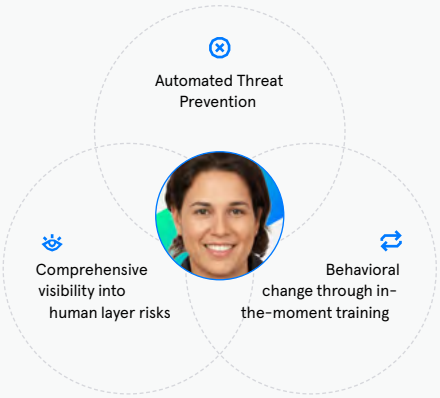
TESSIAN

PROTECT YOUR PEOPLE

Human Layer Security Platform Overview

Tessian is the world's only Human Layer Security platform that automatically stops data breaches and security threats caused by employees on email.



How are you preventing Human Layer Security threats?

Human error is the primary root cause of data breaches over email. To prevent today's email threats, security controls must understand human behavior, and security and IT teams must have clear visibility into their human layer threats.

Tessian uses machine learning technology to uniquely address the risks posed by employees.

WE DO THIS BY:

Providing comprehensive visibility into your human layer risks.

Automatically detecting and preventing threats like accidental data loss, data exfiltration, and advanced phishing attacks (that legacy solutions can't detect).

And more importantly, we change behavior: we continuously drive your employees toward secure email behavior through contextual, in-the-moment training.

All of these together continually reduce security threats at the human layer and strengthen your organization's security posture. This is all done with no disruptions to your employees' productivity.

Tessian deploys within minutes, learns within hours and starts protecting in a day.

Platform 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 24 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 nudging 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. You can set it and forget it, or partner with Tessian's dedicated team of security experts to optimize for your environment. Tessian is invisible to employees until they need it.

Tessian Human Layer Security Platform Modules

PEOPLE MAKE MISTAKES →

TESSIAN GUARDIAN

Accidental Data Loss

Prevent misdirected emails and misattached files.

PEOPLE BREAK THE RULES →

TESSIAN ENFORCER

Data Exfiltration

Prevent unauthorized emails.

TESSIAN CONSTRUCTOR

Prevent non-compliance and data loss using custom policies.

PEOPLE CAN BE TRICKED →

TESSIAN DEFENDER

Impersonation Attacks

Prevent spear phishing, BEC, and other impersonation attacks.

OUTBOUND DATA LOSS

INBOUND EMAIL SECURITY

HLS INTELLIGENCE

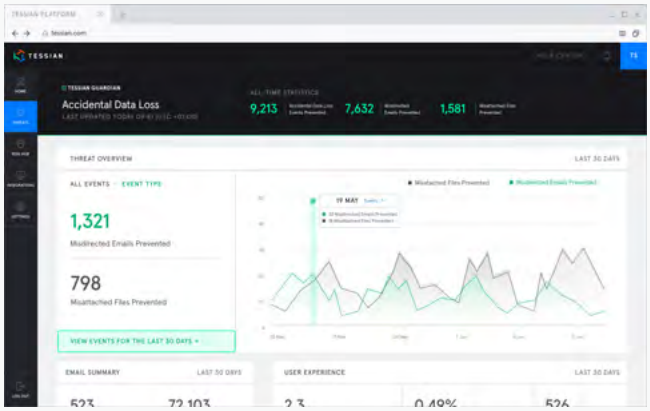
Insights, Investigation and Remediation

Intelligence to investigate, remediate, and reduce human layer risks.

HUMAN LAYER RISK HUB

Risk Management and Reporting

Rapid threat investigation and proactive risk mitigation.

