TESSIAN

TESSIAN SOLUTIONS BRIEF

Protecting the Legal Sector from Data Loss and Inbound Email Security Threats

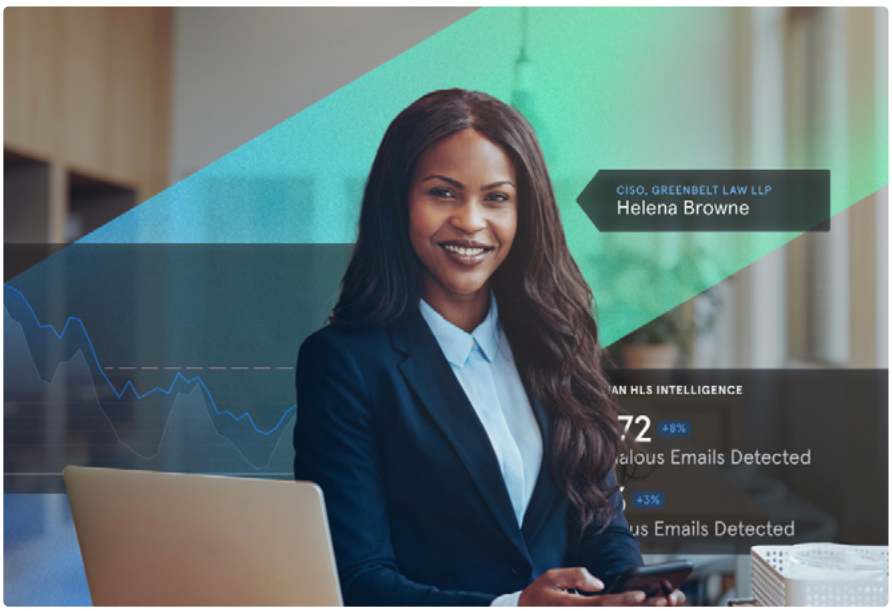
Helping firms detect sophisticated email attacks, and prevent data loss and exfiltration, with no disruption to employee workflows.

Inbound and Outbound Email Security for Law Firms

Law firms operate in a fast paced and constantly shifting environment, balancing numerous client projects at a time. Additionally, attorneys conduct the majority of business over email, receiving and sending sensitive client data every day.

Unfortunately, this makes law firms particularly vulnerable to today's email security threats such as phishing attacks that legacy solutions can't detect and more prone to data loss from human error. Professionals in firms have an ethical and legal obligation to protect the confidences of their clients, which may include trade secrets, intellectual property, merger and acquisition details, personally identifiable information (PII), and confidential attorney-client-privileged data.

However, relying on self-reporting of incidents, policies, legacy solutions such as secure email gateways, encryption and employee training does not provide law firms the needed protection and clear visibility into email threats, data exfiltration or employee behavior on email- making it hard to prevent data loss and avoid breaches or stay compliant.



Key Benefits

AUTOMATED THREAT PREVENTION AND REMEDIATION

Contextual machine learning (ML) understands human behavior on email, can predict normal and abnormal email activity, and can start preventing the most advanced threats within hours of deployment. No pre-configuration required.

HOLISTIC VIEW OF HUMAN BEHAVIOR

Tessian maps employee email activity and builds unique security identities for every individual. Tessian dashboards and analytics surface these insights and give full visibility into threats you've never been able to detect before. Now you can predict and preempt security risks caused by unsafe human behavior.

