DATA LEAKAGE DETECTION

Detect sensitive data exposed by employees, contractors, or third parties.

DATASHEET

DATA LEAKAGE DETECTION

HIGHLIGHTS

- **Immediately detect exposed sensitive data**
- **Search for document markings, brands, and DLP identifiers**
- **Track changes to documents over time to understand if a leak is new**
- **Gain the context you need to make quicker, better decisions**
- **Use playbooks to remediate exposure**
- **Augument existing DLP solutions**

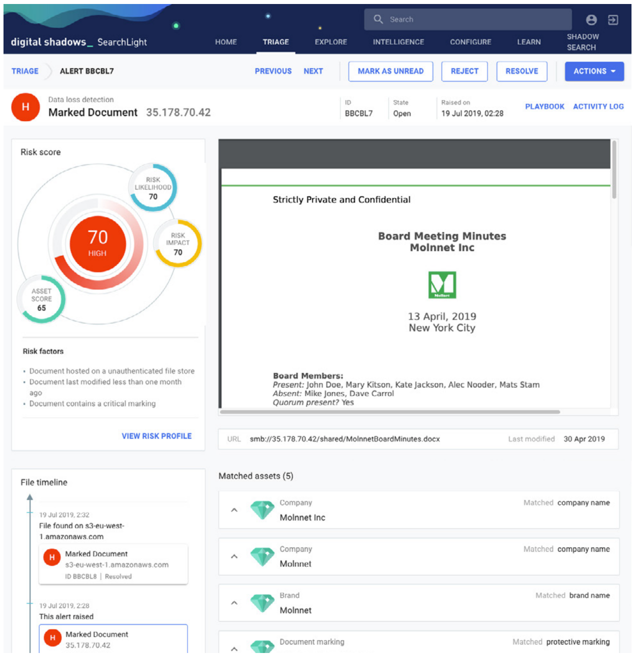
digital shadows_

Whether it’s intellectual property, proprietary code, personal data, or financial information, the goal of information security is to protect these assets. However, its not enough to only focus on your data stores - you need to know what data is already exposed.

When these assets are shared across growing electronic ecosystems, third parties, cloud services, or hosted on infrastructure-as-a-service, it’s easy to lose track. Combine this with exposure from social media and Shadow IT, it’s practically impossible to know where your sensitive data resides online.

A failure to detect this exposed data has serious consequences on your business, from enabling corporate espionage to falling foul of compliance regulations. This data provides attackers with a huge advantage: enabling their reconnaissance, selling your data to the highest bidder, or holding your data to ransom.

SearchLight continually monitors for your technical, sensitive, or personal data across a range of online sources, and instantly alerts you to its exposure. You receive all the context you need to make quick, informed responses.



Data loss detection
Marked Document 35.178.70.42

ID BBCBL7
State Open
Raised on 19 Jul 2019, 02:28

Risk factors
- Document hosted on a unauthenticated file store
- Document last modified less than one month ago
- Document contains a critical marking

Strictly Private and Confidential

Board Meeting Minutes
Molnnet Inc

13 April, 2019
New York City

Board Members:
Present: John Doe, Mary Kitson, Kate Jackson, Alec Nooder, Mats Stam
Absent: Mike Jones, Dave Carrol
Quorum present? Yes

URL smb://35.178.70.42/shared/MolnnetBoardMinutes.docx Last modified 30 Apr 2019

File timeline

19 Jul 2019, 2:32
File found on s3-eu-west-1.amazonaws.com
Marked Document
s3-eu-west-1.amazonaws.com
ID BBCBL8 | Resolved

19 Jul 2019, 2:28
This alert raised
Marked Document
35.178.70.42

Matched assets (5)

Company
Molnnet Inc
Matched company name

Company
Molnnet
Matched company name

Brand
Molnnet
Matched brand name

Document marking
Matched protective marking

Example Exposed Document Alert

ALERTS

Digital Shadows SearchLight™ Enables You to Detect:

Employee Credentials

Exposed employee credentials enable attackers to perform account takeovers. Our data breach repository has over 14 billion exposed credentials, and continues to grow.

