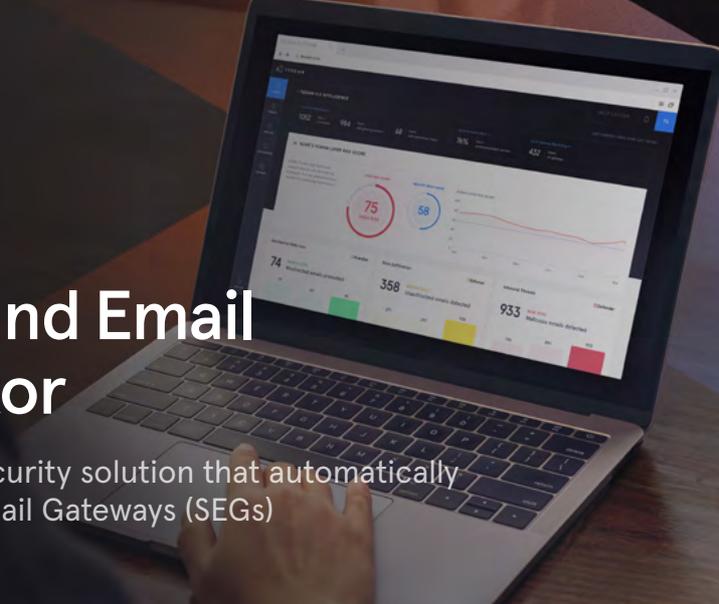




INBOUND EMAIL SECURITY IN LEGAL SERVICES

An Essential Layer of Inbound Email Security For the Legal Sector

Tessian Defender is a comprehensive inbound email security solution that automatically prevents a wide range of attacks that bypass Secure Email Gateways (SEGs)



TRUSTED BY 150+ LEADING LAW FIRMS:

K&L GATES

DENTONS

DAC BEACROFT

BRACEWELL

TRAVERS SMITH

CLYDE&CO

fieldfisher

Allens > Linklaters

EVERSHEDS SUTHERLAND

Shearman & Sterling

HERBERT SMITH FREEHILLS

PENNINGTONS MANCHES COOPER

HILL DICKINSON

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

43%

Of breaches in the last year involved phishing.

VERIZON

95%

Of phishing attacks arrive via email.

VERIZON

12.5BN

Spear phishing has cost global businesses \$12.5bn in losses.

FBI

+2,000%

BEC incidents have increased by nearly 2,000% since 2018.

VERIZON

While businesses across industries are vulnerable, law firms are especially lucrative targets. They handle an incredible amount of sensitive information and high-value payments on behalf of the firm and its clients.

WHY LAW FIRMS CHOOSE TESSIAN OVER OTHER SOLUTIONS:



Threat Prevention

Tessian Defender keeps critical client data safe by **automatically** detecting and preventing **Business Email Compromise (BEC)**, **Account Takeover (ATO)**, spear phishing, and impersonation attacks **on both desktop and mobile**. These advanced email attacks slip past SEGs, Microsoft 365, and G Suite and could result in financial loss, lost client trust, and a damaged reputation.

[Is Your O365 Email Secure? →](#)



Education and Awareness

When **Tessian Defender** detects potentially malicious emails, warning messages written in plain English offer context and explain exactly why the email was flagged. This helps reinforce security awareness training and helps improve lawyers' security reflexes over time, without impeding on productivity.



Reduce Admin Overhead

Tessian Defender seamlessly integrates with existing email security controls and removes the burden on IT and security teams. Repetitive and time-consuming tasks are automated and human verification isn't required. No more maintaining complex sets of rules, establishing pre-defined policies/configurations, or manually investigating potential threats.

[See all Tessian Integrations →](#)

DEPLOYS WITHIN MINUTES



LEARNS WITHIN HOURS



STARTS PROTECTING IN A DAY

WHAT OUR CUSTOMERS ARE SAYING:



2500 EMPLOYEES

"Tessian does what it says it does. Since deployment, we've seen a massive drop in security incidents and a massive drop in our risk."



David Aird
IT DIRECTOR
DAC BEACHCROFT LLP

"It just works. It is the only tool I've implemented that has had nothing but a positive response from lawyers."



