INTEGRATION BRIEF

Proofpoint and ServiceNow Partnership

Improve trust in email and data security

Products

Proofpoint

- Enterprise Data Loss Prevention
- Cloud App Security Broker
- Secure Email Relay
- Threat Response

ServiceNow

- DLPir
- ITSM
- Security Incident Response

Capabilities

- Data loss prevention
  - Data exfiltration
  - Data compliance
- Email authentication
  - Increased deliverability
  - Message scanning
  - SPF alignment
  - DKIM signing
- Operations
  - Workflow automation
  - Automated ticket creation

Today’s organizations face many daunting challenges. For one, they must quickly identify security threats and vulnerabilities. They must also prioritize them and coordinate with IT to remediate them in a timely manner. Most may find that they need to do more to protect their sensitive data. And that they need to reduce the non-delivery rate of important messages. But many have understaffed security teams. And so, they might look to more automation to address their needs.

Integrating Proofpoint and ServiceNow solutions can help. They improve response efficiency and reduce the workload of your security teams. They can help automate remediation tasks and enhance protection against data loss. And they can ensure the delivery of vital email.

Proofpoint detects, analyzes and blocks advanced threats. These threats can include data-loss issues in the cloud as well as ransomware delivered through email. We give you the visibility, tools and services that you need to authorize legitimate emails. And we help secure your ServiceNow email channel against deliverability challenges.

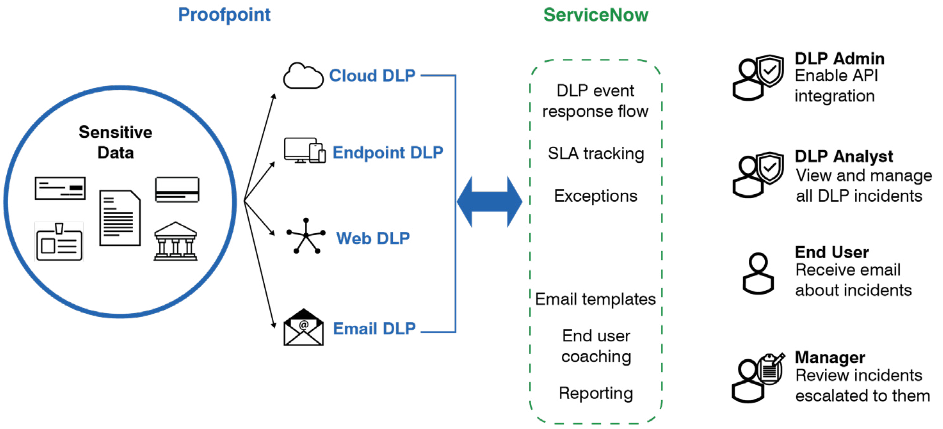

Figure 1: Proofpoint and ServiceNow DLP incident response.

ServiceNow gives your security and IT teams a single, shared platform to identify critical incidents. It lets them apply powerful workflow and automation tools to speed up their remediation efforts.

Our partnership helps you to:

- Protect incoming and outgoing sensitive data within ServiceNow
- Investigate Proofpoint Enterprise Data Loss Prevention (DLP) alerts in the ServiceNow Data Loss Prevention Incident Response (DLPir) module
- Improve the deliverability of ServiceNow emails and reduce risk of email impersonation
- Automate ticket creation in ServiceNow Security Incident Response with Proofpoint Threat Response input

Data Protection

Integration with Proofpoint's API-based Cloud App Security Broker (CASB) helps you to protect sensitive data in NOW tenants. It also helps you to manage DLP outcomes. It features:

- **Data exfiltration.** Scan for sensitive files that are exported from ServiceNow. Sensitive files are those that include data such as product details, designs, road maps and more.
- **Data compliance.** Scan for sensitive data that your customer does not want uploaded or stored in ServiceNow. Sensitive data can include PCI, PII, PHI and more.

Proofpoint first scans files. Then it notifies ServiceNow of any data exfiltration or compliance violations. ServiceNow then alerts their customers. And these customers can create new tickets or workflows based on the alerts.

DLP Incident Response

You can integrate Proofpoint Enterprise DLP with ServiceNow DLPir. This can help speed up investigations. And it can expedite response and remediation of DLP incidents in the cloud, endpoints, email and the web. It lets you synchronize the status and comments for DLP incidents across Proofpoint DLP and ServiceNow Security Incident Response. It helps to minimize incident impact, data loss and exposure. And it adds context to threats, data loss events and more to enhance your security operations.

Email Authentication

With Proofpoint Secure Email Relay integration, you can add our security and compliance controls to transactional emails that are sent from ServiceNow on your behalf. This helps protect your email identity. It also improves the deliverability rate. And it provides centralized control.

Secure Email Relay uses a secure connection between ServiceNow and Proofpoint. SMTP authentication addresses misconfigured email sending systems as well as broken email authentication validation checks. Before sending, all messages receive DKIM signing for DMARC compliance. This cuts the number of rejections of legitimate emails.

Secure Email Relay can also protect personally identifiable information and personal health information through optional encryption. And it can restrict this sensitive data with DLP.

Automated Ticket Creation

Integrating with Proofpoint Threat Response helps to speed up response times. Using custom scripts, Threat Response informs ServiceNow ITSM of incidents. It then enriches data with information related to these incidents. And it enables automatic ticket creation in ITSM.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.