

Falcon Shield: SaaS Security for Law Firms

Protect sensitive client information

As the legal industry's reliance on software as a service (SaaS) applications such as DocuSign, Box, Zoom, and Microsoft 365 to manage client files and legal documents increases, so does the need to secure their applications. Failure to do so puts them at risk of lost files and crippling reputational damage when SaaS data is breached or compromised.

CrowdStrike Falcon® Shield provides the widest SaaS application security coverage, with out-of-the-box integrations for over 150 applications that oversee client secrets and store highly sensitive data for extended periods of time. The Falcon Shield SaaS security solution improves the security posture of the entire SaaS stack. It alerts security teams when high-risk configurations are changed, monitors users and devices accessing SaaS applications, and reviews permission settings for every connected third-party app. Most importantly, it detects threats from across the SaaS stack, enabling SOC teams to stay ahead of incidents.

Benefits of SaaS security posture management (SSPM)

- Secure high-risk misconfigurations
- Detect threats from across the SaaS stack
- Identify high-privilege users using low-hygiene devices
- Prevent high-risk connected application access
- Detect and prevent data leakage

Use case spotlight

Document management and data protection

Law firms manage millions of documents, each with unique share settings. Many firms use SaaS applications like DocuSign or Adobe Acrobat Sign to collect approvals and get signatures. A misconfiguration or overshared document could have a significant impact on a business deal, court case, or application. Falcon Shield provides visibility into publicly and externally shared documents. The solution also manages configurations, allowing administrators and security teams to understand the risk brought on by each configuration change.

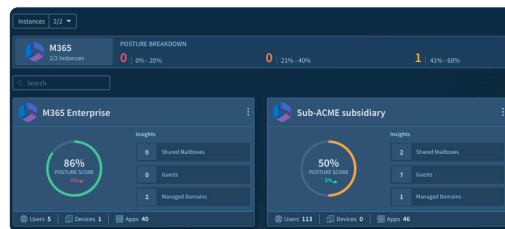


The screenshot displays the Falcon Shield SaaS security interface. At the top, there are four tabs: 'ALL' (12 items), 'NOT ACCESSIBLE' (1 item), 'SaaS RESOURCES' (14 items), and 'PUBLIC RESOURCES' (1 item). Below the tabs is a table with columns: NAME, SOURCE, OWNER, CREATED ON, LAST ACCESSED, and LAST MODIFIED. The table lists several document access events, including 'Download (2/16/2023)', 'Unlabeled Document (2/16/2023)', 'Email Attachment (2/16/2023)', 'File (2/16/2023)', 'Text (2/16/2023)', and 'Text (2/16/2023)'. Each row shows the document name, source (e.g., DocuSign, Adobe Acrobat), owner (e.g., John@sumphades.com, Sandy@sumphades.com), creation date, last accessed date, and last modified date.

NAME	SOURCE	OWNER	CREATED ON	LAST ACCESSED	LAST MODIFIED
Download (2/16/2023)	DocuSign	John@sumphades.com	Mar 9, 2023	1 Month ago	1 Month ago
Unlabeled Document (2/16/2023)	DocuSign	Sandy@sumphades.com	Feb 23, 2023	4 Weeks ago	1 Month ago
Email Attachment (2/16/2023)	DocuSign	John@sumphades.com	Feb 23, 2023	2 Weeks ago	1 Month ago
File (2/16/2023)	Adobe Acrobat	John@sumphades.com	Jan 4, 2023	2 Weeks ago	2 Months ago
Text (2/16/2023)	DocuSign	Sandy@sumphades.com	Dec 25, 2022	N/A	N/A
Text (2/16/2023)	DocuSign	John@sumphades.com	Dec 25, 2022	3 Weeks ago	6 Months ago

Multi-tenant applications

When law firms merge or are acquired, they often have multiple tenants of the same SaaS apps. With Falcon Shield, users can view the posture of each tenant, allowing them to compare settings and posture, benchmark settings on different instances, and help them meet the firm's company's security and compliance standards.



Permissions management

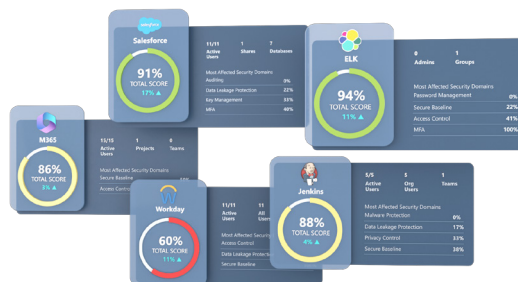
Applications like Salesforce frequently contain sensitive client information, including case files. The application's permission structure is complex, with multiple layers of permission sets, profiles, and custom permissions. This makes it nearly impossible to see which paralegals, assistants, and lawyers have access to sensitive information. Falcon Shield's permissions inventory allows law firms to easily see the level of access granted to each employee, the level of access granted to each role, and each permission set from a single screen.

The screenshot shows the 'System Administrator' interface in Falcon Shield. It displays a table of permissions for a specific application (Salesforce). The table has columns for 'ID', 'Sub Type', 'Created On', 'Updated On', and 'Created By'. Below the table, there are sections for 'Users (2)', 'Permissions (184)', and 'Object Permissions (140)'. The 'Object Permissions' section is expanded, showing a list of objects and their corresponding permissions (VIEW, EDIT, DELETE, etc.).

OBJECT	MODIFY	VIEW ALL	DELETE	CREATE	EDIT	READ
ContactPointEmail	✓	✓	✓	✓	✓	✓
PushTopic	✓	✓	✓	✓	✓	✓
ProcessException	✓	✓	✓	✓	✓	✓
CustomSubscriptionCha...	✓	✓	✓	✓	✓	✓
Pricebook2	✓	✓	✓	✓	✓	✓
Customer	✓	✓	✓	✓	✓	✓
ApkKnowledgeEventStore	✓	✓	✓	✓	✓	✓
Survey	✓	✓	✓	✓	✓	✓

Custom and industry application integrations

Law firms often use legal-specific applications to manage cases, documents, billing, and other professional services tasks. With Falcon Shield's integration builder, law firms can secure their entire SaaS stack, continuously manage and control all SaaS apps, and govern all SaaS users and risks associated with their devices.



See your SaaS security posture in minutes

1. Connect SaaS applications via API
2. See initial application security posture scores within minutes
3. Identify high-risk configurations
4. Remediate risk
5. Improve application security posture

[Learn more](#)

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: <https://www.crowdstrike.com/>

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

