

Satori DLP Triage Agent

Reduce data loss risks and team burnout with autonomous DLP alert triage



Key benefits

- Eliminates L1 security toil by automating repetitive DLP alert triage efforts
- Reduces data loss risk, as teams immediately address true, escalated DLP alerts to quickly close the data loss windows of exposure
- Handles alert volumes consistently without the need for additional human staff
- Combines autonomous execution with guardrails, human supervision, explainability, and audit

Modern security teams are overwhelmed. User-reported suspicious emails, data loss prevention (DLP) alerts, and policy violations generate thousands of repetitive, low-value decisions every day. Even with strong detection, security operations center (SOC) and data security teams remain buried in level 1 (L1) triage. This slows response, increases burnout, and limits the value of upstream investments.

Proofpoint Satori addresses these problems. Satori is a set of solutions for autonomous security operations. Powered by agentic AI, Satori safely automates high-volume security workflows. It removes repetitive triage while preserving trust, control, and accountability.

Teams can scale operations without sacrificing governance.

Satori DLP Triage Agent

DLP is a world of tedious and time-consuming alert triage, even with finely-tuned data security tools. Proofpoint Satori DLP Triage Agent autonomously analyzes all alerts, eliminating false positives and noise. Analysts can focus instead on true escalated incidents that have a potentially critical impact on the organization.

Satori DLP Triage Agent uses a multi-step agentic workflow, called a mission, which labels and classifies all alerts, to prioritize alerts that represent true risk and resolve those that do not. Acting as an agentic analyst, Satori will label all alerts as false positives, not an issue, or escalated.

Missions reason using Proofpoint's rich telemetry, apply guardrails, act where permitted, and log every decision.

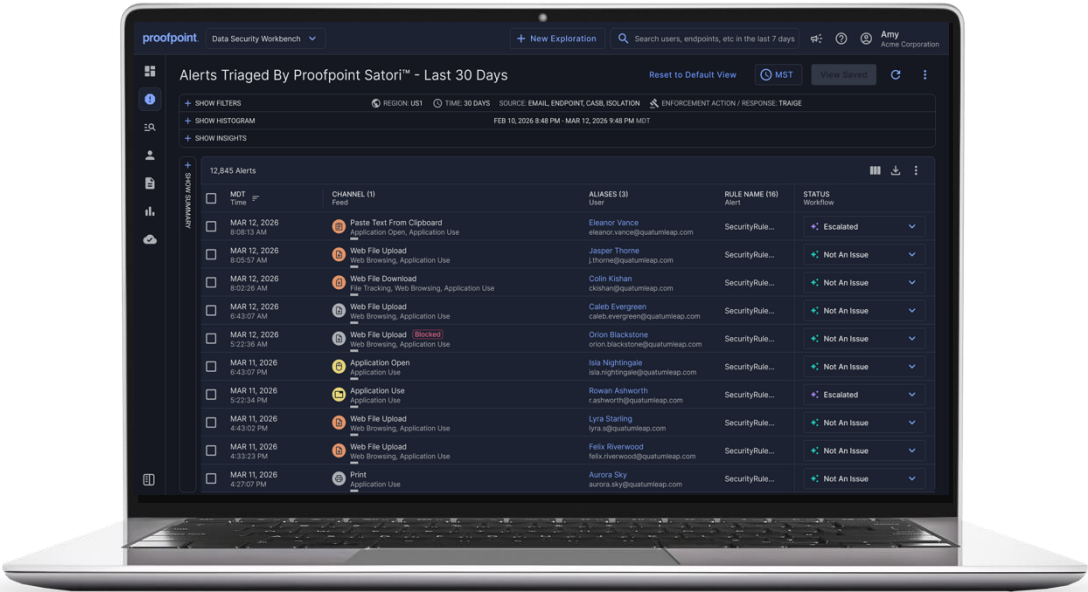


Figure 1. Satori DLP Triage Agent operates in the Data Security Workbench. Satori decisions appear on the right in the STATUS column, denoted by the Satori “sparkle.”