Ed Terry
MANAGER OF INFORMATION SECURITY
CAPLIN & DRYSDALE



150 EMPLOYEES

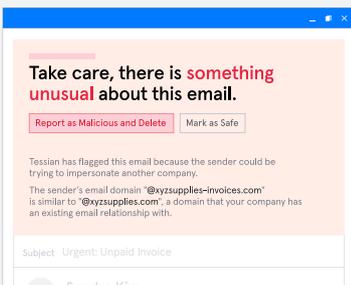


5000 EMPLOYEES

"We invested in Tessian because training and awareness are especially important to us. We want to give our employees the knowledge and confidence to make the right decisions. Tessian's warnings offer people the right information at the right time, rather than being noisy and ineffective like other pop-ups."



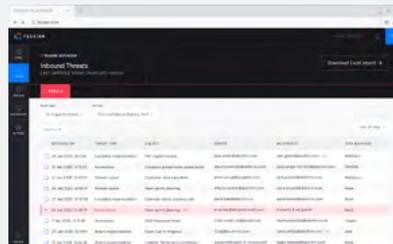
James Travis
HEAD OF INFOSECURITY
HERBERT SMITH FREEHILLS



Comprehensive Coverage

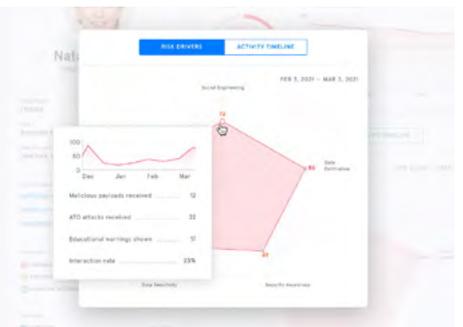
The most advanced threats bypass legacy solutions, leaving people as the last line of defense. But people are stressed and distracted, and bad actors carefully craft emails to dupe targets. Tessian automatically prevents internal and external impersonation, including whaling, CEO Fraud, and ATO.

[Learn more about ATO Protection →](#)



Bulk Remediation

Tessian Defender automatically quarantines emails determined to be highly malicious and allows admins to bulk-remediate malicious emails in 1 click. Delete suspicious emails in users' inboxes directly from the portal and thwart burst attacks by deleting entire campaigns from users' inboxes.



Unique Risk Insights

Security teams can view top threats, top target users, and a detailed breakdown of anomalous events detected by Tessian Defender. And, with granular visibility of employee behavior, you can quantify risks, compare trends, and benchmark your security posture against other firms in the legal sector.

[Learn more about Tessian Human Layer Risk Hub →](#)

WHAT OUR CUSTOMERS ARE SAYING:



1500 EMPLOYEES

“Tessian is a security product that’s about the people. It’s about engaging people and making security intrinsic to what they do, without getting in their way.”



Mark Parr

GLOBAL INFOSECURITY MANAGER
HFW

“Security products should only be seen when there is a security issue, while also playing a role in better educating users about security risks. With Tessian, we can be confident that employees won’t see notifications unless it really matters.”

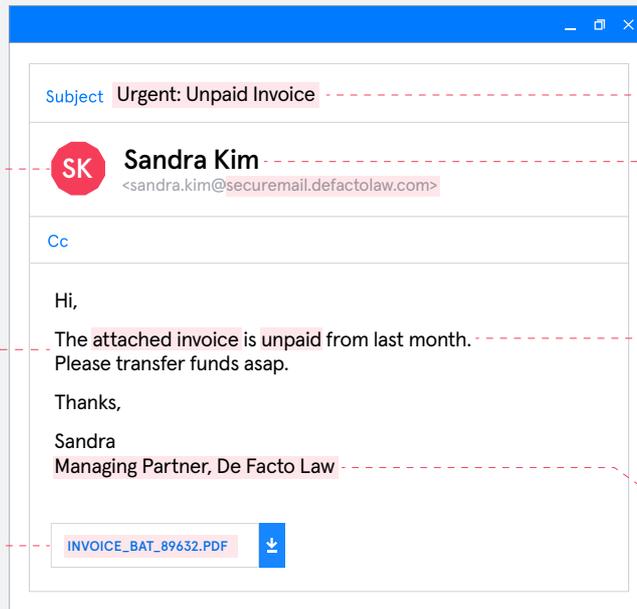


Ara Margossian

TECHNOLOGY AND SECURITY STRATEGY PARTNER
WEBB HENDERSON



200 EMPLOYEES



See how you can turn your email data into your biggest defense against inbound email attacks.



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 and Balderton and has offices in San Francisco and London.