Sensitive Documents

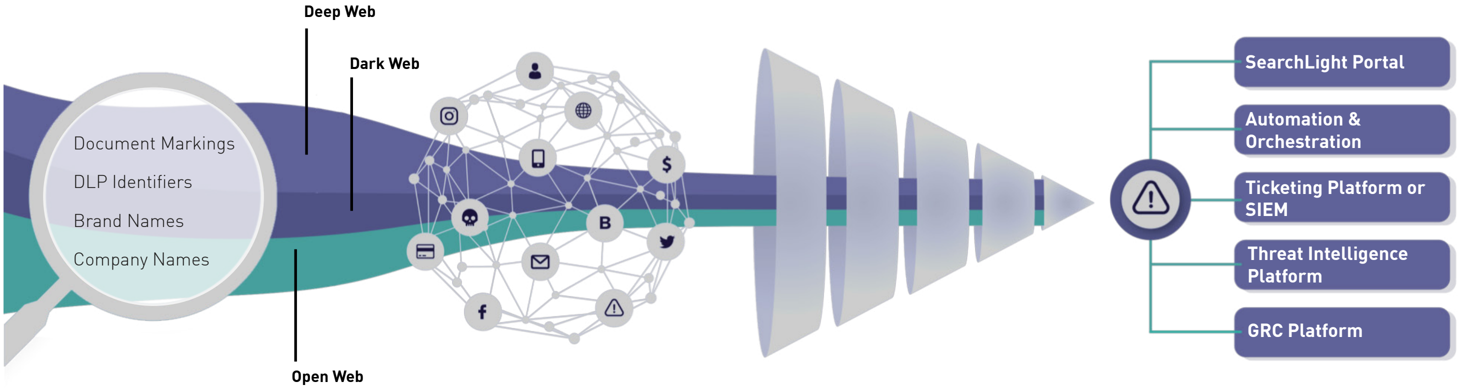
Confidential, private and sensitive documents not meant for distribution, such as exposed contracts, employee pay stubs, and confidential board minutes.

Customer Data

Exposed details about your customers can create brand and business risk, as well as regulatory problems. Detect customer data (such as Personally Identifiable Information and leaked payment cards).

How SearchLight Detects Data Leakage

With SearchLight, organizations register their document markings, DLP Identifiers, Brand Names, and Company Names as assets. SearchLight continually monitors for these assets across the open, deep, and dark web to notify you of online exposure. Each alert includes context and remediation options, including the ability to launch takedowns from within the SearchLight portal.



Configure
Identify Key Assets

Collect
Monitor for Exposure

Analyze
Risk Identification

Mitigate
Take Action and Protect

SOURCES OF EXPOSURE

SearchLight continually monitors for a range of exposed credentials and file types, including PDFs, documents, spreadsheets, and presentations. These often contain sensitive information that threat actors can use to their benefit and harm your organization. Common examples include board minutes, penetration tests, patent information, and exposed PII. SearchLight has the widest sources of collection, searching across billions of exposed files.

- Publicly-available online file stores, such as Amazon S3, SMB, FTP, and RSync. These are popular as a central file repository for storing backup archives and also for hosting content that is referenced by websites and production systems.
- Company websites that include content hosting services, such as web index folders and CDNs.
- Criminal sharing platforms that are popular with threat actors, including dark web forums and messaging services such as Telegram, where files are transferred during the sale of information
- Online code hosting services, such as GitHub and GitLab that host documents.
- Document sharing sites, such as Scribd and Slideshare.
- Large data breaches. Collected by our technology and Closed Sources Team.
- Paste Sites. Including, but not limited to Pastebin.

2.3B

Files exposed across misconfigured online file stores

50%

Of customers detect exposed data every week

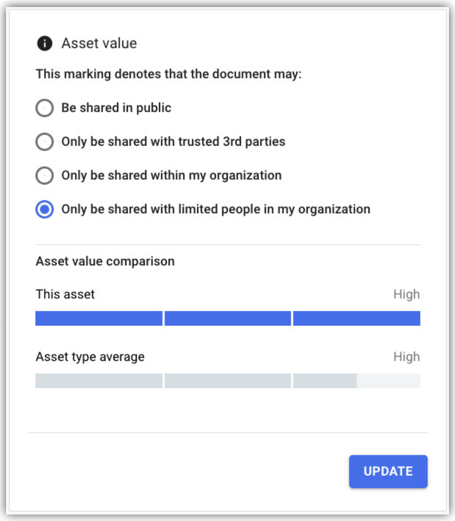
>14B

Credentials collected to date by Digital Shadows

INSTANT CONTEXT

For every alert, SearchLight provides rich context that enables you to make better decisions, faster. Here are the top four pieces of context we draw out for marked document risks, as an example.

1. **Asset Match Score**. Understand which of your assets SearchLight detected on the exposed document. Crucially, we understand that different document markings and DLP identifiers will have different levels of importance to your business. That's why we enable you to provide asset values, as shown to the right.
2. **Identify Risk Factors**. By ascertaining the importance of the documents, as well as it's age and other risk factors. A risk score, based on the FAIR framework, helps to quickly triage and prioritize responses.
3. **Investigate File Metadata**. As well as providing a downloadable PDF of the document, SearchLight also extracts the document metadata - aiding you to quickly ascertain document ownership.
4. **Reputation Score**. View the reputation score of the location hosting the document with data from Webroot. This will identify if it has previously been identified as suspicious.



