TESSIAN

OUTBOUND EMAIL SECURITY

An Essential Part of Law Firms' Data Loss Prevention (DLP) Strategies

Tessian automatically prevents both accidental data loss and data exfiltration on email to help ensure law firms keep sensitive information safe.

TRUSTED BY 150+ LAW FIRMS:

K&L GATES · DAC BEACHCROFT · BRACEWELL · TRAVERS SMITH · fieldfisher · Allens › ‹ Linklaters · Shearman & Sterling · HERBERT SMITH FREEHILLS · PENNINGTONS MANCHES COOPER · HILL DICKINSON

INBOUND THREATS ARE TOP OF MIND FOR SECURITY LEADERS WORKING IN THE LEGAL SECTOR.

800
misdirected emails are sent every year in organizations with 1,000+ employees

34%
of employees working in the legal sector admit to exfiltrating data before leaving a job

27,500
unauthorized emails are sent in organizations with 1,000 employees per year

85%
of security leaders say rule-based DLP is admin-intensive

Download The State of Data Loss Prevention in Legal Services →

WHY LAW FIRMS CHOOSE TESSIAN OVER OTHER SOLUTIONS:

No Rules Required

Unlike other DLP solutions, Tessian doesn't rely on manual data classification, pre-defined rules, or blacklists because you can't define and predict human behavior with rules. Instead, powered by machine learning, Tessian maps employee relationships to automatically determine whether an email is suspicious or unusual. This means effective, continuous, adaptive email security on desktop and mobile that's hands-off for security teams.

Unique Risk Insights

Security teams can easily view trends over time to identify their most risky users without looking through spreadsheets containing thousands of events. With these insights, customers can identify potential insider threats or negligent employees and take targeted action directly in the portal and outside of the portal before it's too late.

Learn more about Tessian Human Layer Risk →

Education and Awareness

When Tessian detects misdirected emails, misattachments, or data exfiltration attempts, a warning message is triggered, explaining exactly why the email was flagged in plain English. This helps reinforce existing policies around data handling, bolsters security awareness training, and drives employees towards safer behavior on email long-term.
Low rates of false positives mean warnings are helpful, not annoying like standard pop-ups.

DEPLOYS WITHIN MINUTES → LEARNS WITHIN HOURS → STARTS PROTECTING IN A DAY

WHAT OUR CUSTOMERS ARE SAYING:

HERBERT SMITH FREEHILLS

5000 EMPLOYEES

"ML-powered security technology like Tessian produce better results and offer a better return than pop-ups or noisy, rule-based DLP, especially for smaller teams like mine. The opportunity to 'set-it-and-forget-it' is huge."

Jamie Travis
HEAD OF INFOSECURITY
HERBERT SMITH FREEHILLS

"Trying to train human error out of employees is near impossible. Tessian's machine intelligence plays a vital role in helping mitigate these kinds of errors and ensure that customer data remains secure and private."

Chris White
GLOBAL CIO
CLYDE & CO

CLYDE&CO

4000 EMPLOYEES

DAC BEACHCROFT

2500 EMPLOYEES

"In the legal sector, time is money. So disturbing our partners unnecessarily isn't going to go down well. Tessian enables us to protect employees and data, without making their jobs harder to do."

David Aird
IT DIRECTOR
DAC BEACHCROFT

"Before we adopted Tessian's technology, we didn't believe we had any problems with misdirected emails. After a pilot, we realized that was only because these issues weren't being reported. We can see ROI in one email."

Andrew Cheung
PARTNER AND GENERAL COUNSEL
DENTONS

大成 DENTONS

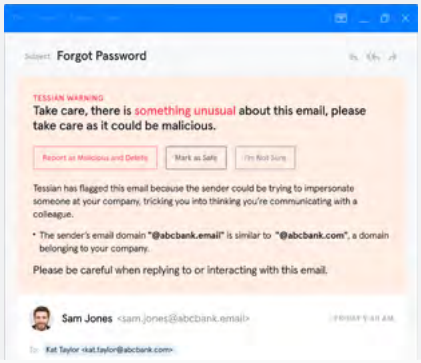
1550 EMPLOYEES

PENNINGTONS MANCHES COOPER

1000 EMPLOYEES

"Tessian is doing the heavy lifting for us now. We're no longer looking through spreadsheets with hundreds or thousands of events. With Human Layer Risk Hub, we get incredible visibility within the portal into high-risk users and high-risk events."

