aws marketplace

Forcepoint Data Loss Prevention

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap . . . . . 3 - 4

Valuable Features . . . . . 5 - 10

Other Solutions Considered . . . . . 11 - 13

ROI . . . . . 14 - 15

Use Case . . . . . 16 - 18

Setup . . . . . 19 - 21

Customer Service and Support . . . . . 22 - 23

Other Advice . . . . . 24 - 27

Trends . . . . . 28 - 29

About PeerSpot . . . . . 30 - 31

Product Recap

Forcepoint Data Loss Prevention

Forcepoint Data Loss Prevention Recap

Forcepoint Data Loss Prevention offers comprehensive data protection with strong template support, seamless cloud integration, and detailed reporting. It ensures data security through extensive endpoint, network, and server-level controls.

Forcepoint Data Loss Prevention is equipped with advanced fingerprinting technology, optical character recognition, and a large library of predefined rules. Organizations gain comprehensive data visibility and effective policy enforcement, supported by dynamic user behavior analysis and compliance capabilities. Its intuitive interface and flexible deployment options position it as a top choice for data security, although it could improve in communication reliability and language support. Complex reporting, machine learning integration, and cross-platform compatibility require enhancements.

What are the key features of Forcepoint Data Loss Prevention?

- Fingerprinting Technology: Enables precise data tracking and protection.
- Optical Character Recognition: Enhances identification of sensitive information in documents.
- Built-in Rules and Classifications: Offers a vast library ready for immediate use.
- Dynamic User Behavior Analysis: Provides insights for proactive security management.
- Cloud Integration: Ensures seamless data protection across cloud environments.

What benefits and ROI insights should users consider?

- Policy Enforcement: Robust mechanisms to ensure compliance and data protection.
- Comprehensive Visibility: Offers detailed insights into data movements and security posture.
- Efficient Management: Simplified controls for streamlined security operations.
- Compliance Support: Assists in meeting standards like PCI DSS.

Forcepoint Data Loss Prevention is utilized extensively in industries like finance and law to protect sensitive information from unauthorized transfers. It secures enterprise legal documents, financial assets, and personal data, employing features such as OCR to safeguard data across network, email, and cloud channels.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Forcepoint Data Loss Prevention is a user-friendly product, particularly regarding upgrades."

Shaikh Mubashshir

Cyber Security Technical Engineer at a consultancy with 10,001+ employees

- "Forcepoint enables you to clarify aspects of your data, including which data to protect for how long, what priority to assign to the data and the destinations. It's a comprehensive, dedicated solution. The interface is user-friendly and easy to manage. No other product will give you the same visibility and data classification functions as this tool."

AlexOgbalu

Director at LiveFromSpace Limited

- "The real-time analytics feature is helpful. It alerts within seconds and promptly informs management of any potential security issues."

Md. Shahriar Hussain

Information Security Analyst at Banglalink

"We like the ability to customize our requirements and rules, as well as its ease of use and management. It also has a cloud feature and proxy functionality."

Badrul Hisyam Jamil

IT Manager at a financial services firm with 5,001-10,000 employees

"The technical support for the solution is very good."

Mitesh D Patel

Senior Technical Consultant- Cyber Security at Ivalue Infosolution

"Technical support has been helpful."

SurendarJ

Deputy Manager of IT at FP LAB

"Forcepoint offers many policies that conform to global DLP best practices, including requirements specific to regions like the Middle East, Europe, etc. They have a policy database in their product. That feature is unique to Forcepoint. Their AI and fingerprinting are incredibly effective and robust. We have tested it multiple times. It always catches the correct data being leaked."

Muhammad Ali Aziz

Senior Manager Cyber Security Services & Solutions at Trillium

What users had to say about valuable features:

"We appreciate the user-friendliness and ease of implementation of the Forcepoint Data Loss Prevention platform. The availability of the vendor support team is an added advantage.."

SteffyJoy
Cyber Security Consultant at Mechsoft

Read full review

"I do not have any real valuable features at the moment.

It was mostly stable.

There is a lot of articles and documentation that technical support direct you to.."

