EVALUATOR'S GUIDE

Evaluator’s Guide for Proofpoint Data Security Solutions

Evaluating a software product to ensure it is the right fit for your organisation is an important part of the purchasing process. A proof of concept, commonly referred to as a PoC, is a standard way to do exactly that. Getting hands-on experience with a software product helps you quickly determine if your business needs and use cases are met. A successful PoC takes away the guesswork and provides a tangible experience, which is why PoCs are so critical in the decision-making process.

A good analogy is buying a car: you're almost certainly not going to buy a new car without first taking it for a test drive. In fact, it's this same hands-on experience that Proofpoint offers with its Data Security solutions, through a fully hosted PoC to help you understand how your organisation can protect against data loss and insider threats.

Challenges with PoCs

Despite the benefits of doing a PoC, there can be several challenges that prevent PoCs from getting started and succeeding. Common challenges include:

- Lack of clearly defined use cases
- Getting internal sign-off and approvals
- Limited staff resources
- No access to test machines

Proofpoint offers an innovative approach to a PoC that alleviates these challenges and allows you to test our software quickly and efficiently.

Proofpoint PoC: fast, efficient, effective

Proofpoint provides a quick and easy way to gain hands-on experience with Proofpoint Data Security solutions. Our PoC runs in a fully hosted environment, providing you with all the tools you need to defend data and stop insider threats. Within two weeks, you'll be able to test the most common use cases. When the PoC is complete, Proofpoint will assist in documenting the findings, so you can share the results with your teams.

1. Getting started

You can get started with Proofpoint Data Security PoC on day one with no setup or approvals needed. You'll be provided with two virtual machines and logins to simulate user actions. You'll also have access to the Proofpoint Data Security SaaS environment to investigate users' actions. Working from the centralised console, you can get deep visibility into user behaviour with a user timeline and detailed metadata and screenshots. You can also triage alerts, manage incidents, hunt threats and manage policies, all from the same console. This gives you a cross-channel view of endpoint, email, cloud and web.

2. Use cases

Over the course of two weeks, you can test the most common user stories and use cases:

- A malicious insider trying to exfiltrate sensitive data
- A careless user not being careful with sensitive data
- A careless user mishandling data in GenAI applications
- A compromised user (phishing attack) losing data to an attacker
- A compromised user (telephone-oriented attack delivery—TOAD—for example) losing data to an attacker
- A careless user performing risky web browsing

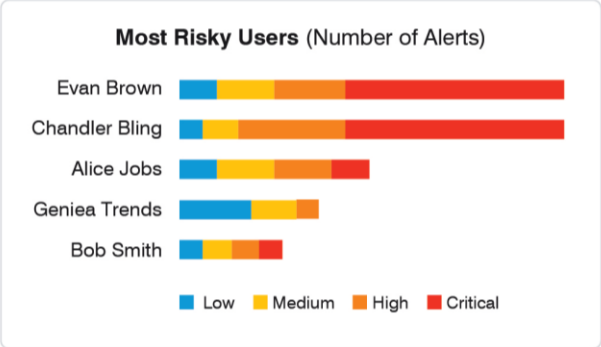
3. Wrapping up

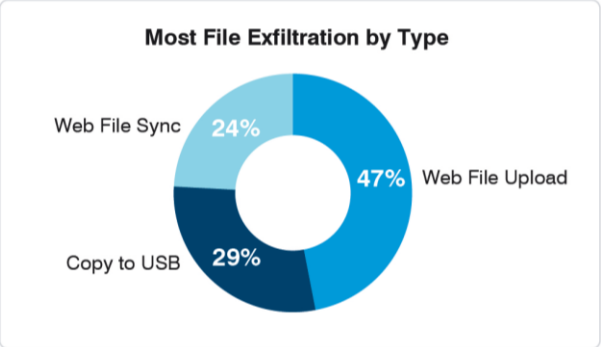
After conducting the PoC, you'll understand better how Proofpoint can accelerate your DLP or insider threat programme. An executive summary will be developed highlighting the use cases and benefits.

Sample Evaluation Criteria

- Proactively monitor risky users through a centralised dashboard
- Understand which data is leaving the company and how
- Understand why a rule was triggered and which sensitive data was detected
- Demonstrate changes in employee behaviour to maintain compliance and reduce risk
- Detect use of an unauthorised application
- Detect and prevent sensitive data exfiltration via web upload, USB and cloud sync
- Identify and prevent email exfiltration of sensitive data
- Detect and auto-remediate cloud-based threats and data exfiltration
- Monitor, detect and prevent data exfiltration via GenAI sites
- Detect changes to a file name and type
- Automatically block emails with the highest probability of causing data loss incidents
- Search and filter activity data to quickly find answers
- View a timeline depicting a user's activity before, during and after an incident
- View historical data of a user's activity
- Capture screenshots for forensics evidence
- Distinguish between a careless, compromised and malicious user
- Export a consumable report of user activity to HR and Legal
- Educate users with popup notifications and justification requests

Data security summary





8
Users browsing to GenAI websites

20
Files automatically remediated for oversharing

45
Blocks of unapproved web file upload

80
Sensitive emails send to unauthorized accounts

Benefits of a Proofpoint PoC

Without the need for setup or approvals, you can start testing Proofpoint Data Security solutions immediately in a fully hosted environment.

Quick time to value

A PoC with Proofpoint takes less than two weeks, providing a quick and easy way to gain hands-on experience and helping accelerate the decision-making process.

Measurable results

You can test the most common user stories and use cases with full access to Proofpoint Data Security solutions, gaining multichannel visibility across endpoint, email, cloud and web.

Proofpoint PoC: not your standard PoC

CRITERIA	STANDARD POC	PROOFPOINT POC
Setup time	Weeks to months, depending on approvals	Hours
Duration	Weeks to months	Less than 2 weeks
Customer effort	Significant	Minimal
Dedicated test machines	Needed for PoC	Not needed for PoC
Use cases	Need to be clearly defined	Most common use cases are available out of the box; can be augmented with specific use cases