MAKE PEOPLE YOUR STRONGEST DEFENSE

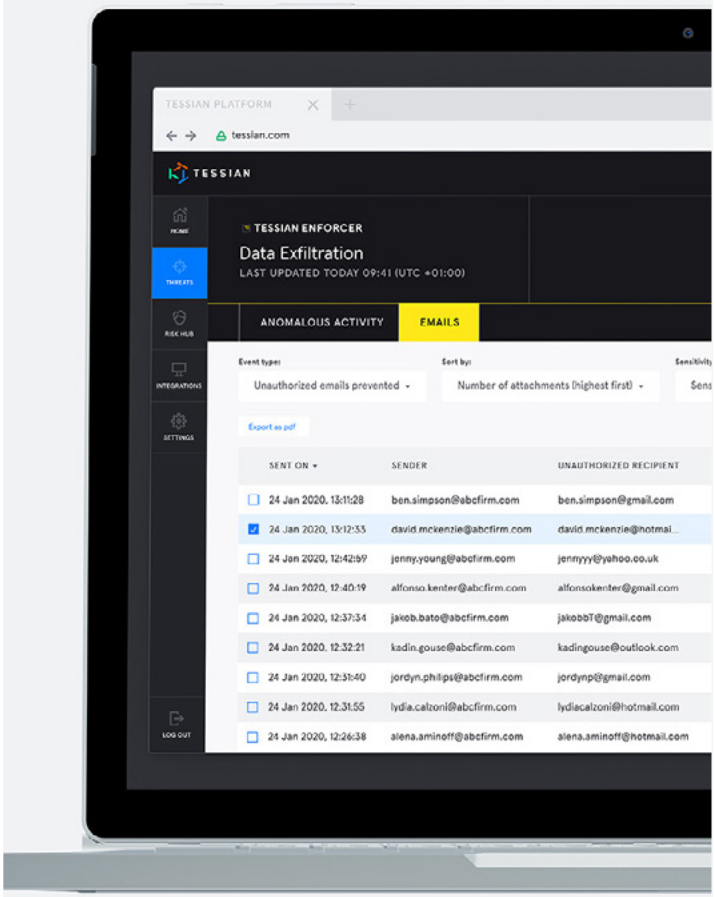
Tessian warnings act as in-the-moment training for employees, continuously educating them about threats, reinforcing your policies, and coaching them toward safe behavior. Take the right educational interventions and targeted remedial actions at scale.

EFFORTLESS AND NON-DISRUPTIVE

Easy to deploy, to manage, and to integrate with any email environment and enterprise security applications.

FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS

Tessian deploys in minutes and automatically prevents data breaches through email within hours of deployment, across all devices, desktop and mobile.



DATA LOSS PREVENTION

Detect and Prevent Insider Threats

Three-fourths (75%) of all security incidents in the legal sector reported to regulators were caused by insiders, both negligent and malicious. With the majority of communication happening over email and working with an incredible amount of sensitive information, law firms are particularly at risk of breach from data loss. Whether a departing partner is stealing client information or an attorney accidentally sends a sensitive attachment to the wrong person, it may result in numerous consequences for the firm.

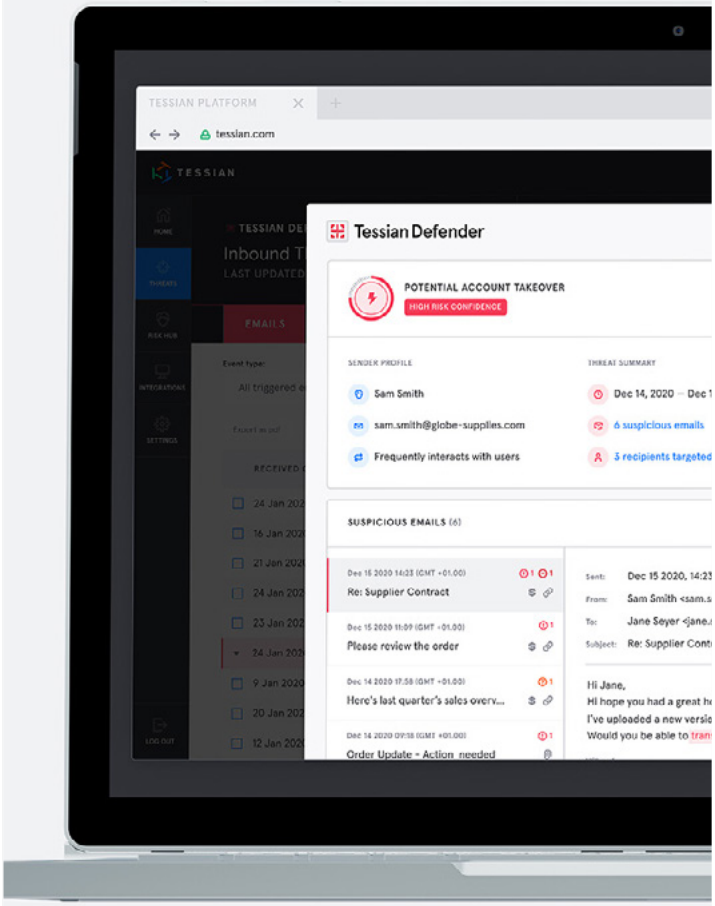
Prevent data breaches involving personally identifiable information (PII), safeguard client data, and help ensure continuous regulatory compliance. Tessian automatically protects sensitive client information by making sure that emails and attachments are only sent to the right people, and detects data exfiltration to personal or unauthorized accounts without the need to create and maintain DLP policies and deny lists.