Owen Nunez
Security Engineer at Protego Trust Bank

Read full review

"Some good features are basically its UAV Analytics engine. And even fingerprinting is really good in Forcepoint.

Forcepoint recently released an in-line proxy feature, which is a great addition. Previously, users had to add an extension to their browsers, but now that's not necessary. Now, that extension is not needed. ."

Shruti Shetty
Implementation Specialist - Data Privacy at EVSPL

Read full review

"Forcepoint Data Loss Prevention is a user-friendly product, particularly regarding upgrades. Every function and task, such as backups, forensics, and policy creation, is defined clearly and is easy to manage. It provides multiple customization options for policies, which makes it superior to Symantec. Fingerprinting technology is supported, although I primarily monitor with a data classification tool.."

Shaikh Mubashshir
Cyber Security Technical Engineer at a consultancy with 10,001+ employees

Read full review

“First, you need to categorize your data—what kind of data it is, the severity of its sensitivity, how long it needs protection, and the destinations that need protection. Forcepoint provides a dedicated solution with a user-friendly interface that makes it easy to manage. Remember that DLP doesn't handle data classification independently, so you'll need another tool to classify your data. For instance, you might use a classification tool to label documents as confidential, private, or internal.

Once the classification agent is installed on the endpoint, users need to label their data accordingly. For example, a Word document containing sensitive information should be labeled confidential. After labeling, you can create a policy in the DLP solution, such as Forcepoint, to block any data labeled as confidential from being shared. You can specify destination addresses to block at various levels, like the network, email, or RDP..”

AyoubAkhtar

Cyber Security Engineer at a tech services company with 1,001-5,000 employees

Read full review

"Forcepoint enables you to clarify aspects of your data, including which data to protect for how long, what priority to assign to the data and the destinations. It's a comprehensive, dedicated solution. The interface is user-friendly and easy to manage. No other product will give you the same visibility and data classification functions as this tool.

You install the agent to your endpoint, and the end user needs to label the data as confidential, private, internal, etc. After you label the document, you can confirm the confidentiality and go to the DLP to make a new policy to block the specified destination addresses at the Forcepoint level, such as network, email, RDP, etc.

Forcepoint uses machine learning and AI file or database fingerprinting. This can give you an early chance to prevent incidents fast. File fingerprinting gives you 100 percent accurate DLP results. ."

AlexOgbalu
Director at LiveFromSpace Limited

Read full review

Other Solutions Considered

"I have used a similar Microsoft solution to Forcepoint Data Loss Prevention, and the Microsoft solution was better. However, we were using Forcepoint Data Loss Prevention because we had a contract.."

Verified user

Senior Cyber Security Analyst at a logistics company with 5,001-10,000 employees

Read full review

"We evaluated Symantec, McAfee, and Trend Micro but found that Forcepoint was the best for complete on-premise without comparing the CASB solution, had the best UI, and was the most easily maintained.."

AtulVats

Information Security Consultant at a tech services company with 10,001+ employees

Read full review

"Forcepoint offers a more cost-effective solution because everything, including OCR, is included in one package, unlike Symantec, where it is an add-on with an additional cost. We also considered McAfee before choosing Forcepoint.

So, the main reason we chose Forcepoint is the cost because it's a single package.."

Badrul Hisyam Jamil

IT Manager at a financial services firm with 5,001-10,000 employees

Read full review

"Instead of Forcepoint Data Loss Prevention, I recommend Purview to others, especially if you are located on Microsoft platform, since it helps with compliance and not only as a DLP tool. There is a gap we need to close in Forcepoint Data Loss Prevention as it is useful for security operations. For example, it can be used to ask an end user to unlock your blocked emails.."

Verified user
Consultant at a tech services company with 1,001-5,000 employees

Read full review

"I'm just looking for a SaaS-based model. That's what I am exploring right now.

Fortunately or unfortunately, Forcepoint has not come up with a pure SaaS-based DLP. I'm just looking in the market to see what the best solution I can get is in terms of the same sort of production or to see how I can gradually migrate it or have a one-time migration of my Forcepoint policies directly to the SaaS-based solution. I'm hoping I can reduce my administration efforts in terms of managing the hardware.."

