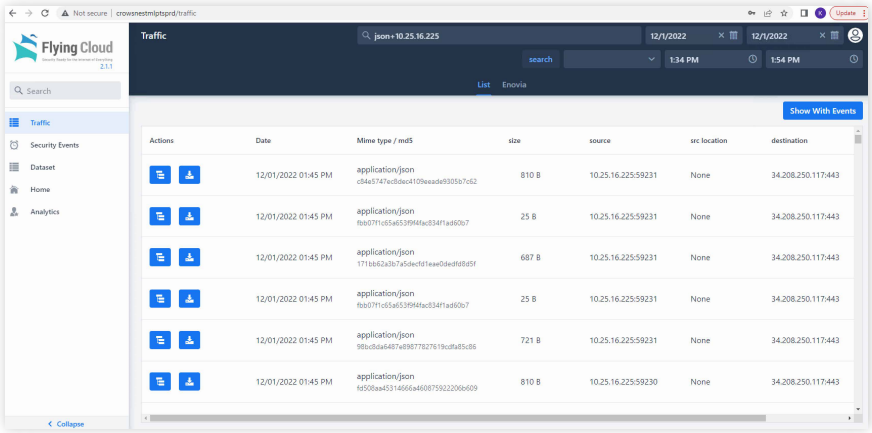

Figure 2. Track file types, activity, alerted events, and other attributes. Drill down to packet-level detail for any piece of data.

Defend Your Data

You decide how you want CrowsNest to track your data and defend it. Set event parameters based on your criteria and receive real-time alerts when policy is violated. Or, automatically trigger other security controls to respond. Once created, policies apply not just to the fingerprinted data, but to all data flowing across the network.

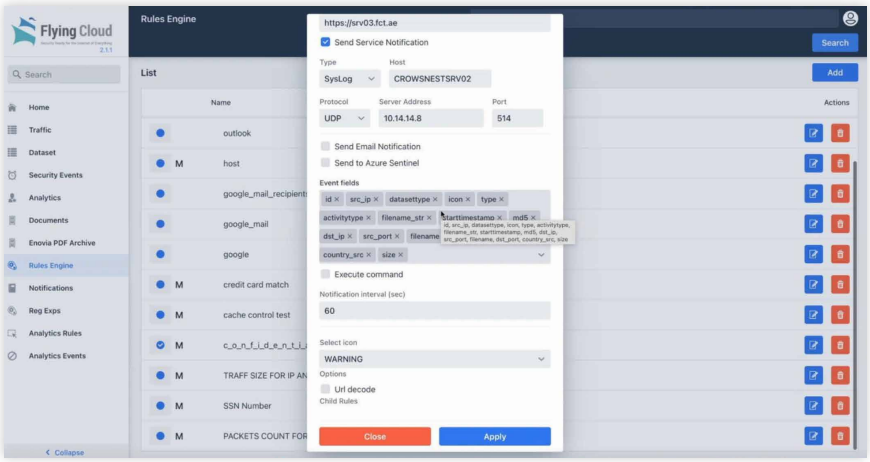

Figure 3. Our easy-to-use rules engine lets you apply policy to the data itself, based on content, sensitivity level, or any other parameter.

CrowsNest delivers far more powerful control over your data than DLP solutions. It also can identify and isolate data behaviors characteristic of ransomware, botnets, malware, Bitcoin, back doors, and command-and-control software.

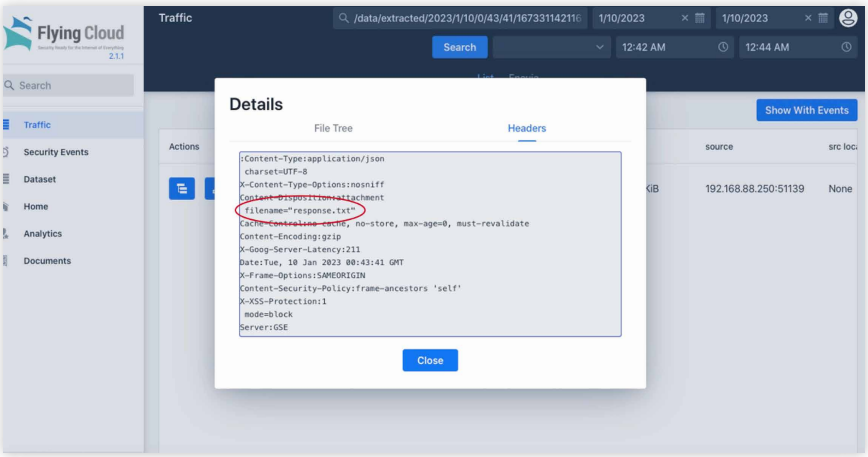

Figure 4. View session data at the packet level and export the PCAP file to other security analysis tools.

Go deeper with data forensics. CrowsNest provides complete event context at the packet level. You can replay data anomaly events for analysis and store them for regulatory purposes.

Benefits

Support Compliance and Executive Decision-Making

CrowsNest provides a ledgerized chain of custody for any data—from who creates it, to who consumes it, to everywhere that data goes and how it changes. If an event occurs, you have a record to show exactly what happened, how it happened, and which data was affected. A chain of custody provides you with the documentation needed to support executive and Board-level decision making, as well as compliance initiatives.

Expand PLM Security

Track data across systems, interfaces, and users on the company's network—inside and outside of the PLM. With detailed session data, you can account for any data leaving and entering the PLM environment. In the event of an authorized user allowing data to leave the network, you will know and can take mitigation measures.

Improve Overall Security Posture

CrowsNest enables you to secure and defend non-IP data that is still essential in the digital thread. This includes operational, financial, marketing, HR, IT credentials, and planning data. These essential functions still rely on critical data to ensure business continuity and resiliency.

Ensure Other Controls Work As Expected

Ensure that other security controls—such as DMZ and network segmentation—are working as expected. CrowsNest will alert you to fingerprinted and other sensitive data moving where it shouldn't.

For more information, request a meeting.
Or visit us at www.flyingcloudtech.com.

About Flying Cloud

Flying Cloud secures the one thing that matters most—data. We enable organizations to see their data as it is created, moves, and is consumed across the network. Founded in 2014, Flying Cloud holds nine data surveillance patents. Our CrowsNest data surveillance solution gives customers the first-time ability to look at their data analytically, forensically, as well as control where it goes. Flying Cloud is privately held.