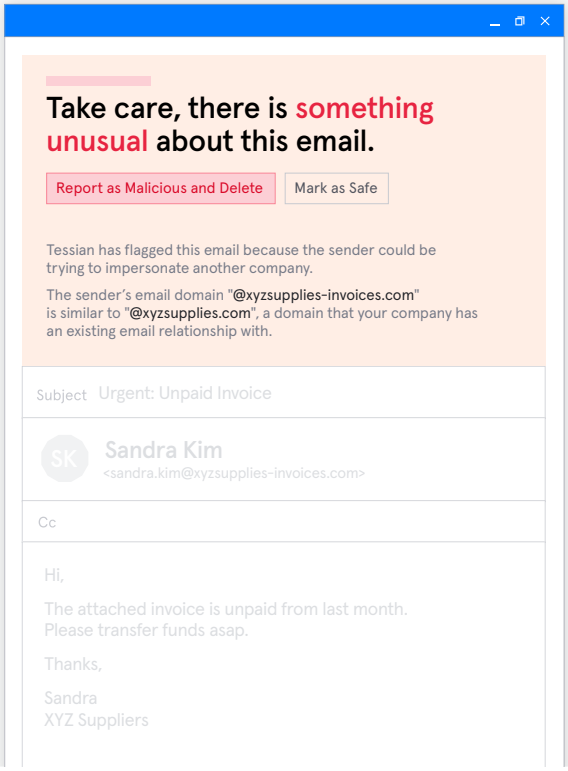
ADVANCED EMAIL SECURITY

Prevent and Remediate Inbound Email Attacks

According to the American Bar Association, around one out of every four law firms is a victim of data breach. The legal sector handles a large amount of sensitive data, making them a frequent target of attacks, such as Phishing and Account Take Over (ATO). ATO threats pose a great danger to firms as hackers use sophisticated impersonation techniques and trusted email accounts to launch attacks that bypass conventional threat detection tools. Successful attacks can result in a variety of consequences including loss of client trust, regulatory fines, and reputational damage. Additionally, there's the wasted hours of senior partners trying to resolve the problems.

Defender protects against both known and unknown email attacks, including Business Email Compromise (BEC), Account Takeover (ATO), spear phishing, and all impersonation attacks (ex. impersonations of the managing partner) that bypass Secure Email Gateways, Microsoft 365, and G Suite.





SECURITY AND AWARENESS TRAINING

Easy to use, Non-disruptive and guides employees towards right security behavior in-the-moment

Disruptions to employee productivity have a large impact on the potential revenue of law firms. Partners need to be able to access their email and communicate with their clients, however, traditional approaches have come at the expense of user experience as unintelligent pop-ups cause user fatigue.

When Tessian discovers anomalies, it displays contextual warning messages with precise flag reasons. And because Tessian warns users only when true events are detected, partners are protected, without disruption to their day-to-day work.

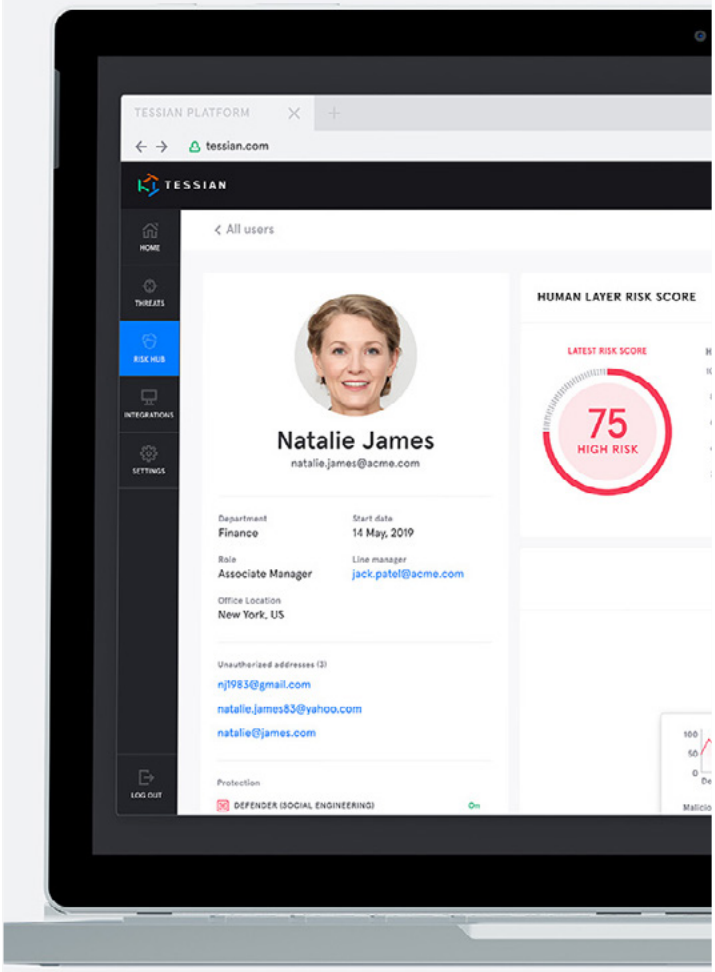
THREAT VISIBILITY AND INTELLIGENT MITIGATION