Asset value

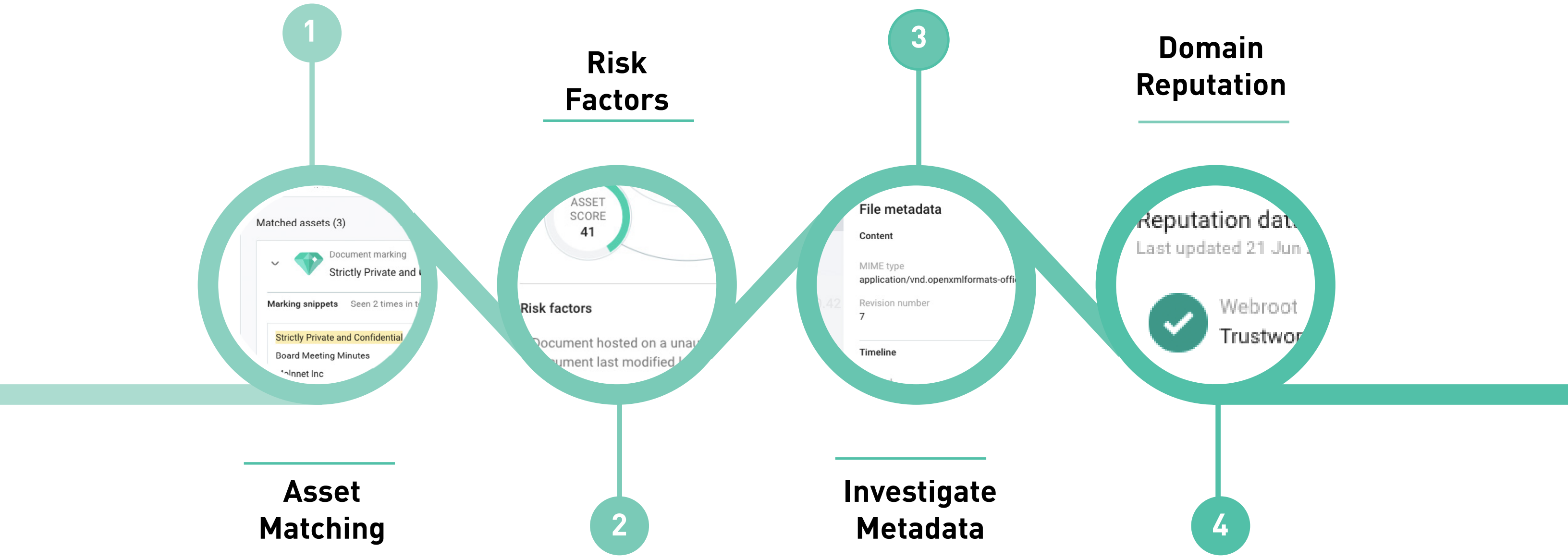
This marking denotes that the document may:

○ Be shared in public
○ Only be shared with trusted 3rd parties
○ Only be shared within my organization
● Only be shared with limited people in my organization

Asset value comparison

This asset High

Asset type average High

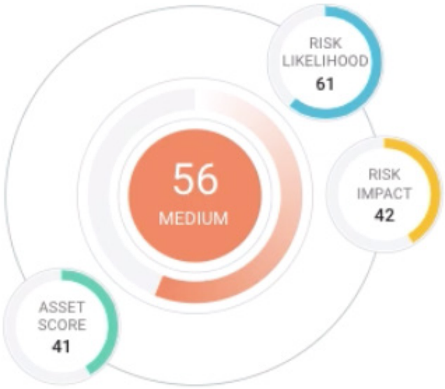


REMEDIATION

Data leakage alerts are made available through our SaaS portal, as well as through our free third-party API integrations with ticketing, SIEM, and other platforms.

Prioritize Based on Risk Score

Each alert has a risk score, derived from the threat, impact, and risk attributes to provide a risk score. These are all aligned to the Factor Analysis of Information Risk (FAIR) framework, enabling you to prioritize your efforts and respond more effectively.



FAIR-Aligned Risk Scores for Alerts

Playbooks for Remediating Risk

Within each alert, response playbooks guide you to the actions you should take. These playbooks are mapped to the following NIST Incident Response Plan stages:

- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

Augment Data Loss Prevention (DLP) Tools

For organizations using DLP tools, detecting sensitive data outside of your network can be an indication that something is not working or misconfigured. By adding this external monitoring, you can close the loop on data loss.

Managed and Templated Takedown Options

In some instances it might be necessary to remove certain pieces of content. We provide options to launch templated and managed takedowns. Managed takedowns provide end-to-end management of submitting, chasing, and confirming takedown requests. This empowers security teams to take action without adding work to their teams. Learn more about Managed Takedowns here.

TRY FOR FREE WITHIN SEARCHLIGHT ▶

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threats. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface. To learn more and get free access to SearchLight, visit www.digitalshadows.com.

digital shadows_