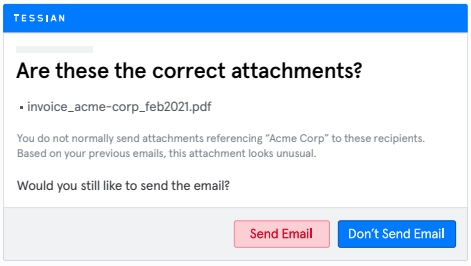


Tessian Guardian

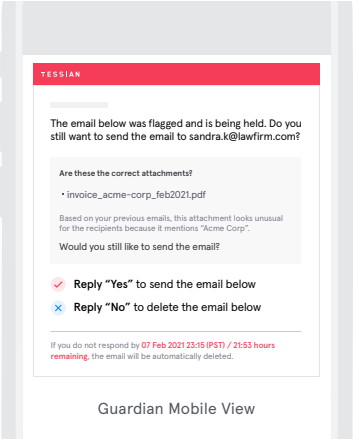
OUTBOUND DATA LOSS

Tessian Guardian is the industry's only solution that automatically prevents accidental data loss from misdirected emails and misattached files (sending wrong attachments over email).

Guardian compares millions of data points for every outbound email and detects anomalies that indicate whether the email is being sent to the wrong person or if a wrong document is being attached and alerts the user before the email is sent.



Guardian Desktop View



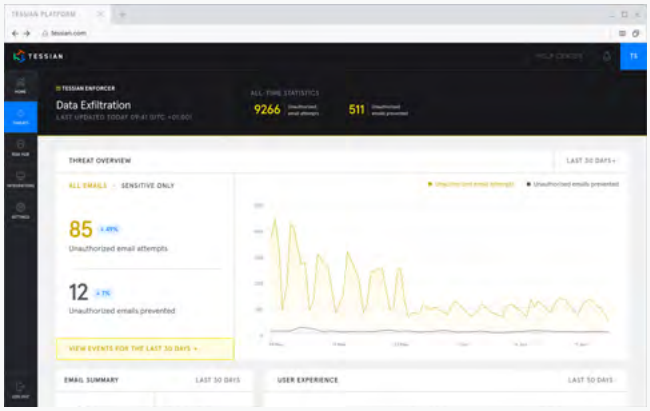
Guardian Mobile View

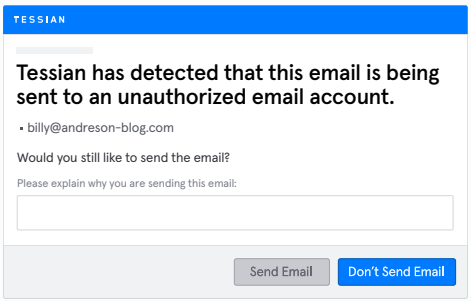
Tessian Enforcer

OUTBOUND DATA LOSS

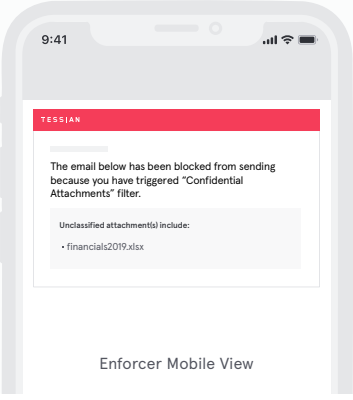
Tessian Enforcer is the industry's first solution that uses machine learning to automatically prevent data exfiltration via email to employee personal, unauthorized and non-business accounts.

Powered by Tessian's proprietary Human Layer Security Engine, Enforcer analyzes millions of data points for every outbound email and detects anomalies that indicate data exfiltration before it leaves your organization. Tessian Enforcer notification messages can be customized to reinforce security awareness and data protection policies through in-the-moment training.