SurendarJ
Deputy Manager of IT at FP LAB

Read full review

“I'm also aware of Symantec and McAfee.

Forcepoint has extensive coverage compared to Symantec or McAfee. The reliability was good. I'm getting better coverage in terms of security, and I get better insights as well.

Symantec also seems to be good. That's my understanding of the market. However, due to their recent acquisition via Broadcom, they have some higher renewal costs.

Forcepoint, from a coverage perspective, it is giving better insights on the content. We cannot compare the insights with Microsoft, Palo Alto, or even Trend Micro..”

SurendarJ
Deputy Manager of IT at FP LAB

Read full review

ROI

Real user quotes about their ROI:

"As a partner, we have seen ROI with Forcepoint. We cover our costs through licenses, implementation services, and SLAs in which we support our customers and help resolve their issues whenever they want to open cases or adjust configuration.."

Kamal Abdelrahman
Country Manager at Magarah

Read full review

"My clients are seeing ROI because the privacy office is quite comfortable now that they've done everything reasonable to meet the compliance requirements. There is a level of assurance provided by the DLP solution.."

Verified user
Management Executive at a security firm with 11-50 employees

Read full review

"We have seen return on our investment because we're able to track our data. It's not so much an active return on investment, but more like an insurance policy. It prevents bad things from happening.."

AjitMatthew
Principal. - Head - IT, Information Security and Admin at a consultancy with 201-500 employees

Read full review

"One of our recent deployments of Forcepoint was for a bank that has requirements for PCI compliance. In terms of what they invested in the solution, they got the value back within a quarter.."

MUHAMMAD FAHAD HASSAN
System Engineer at ABM Info. tech

Read full review

"Forcepoint DLP helped customers save some money at the end of the cyber security field. Data is the most important thing you need to implement for a DLP solution in your environment. You could also face insider threats. Implementing a DLP solution helps prevent potential data leaks by giving you control over what kind of data is being accessed, where it's stored, and how it's being used within your environment. It also allows you to monitor and prevent unauthorized sharing of sensitive data, ensuring better security across your organization.."

AyoubAkhtar
Cyber Security Engineer at a tech services company with 1,001-5,000 employees

Read full review

Use Case

"Our main use case for the product involves classifying and protecting organizational data from unauthorized transfers, especially when users attempt to upload or transfer classified data to public cloud services or data-sharing platforms.."

Md. Shahriar Hussain
Information Security Analyst at Banglalink

Read full review

"In most of the banks that my company has implemented the tool, we have EMI and credit card information, and they don't want it to go outside the bank. It is also used to prevent company and other financial information.."

Verified user
Technical Support Engineer at a tech services company with 11-50 employees

Read full review

"The main purpose of DLP is to protect data from being sent outside of the organization without authorization. So, my client uses it to protect emails and web traffic and to integrate with content classification and USB blocking systems.."

Shruti Shetty
Implementation Specialist - Data Privacy at EVSPL

Read full review

"The main use case is the built-in OCR feature that the customer needs, but the OCR feature is limited to the network level. You cannot use this at the endpoint level, where there's a risk of data leakage. End-users can leak scanned pictures or screenshots, so customers need protection against these data leaks.."

AlexOgbalu
Director at LiveFromSpace Limited

Read full review

"The main use case for Forcepoint DLP is its OCR feature, which many customers need. The OCR capability can only be used at the network level, not at the endpoint level. It enables network-based data security, such as scanning emails or web traffic for potential data leaks. It's useful when dealing with scanned documents or screenshots containing sensitive information, preventing data leakage for multiple customers who require this level of security.."

AyoubAkhtar
Cyber Security Engineer at a tech services company with 1,001-5,000 employees

Read full review

"Major compliance issues are faced by every manufacturer or by those who use customer data. From a compliance point of view, people want a DLP solution for their organization. Every organization needs a DLP solution to prevent data leakage to external sources outside the company, making it one of the major use cases for every customer as they require a DLP tool that covers multiple channels like email, web, network, printers, USB, and removable devices.."

