Your data moved. Did your security move with it?

As data becomes more complex, agencies must trade legacy DLP for behavior-based defenses.

proofpoint.

Public sector organizations are awash in data — far more of it, moving far faster, across far more systems than legacy security tools were ever designed to handle. Every email, file transfer and download expands the attack surface. Yet many security programs are still built on a 20-year-old assumption that sensitive data is easily defined, lives in predictable places and can be locked down with static rules.

Today's reality is very different. As Jeremy Wittkop, principal enterprise architect at Proofpoint, explained, even the meaning of "sensitive data" has changed.

"At one point, the only things that really counted as personally identifiable information (PII) were social security numbers or other identifying numbers," he said. But today, organizations must protect a sweeping spectrum of personal and contextual details that can reveal identity or intent. "Society as a whole has taken a more expansive view of PII to mean data like addresses, phone numbers, eye color, height and weight."

More critically, sensitivity often emerges not from a single data point, but from how elements combine. "My name may not be sensitive … but connecting my name to another element that identifies something about me may be sensitive," Wittkop noted. These "toxic combinations" defy the traditional playbook of keyword lists and regex patterns that once defined the data loss prevention (DLP) industry.

Driven by distributed work, data mobility and evolving privacy expectations, organizations in every sector understand that safeguarding information requires far more than pattern matching. It demands understanding context and behavior — why a user is accessing data, how they're interacting with it and whether that activity is normal.

How modern work changed government's approach to sensitive data

Despite widespread concern about data sprawl, Wittkop argued the biggest shift is in how people work with data and access it. When data lived on controlled file servers behind a firewall, governance was simpler. Now, "data is everywhere. People are everywhere. They need access to the data, *but what they do with it* is what we're trying to govern."

Cloud repositories and modern applications offer better logging and API access than legacy infrastructures ever did. But the loss of natural choke points makes it harder for traditional DLP tools to understand *who* is interacting with data and *why*.

Proofpoint's modern, behavior-aware strategy

Modern risks fall into three categories, Wittkop noted: accidental sharing, third-party exposure and insider threats. Traditional DLP tools built around content inspection alone struggle across all three. They miss obscured data, can't recognize intent and often overwhelm teams with noisy alerts.

Proofpoint's approach is fundamentally different. It brings content, context and behavior into a single, unified, cloud-native platform so teams can identify true risk with far greater accuracy and stop data loss wherever it occurs.

Context allows organizations to protect data even when they cannot inspect its contents. Sensitive repositories such as research environments, regulated data stores or controlled government systems can be safeguarded based on their origin rather than their specific content.

"If something is downloaded from a certain place, we're going to assume it's sensitive and it should not leave our environment," Wittkop said. Behavior is equally critical for identifying both malicious insiders and accidental mistakes. Proofpoint establishes a baseline for each user and flags deviations, whether that's encrypting files before exfiltration, renaming or reformatting data, moving files to unapproved cloud services or misaddressing an email.

"People who are stealing data on purpose are going to try and circumvent your systems," Wittkop said. "The data itself isn't readable at the time it's exfiltrated … however, the behavior of trying to hide that data is very visible."

What sets Proofpoint apart?

Unlike siloed, rule-heavy legacy tools, Proofpoint provides:

- **Cross-channel visibility** from email to cloud to endpoint
- **Accurate content detection** with optical character recognition, exact data matching and large language model (LLM)-assisted classification
- **Adaptive policies** that adjust to user behavior and risk
- **A stable, cloud-native architecture** that scales automatically
- **A unified console** that reduces investigation time and false positives

"People who are stealing data on purpose are going to try and circumvent your systems. The data itself isn't readable at the time it's exfiltrated... however, the behavior of trying to hide that data is very visible."

– Jeremy Wittkop,
Principal Enterprise Architect, Proofpoint

Scaling modern data protection with automation and AI

As data volumes grow and alerts multiply, automation has become essential to keeping DLP programs efficient. Wittkop described automation as "an efficiency tool," noting that large organizations routinely face overwhelming caseloads. "If I can do 100 investigations instead of 1000, that saves me time," he said.

Proofpoint's approach focuses on consolidating context and reducing repetitive tasks so analysts can focus on true risk. This vision now extends through Proofpoint Satori™, which brings AI agents directly into security workflows. These agents help eliminate false positives, accelerate triage and ensure teams don't miss an alert.

The Satori DLP Triage Agent processes DLP alerts at machine speed, while the Satori Abuse Mailbox Agent can resolve thousands of user-reported suspicious emails in seconds. Additional agents, such as the Satori Phishing Simulation Agent, strengthen human resilience by generating attack-informed training automatically.

Together, these AI-driven capabilities reinforce Wittkop's broader point: Automation isn't replacing analysts, but rather giving them the scale, speed and insight that are required for modern data protection.

Building long-term resilience

At the end of the day, data security is about protecting people and enabling them to work safely. And as data becomes more distributed and dynamic, organizations need a DLP approach that understands human behavior, adapts to evolving risks and keeps pace with modern work.
"DLP isn't a technology. It's an organizational tool that's facilitated by technology," said Wittkop. Success requires ongoing alignment between leadership, security teams and evolving mission needs. With its integrated platform built around people, context and content, Proofpoint offers agencies and organizations the visibility and control they need to secure their most valuable information wherever it goes.

Click to learn more about Proofpoint's modern approach to Data Loss Prevention.