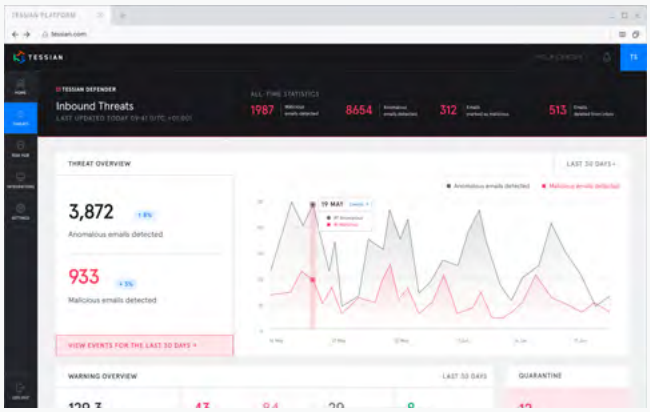




Enforcer Desktop View



Enforcer Mobile View

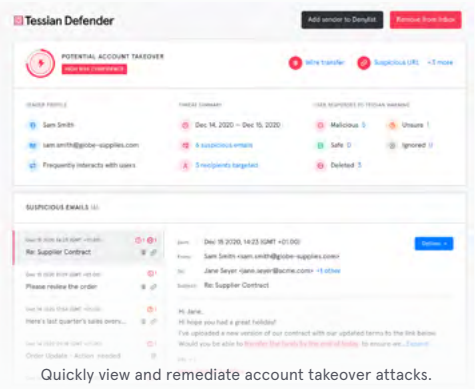


Tessian Defender

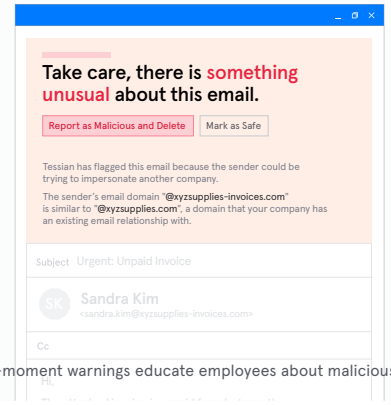
INBOUND EMAIL SECURITY

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

- Protect against both known and unknown email attacks, including business email compromise, account takeover, spear phishing, and all impersonation attacks that bypass SEGs, M365, and G Suite.
- With Defender's in-the-moment training, organizations can educate and empower users to build continuous email security awareness.
- Remove the burden on your Security Operations Center and admins by automating repetitive tasks such as maintaining triage and review. This eliminates the need for human verification of email threats, reducing FTE requirements.



Quickly view and remediate account takeover attacks.



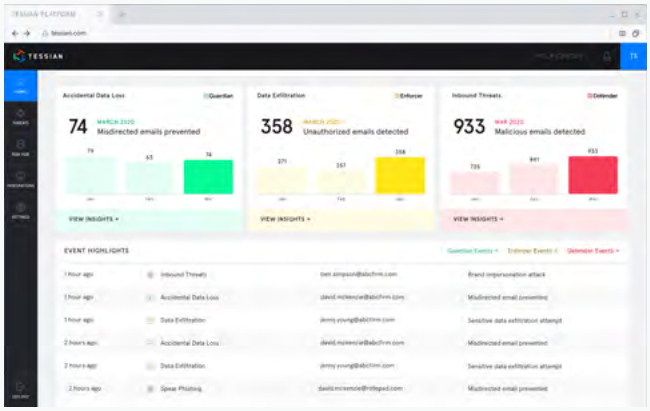
In-the-moment warnings educate employees about malicious emails.

Tessian HLS Intelligence

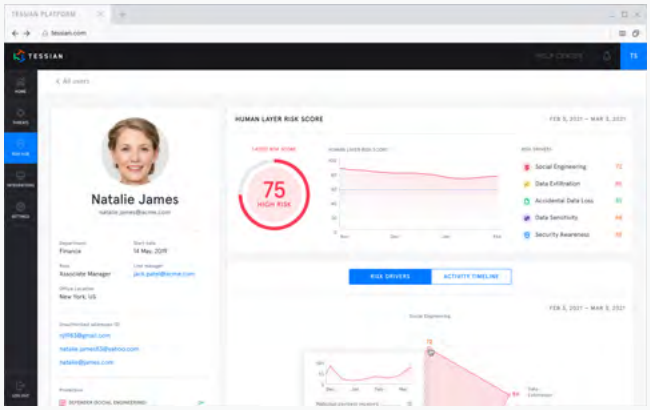
INVESTIGATE AND REMEDIATE

With Tessian HLS Intelligence, security teams can now readily view curated security events prevented by Tessian with detailed threat breakdowns, make informed prioritization decisions, and respond to threats faster while benchmarking risks against industry peers.