Mitesh D Patel
Senior Technical Consultant- Cyber Security at Ivalue Infosolution

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"The initial setup is simple. Each component is installed separately if needed, allowing flexibility in implementing data loss prevention with large numbers of users.."

Shaikh Mubashshir Read full review

Cyber Security Technical Engineer at a consultancy with 10,001+ employees

"The initial setup is simple. It's now easier than Microsoft, for example.

We currently use a hybrid model with on-premises deployment for the top and cloud access for laptops.."

Badrul Hisyam Jamil Read full review

IT Manager at a financial services firm with 5,001-10,000 employees

"When deploying a DLP solution in your environment, it is important to follow best practices and start with monitoring mode. Initially, you may not know where your data resides, which users need access to it, or the nature of the data itself. Deploying an agent and monitoring the data flow and usage for three to six months is essential. ."

AyoubAkhtar

Cyber Security Engineer at a tech services company with 1,001-5,000 employees

Read full review

"Before deploying, you have to set up your prerequisites. Your Active Directory should be integrated, and the best practices should be established in your environment. The time needed to deploy depends on the scope of your environment. You need some technical expertise to implement a DLP solution. It generally takes three to six months of testing and monitoring. ."

AlexOgbalu

Director at LiveFromSpace Limited

Read full review

“The setup was quite straightforward.

The deployment took approximately one week and required remote and physical support from a local partner and the necessary hardware and appliances.

I rate the process a nine out of ten. .”

Md. Shahriar Hussain

Information Security Analyst at Banglalink

Read full review

“The product's initial setup phase was easy.

The solution is deployed on an on-premises model.

The time taken to deploy the product is something which depends on the solution or the setup. Mostly, the solution can be deployed within three days, after which some finetuning is required to meet the requirements of our company's customers. .”

Mitesh D Patel

Senior Technical Consultant- Cyber Security at Ivalue Infosolution

Read full review

Customer Service and Support

"I rate Forcepoint support six out of 10. It depends on if you get support from the Indian or European side. Overall, Forcepoint support is not very good.."

AlexOgbalu
Director at LiveFromSpace Limited

Read full review

"I would say that their technical support is quite helpful. I would rate them a seven, on a scale from one to 10, with one being the worst and 10 being the best.."

ManjitSingh
Cyber Security Engineer, team lead at a wellness & fitness company with 10,001+ employees

Read full review

"Whenever there are issues, the support engineer is available to handle them. They conduct sessions to check logs and policies, unlike Symantec, where engineers may temporarily check and ask for logs, causing delays.."

Shaikh Mubashshir
Cyber Security Technical Engineer at a consultancy with 10,001+ employees

Read full review

"Customer support simply directs us to links to read up on our own. When we contact support, we need one on one help, not directions to articles. They need to improve the way they deal with customers and be more hands-on. ."

Owen Nunez
Security Engineer at Protego Trust Bank

Read full review

"It can be hard to contact customer service and support, and their response times and solutions can be slow and sometimes irrelevant.

A lot of time their feedback is not helpful. ."

Badrul Hisyam Jamil
IT Manager at a financial services firm with 5,001-10,000 employees

Read full review

"The solution's technical support was bad as they have no skills at all. We are not able to get replies from the tool's support team. I am not sure if the tool's team could offer advice or consultations because a local company used to do it for the product, as there are just a few skilled people available at Forcepoint, which is also an issue.."

Verified user
Consultant at a tech services company with 1,001-5,000 employees

Read full review

Other Advice

"Overall, I rate Forcepoint Data Loss Prevention eight out of ten. I recommend it to users looking for on-premise solutions. Proofpoint is a main competitor for on-premise solutions.."

Shaikh Mubashshir
Cyber Security Technical Engineer at a consultancy with 10,001+ employees

Read full review

"I rate Forcepoint Data Loss Prevention eight out of 10. Maybe we can find a better DLP solution, but I always prefer Forcepoint because I have experience and expertise with it. ."

AlexOgbalu
Director at LiveFromSpace Limited

Read full review

“The platform's key features include blocking unauthorized data copying to USB drives, preventing data transfers to the cloud, and discovering, classifying, and monitoring data without causing friction for users.