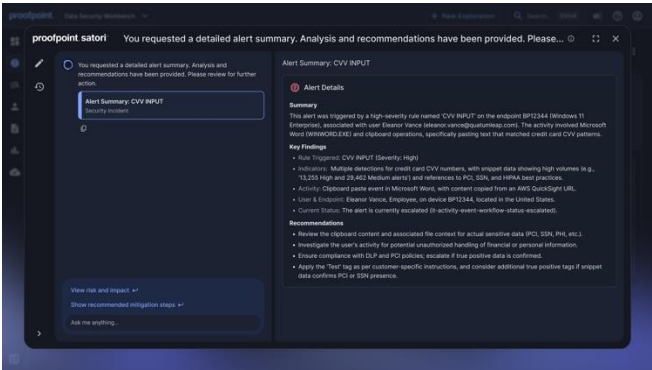
Execution with Full Explainability

The Satori DLP agent works in the Data Security Workbench, executing work as an agentic analyst, classifying all alerts. It also has an explainability mode with a chat window, allowing analysts to interrogate Satori for a deeper understand of Satori’s decisions and related thought processes for the work it has carried out.

Powerful precision with Satori Memories

Satori also leverages a “Memories” capability to tailor its outputs to each organization. It combines broad, global memories, based on universal patterns, with local memories established during a brief onboarding process, continuously refined over time through natural-language instructions operators share in the chat interface. Memories deliver precise, context-aware results from day one, and also allow customers to continually refine the agent’s go-forward behavior.

Figure 2. Satori DLP Triage Agent’s Explainability mode shows greater detail on Satori decisions. Its chat window allows operators to ask any question about its decisions or share Memories to change future behavior.



Human-in-the-loop supervision

Agentic workflows are powerful and autonomous, but also benefit from multiple layers of human supervision for accountability. Humans-in-the-loop proactively sample and validate agent decisions for accuracy and policy adherence, while reviewing and even challenging Satori's decisions to shape its go-forward behavior.

Key capabilities

Feature	What It Does
Cross-surface DLP Coverage	Assesses alerts across Proofpoint DLP sources and surfaces—including endpoint, cloud, and email excluding Adaptive Email DLP (AEDLP).
Automation with Humans-in-the-Loop	Automates DLP triage with hidden Proofpoint expert oversight that spot-checks, reviews decisions, and supports escalation for high-risk or ambiguous cases.
Precise outcomes with Satori Memories	Memories are natural-language instructions customers share with Satori to define go-forward behavior for ever-more precise outcomes mapped to organizational security, operational, or compliance preferences.
Business context setup	Immediate accuracy through onboarding that analyzes a sampling of historical DLP alerts paired with a structured questionnaire to understand business context ensuring alerts are triaged correctly from day one.
Execution Mode	Satori working as an agentic analyst, evaluating contextual factors for each alert for instant, consistent alert triage.
Explainability Mode	Shows why an alert was classified or escalated
Automated workflows	Can trigger optional, customer-created workflow to automate next steps after Satori DLP triage.
Reporting & Audit trails	Records classifications and analyst interactions in Proofpoint logs
AI Guardrails	Mission guardrails bound agent actions; agents do not carry out enforcement (block/delete/policy changes); high-risk exfiltration alerts escalated to humans.
In-tool Data Privacy	Satori protects data in agentic workflows using strong cryptographic encryption and authenticated service-to-service communication. All LLM inference occurs within Proofpoint’s security-reviewed and contractually enforced system boundaries; data is processed ephemerally.
24x7x365 elastic operation	Satori scales instantly during alert surges without volume constraints.
Action-Based pricing	Satori has an action-based pricing model—customers pay for automated work performed, not per seat, agent, or mission.
Data Residency (EU Planned)	Agent memories and chat history are stored at rest; DLP alert data processed in memory and dropped after classification. Currently in the United States; EU data residency targeted for Q3.



About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint’s collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com.

Connect with Proofpoint: [LinkedIn](#)

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.

[DISCOVER THE PROOFPOINT PLATFORM](#) 