- Insights: Automated insights by inbound and outbound threat categories where you can view top threats and trends, and benchmark against peers.
- Investigation: Detailed event logs and threat breakdown, curated event priorities, and API integrations to connect to your SIEM/SOAR platforms.
- Remediation: Quarantine and post-delivery protection, automated domain blacklisting from shared threat intelligence, and rule-free, single-click domain blacklisting.



Tessian Human Layer Risk Hub



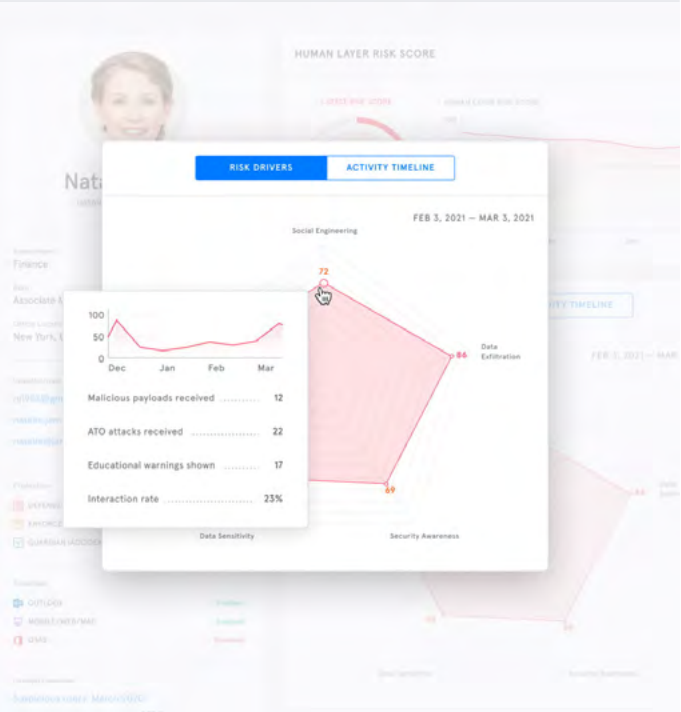
INVESTIGATE AND REMEDIATE

Tessian's Human Layer Risk Hub enables security and risk management leaders to deeply understand their organization's email security posture by providing granular visibility and reporting into individual user risk levels and drivers.

With the Human Layer Risk Hub, SRM leaders will be able to quantify risk levels, pinpoint their high risk user groups, perform targeted remediation at scale, measure impact and demonstrate progress in lowering risks posed by employees.

THE HUMAN LAYER RISK HUB OFFERS:

- Unified Risk View: Email security, training, and risk analytics are offered all in one platform. It delivers a broad spectrum of risk analytics across outbound and inbound email threats and hard to solve problems such as accidental data loss, data exfiltration and advanced phishing attacks, with laser focus on the human layer.
- Unique Risk Insights: Enriched individual risk profiles that are modeled with a broad range of signals from email usage patterns, relationship graphs, security decisions in real time as well as from historical emails. Because of this unique data modeling, Tessian provides a profile that is contextually rich from day 1 of deployment.
- Defensible Audit: Detailed reporting and audit logs provide defensible proof against data breaches. If risk is identified, Tessian's Human Layer Risk Hub enables you to formally document all associated events such as exposure, owner, mitigation decisions and actions.



TESSIAN PROTECTS ENTERPRISE ORGANIZATIONS JUST LIKE YOURS:

Evercore · arm · Prudential · RealPage · affirm · Schroders · rightmove · Investec · Graphcore · sanne · K&L Gates · cordaan · Dentons · MSCI · ERT · Clyde&Co · Bracewell · gubra · Intertrust · ManGroup plc

See Tessian in action. Automatically stop data breaches and security threats caused by employees on email.

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.