Richard Mullins
IT SECURITY ENGINEER
PENNINGTONS MANCHES COOPER

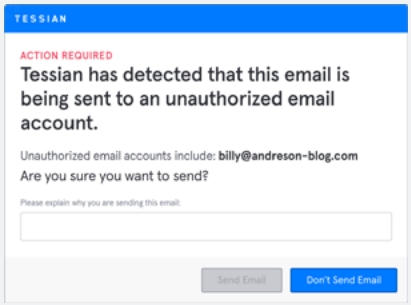


PREVENT ACCIDENTAL DATA LOSS

Tessian Guardian

As misdirected emails and incorrect attachments are detected, employees are alerted in real-time with clear, simple explanations and precise reasons for anomalies and correct recipients are suggested. This way, they can correct the recipient(s) and review attachments before the email is sent.

LEARN MORE →

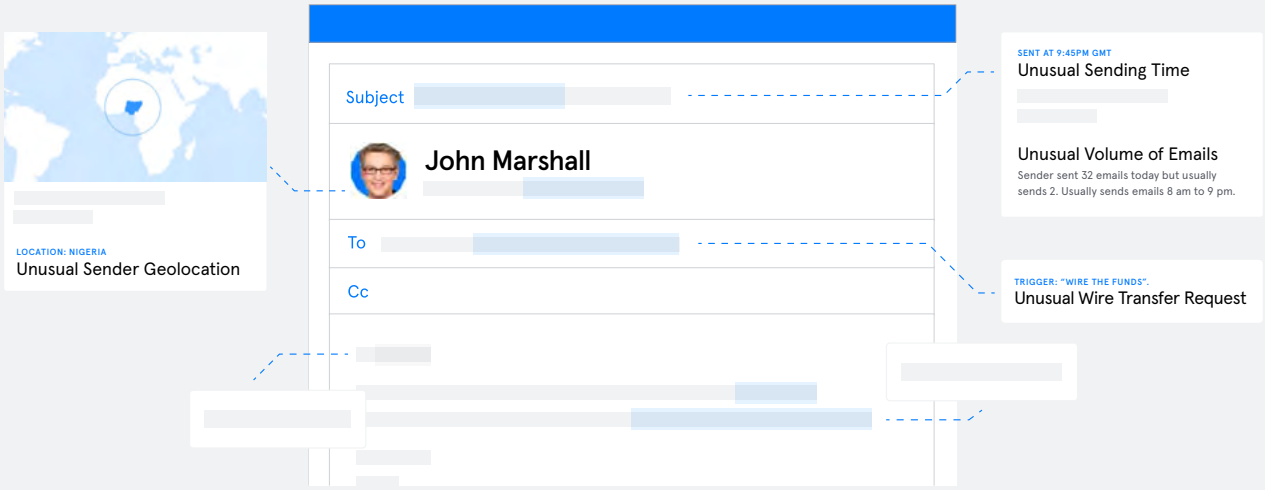


PREVENT DATA EXFILTATION

Tessian Enforcer

Real-time warnings are shown to employees when data exfiltration threats are detected. Warning triggers can be tailored to suit your company's security policies and workflow requirements; employees can be warned, emails can be blocked, or activity can be silently tracked.

LEARN MORE →



See how you can turn your email data into your biggest defense against outbound data loss.

REQUEST A DEMO →

TESSIAN | Human Layer Security

TESSIAN.COM

Tessian's mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error – like data exfiltration, accidental data loss, business email compromise and phishing attacks – with minimal disruption to employees' workflow. As a result, employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like Sequoia, Accel, March Capital, and Balderton and has offices in San Francisco and London.