DATA SHEET

ServiceNow Data Loss Prevention Incident Response

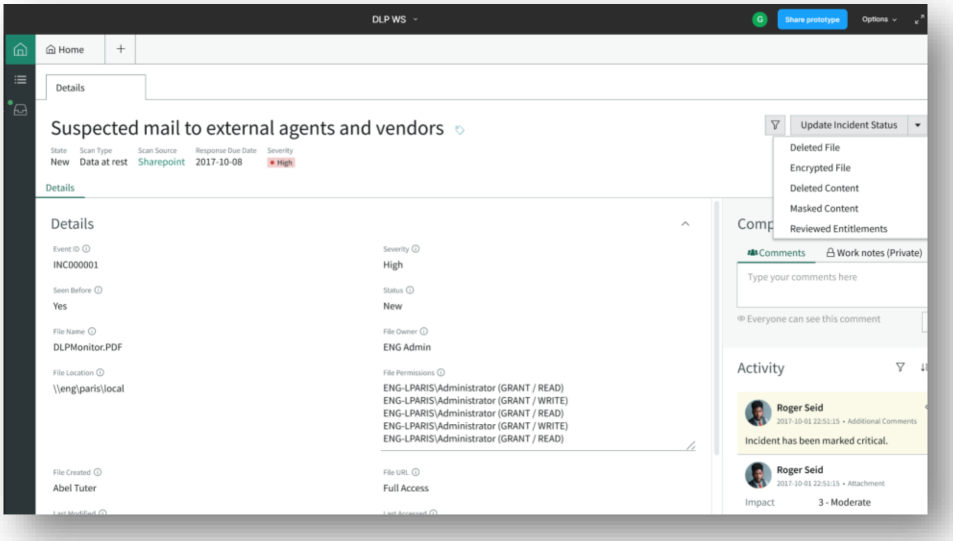
Why it's needed

Organizations today are struggling to maintain and keep up with the overwhelming amount of data loss prevention incidents they see on a daily basis. Due to disparate products across their infrastructure- incidents are difficult to track and manage in a timely fashion, making day to day tasks frustrating for end users and their managers.

- Data loss incidents happen on email 38x more often than IT leaders think
- 45% of us employees admit to downloading, saving, or sending work-related documents to their personal accounts before leaving or after being dismissed from a job
- 19% of security leaders deem machine learning and intelligent automation the most effective way to prevent data loss

What can ServiceNow DLP Incident Response do to help?

ServiceNow Data Loss Prevention Incident Response (DLPIR) allows you to import DLP Incidents from email, network, endpoint, and cloud sources by integrating with Data Loss Prevention products, ultimately pulling this data onto one platform. By using a remediation workflow- ServiceNow can automatically assign incidents to end users, managers, and DLP analyst teams through automated incident assignment and escalation, all by using intuitive and convenient workspaces specifically designed to simplify managing and reporting this work.



Suspected mail to external agents and vendors

State: New
Scan Type: Data at rest
Scan Source: Sharepoint
Response Due Date: 2017-10-08
Severity: High

Details

Event ID: INC000001
Severity: High
Seen Before: Yes
Status: New
File Name: DLPMonitor.PDF
File Owner: ENG Admin
File Location: \\eng\paris\local
File Permissions:
ENG-LPARIS\Administrator (GRANT / READ)
ENG-LPARIS\Administrator (GRANT / WRITE)
ENG-LPARIS\Administrator (GRANT / READ)
ENG-LPARIS\Administrator (GRANT / WRITE)
ENG-LPARIS\Administrator (GRANT / READ)
File Created: Abel Tuter
File URL: Full Access

Roger Seid
2017-10-01 22:51:15 • Additional Comments
Incident has been marked critical.

Roger Seid
2017-10-01 22:51:15 • Attachment
Impact 3 - Moderate

Key features

Integrate with multiple third-party DLP solutions to gain a unified view of incidents in the Now Platform – including Proofpoint, Netskope and Symantec DLP

Improve the efficiency of the DLP operations teams to monitor DLP incidents and assign incidents to end users that enable you to streamline DLP incident management

Help employees through customized email templates and notifications sent for each incident as well as in the form of a digest

Seamlessly escalate overdue DLP incidents from end users to managers providing real time feedback to help shape the corporate security culture

Easily track trends by open incidents, top offenders, incidents by scan source, and so on

Direct Incident Assignment

As many incidents are created due to error on the part of the end-user, DLIR reduces stress on the DLP analyst team. With ServiceNow, incidents can be assigned directly to end-users or managers and email templates can be used- as a weekly digest or whenever the incidents are discovered, including why the incident was generated and how to resolve it. End users and managers can access the incidents assigned to them in the DLPIR end user workspace.

Custom Incident Escalation

When necessary, incidents can be escalated up the chain of command. DLP Admins can specify specific escalation criteria for different types of incidents.

Cross-Org Communication Capabilities

DLP administrators have the power to configure email templates for coaching purposes as well as communicating with end users. They also have the ability to configure delegates for executives to allow other users to receive communication and respond on behalf of executives.

Dedicated-Customizable Workspace

DLP analysts can access DLP IR ops workspace to view and manage all DLP incidents across the organizations. With the help of DLP admin, they will be able to define and use custom incident states during incident management. Also, DLP analysts have the ability to create child incidents and easily identify repeat offenders.

Visibility into Valuable Metrics

DLP analysts have access to DLP incident summary reports as well as detailed incident and remediation trend reports.

Integration between ServiceNow and DLP products allows organizations to import incidents from multiple sources, such as endpoint, network, email, and cloud. This provides DLP teams the ability to drive remediation workflows involving end users, managers, and DLP operations team with automated incident assignment and escalations.

Key Stakeholders

DLP Admin
Enable API integration with DLP vendors, define incident assignment rules, escalation rules, email templates, incident response options, etc.

DLP Analyst
View and manage all the incidents, assign to different users/managers, create child incidents, and close incidents

End User
Receive email communication about DLP incidents that were generated due to their actions, review the incidents in the workspace, and respond to the incidents

Manager
Review the incidents escalated to them from end users, and respond to the incidents

InfoSec Executive
Needs visibility into current risk posture associated with containerized applications

servicenow

SN_DataSheet_DLPIR_June_2022