The real-time analytics feature is helpful. It alerts within seconds and promptly informs management of any potential security issues.

I suggest thoroughly understanding your organization's data leakage channels and the criticality of your data. With this understanding, you may fully benefit from using DLP.

Overall, I rate it an eight out of ten. .”

Md. Shahriar Hussain
Information Security Analyst at Banglalink

Read full review

“The real-time analytics feature is good, and the tool is really easy to use. I have no concerns regarding the tool.

It is easy to integrate the product with other solutions like SIEM solutions. We have multiple products that we have integrated with Forcepoint Data Loss Prevention, including Microsoft.

I have only used the machine learning part of the tool, which is easy to use.

I recommend the tool to others.

I rate the tool an eight out of ten..”

Verified user
Technical Support Engineer at a tech services company with 11-50 employees

Read full review

"You have two primary use cases for encryption: one for USB devices and the other for network-level data, like email. For email encryption, you can use an appliance that encrypts emails before sending them to another recipient. You can set up DLP for USB devices to manage and secure the data copied to the USB. By registering the USB with your DLP administrator or security tool, such as Forcepoint Security Manager, you can ensure that any data transferred to the USB is protected through encryption, preventing unauthorized access.

Integrating a DLP solution with your Active Directory is a prerequisite for implementing it in your environment. Ensuring your Active Directory follows best practices and benchmarks is crucial for seamless integration and optimal functionality of the DLP solution. You need to add the Active Directory to the environment. It must be integrated because you cannot block your data if your endpoint is not integrated with the endpoint level.

Overall, I rate the solution a nine out of ten.."

AyoubAkhtar
Cyber Security Engineer at a tech services company with 1,001-5,000 employees

Read full review

"AI is mostly used when you have to check the DLP inside artificial intelligence, and it is not perfect. We were also looking for SSE solutions, and the point is that Forcepoint could have been a good candidate, but it is located in some bad countries, making it one of the main issues why the tool was no longer a satisfying solution for our company. The tool is also quite heavy. In some cases, it is slow, making it not so comfortable to operate.

The tool is fine for the DLP features, especially when you are on an on-premises model with a data center. If you are on the cloud, I would not recommend it.

Purview and Forcepoint are almost the same, as both can be used to block, upload data, or send emails. Once something is blocked, you ask the security operations, who will start, to provide us with the document we can look at to see if it is legitimate or not.

The incident management process is not based directly on Forcepoint. Forcepoint is used to detect and block, but the response is not done inside of Forcepoint. It is done at the data level.

I rate the tool a seven out of ten.."

Verified user
Consultant at a tech services company with 1,001-5,000 employees

Read full review

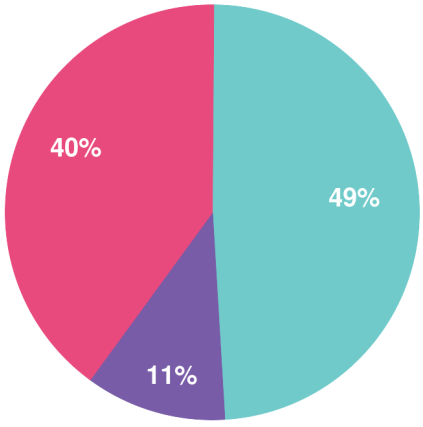
Top Industries

by visitors reading reviews

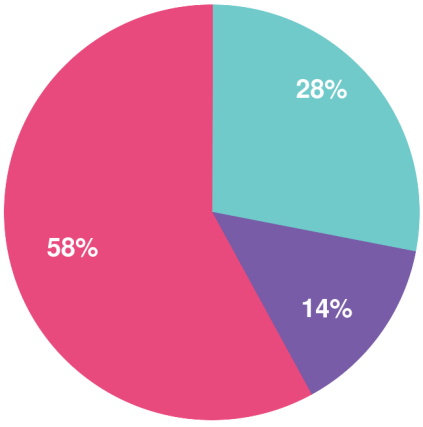
Computer Software Company	14%
Financial Services Firm	14%
Manufacturing Company	10%
Comms Service Provider	6%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944