Holistically Understand Your Human Layer Risk

In order to combat threats within law firms, Security and Risk Management leaders need visibility into key areas of risk. They need to know:

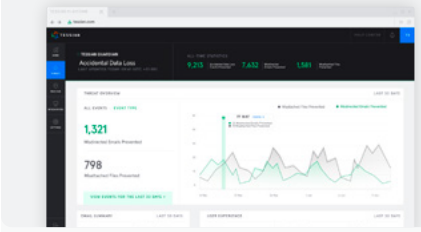
- What kinds of threats are the highest risk in your firm?
- Which partners are most at-risk or likely to make a mistake?
- Where and how can you improve your security stack and improve safer email behavior?

Tessian provides unique insights with enriched risk profiles at the user, department, and company level. With increased visibility into risk areas and drivers, Security and Risk Management teams are able to prioritize mitigation actions and present results to company executives and board members, as evidence of technology reducing risk, not simply reporting it.



TESSIAN CLOUD EMAIL SECURITY PLATFORM

Explore the Cloud Email Security Platform

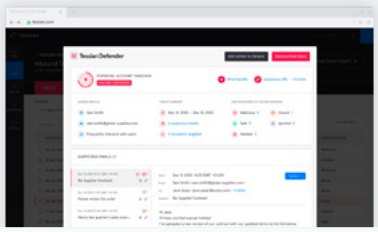


ACCIDENTAL EMAIL DATA LOSS PREVENTION

Guardian

Guardian stops accidental data loss from misdirected emails and misattached files before they happen. Ensure the right email is shared with the right person and prevent data breaches that are impossible to detect with legacy DLP controls.

LEARN MORE ABOUT GUARDIAN →



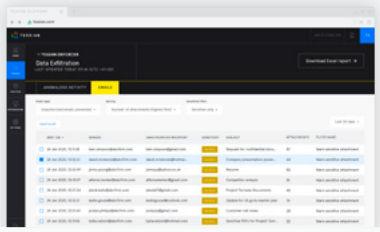
INBOUND EMAIL SECURITY

Defender

A comprehensive inbound email security solution that automatically prevents a wide range of attacks that bypass Secure Email Gateways, while providing in-the-moment training to drive employees toward secure email behavior.

Defender removes the burden on the SOC and admins by automating repetitive tasks such as maintaining triage and review.

LEARN MORE ABOUT DEFENDER→



MALICIOUS EMAIL DATA LOSS PREVENTION

Enforcer

Enforcer automatically prevents data exfiltration over email. Whether it's an employee sending sensitive information to less secure, personal accounts or a bad leaver maliciously exfiltrating information for personal gains, Tessian Enforcer's machine learning model automatically detects data exfiltration and non-compliant activities on emails. No rules required.

LEARN MORE ABOUT ENFORCER →

FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS:

Exchange · Office 365 · G Suite · splunk> · Radar · exabeam · SGS · AICPA SOC · DUO · ALIEN VAULT · RAPID7 · RSA

TRUSTED BY ENTERPRISE CUSTOMERS ACROSS ALL INDUSTRIES:

EVERCORE · arm · HERBERT SMITH FREEHILLS · REALPAGE · affirm · Schroders · rightmove · Investec · GRAPHCORE · sanne · K&L GATES · PeaceHealth · GOCARDLESS · MSCI · ERT · CLYDE&CO · BRACEWELL · RAND MERCHANT BANK · Intertrust · Man Group plc

See Tessian in Action.

Automatically stop data breaches and security threats caused by employees on email.

REQUEST A DEMO →

TESSIAN

Tessian is a leading cloud email security platform that intelligently protects organizations against advanced threats and data loss on email, while coaching people about security threats in-the-moment. Tessian's intelligent approach not only strengthens email security but also builds smarter security cultures in the modern enterprise.