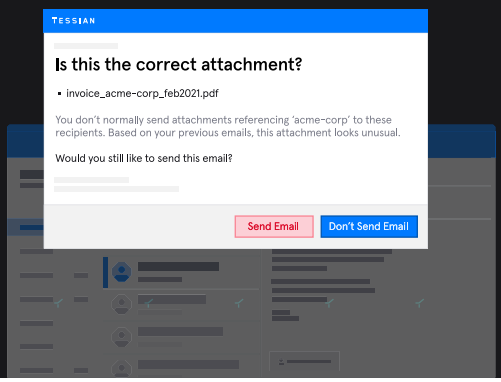
TESSIAN



Tessian Guardian

OUTBOUND EMAIL PROTECTION

Stop Accidental Data Loss Caused by Misdirected Emails and Misattached Files.

Misdirected emails are the number one data security incident reported to data protection regulators across the world. Every day, inadvertent human error on email leads to organizations putting their customer's data at risk, breaching mandatory industry and data protection regulations and losing mission-critical intellectual property.

TESSIAN GUARDIAN is the industry's first and only solution that automatically prevents accidental data loss from misdirected emails and misattached files (sending wrong attachments over email). Powered by Tessian's proprietary Human Layer Security Engine, 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.

Unlike security controls that provide unintelligent and repetitive pop-up notifications which cause alert fatigue, Guardian only shows warning notifications to employees when anomalies are detected. Tessian Guardian keeps notification rates low and provides contextual information that reinforces security awareness and data protection policies through in-the-moment training.

Key Benefits

EFFECTIVE ACCIDENTAL DATA LOSS PREVENTION

- Automatic protection using machine learning. No predefined rules required
- Prevent accidental data loss from misdirected emails, which are impossible-to-detect with legacy DLP controls
- Stop emails with incorrect attachments that can expose classified and sensitive commercial data to unintended recipients
- Safeguard your intellectual property, comply with customer confidentiality agreements, and eliminate the risk of reputational damage
- Meet GDPR, CCPA, HIPAA, and other mandatory data protection regulations
- No behaviour change required for employees; minimal end user disruption and zero admin for security teams
- Reinforce security awareness and data protection policies through in-the-moment training

Key Features

ENTERPRISE GRADE SECURITY

Tessian is used by world leading organizations across healthcare, finance, legal, and technology industries that look for best-in-class security.

POWERED BY MACHINE LEARNING

Provides continuous, adaptive email security.

REAL-TIME ANALYSIS OF EMAILS

Uses our proprietary Human Layer Security Engine that detects anomalies in real-time based on insights from relationship graphs, external data sources, email content and user behavior.

Attachment scanning, deep content inspection and entity relationship anomaly detection to prevent sending wrong attachments in emails.

CONTEXTUAL WARNING MESSAGES

Real-time contextual warning messages are shown before emails are sent with clear and precise reasons on anomalies detected.

FLEXIBLE CONFIGURATION OPTIONS

Enable specific use cases to fit organization's needs and manage user experience.

TESSIAN HLS INTELLIGENCE BUILT-IN

Provides insights, automated intelligence, and detailed reports of misdirected emails/wrong attachments and data breaches prevented.

COMPREHENSIVE PROTECTION

Secures all outbound emails sent across any email client (Desktop, Mobile, Web etc.) with the same consistent analysis.

DEPLOYS IN MINUTES

Automatic protection within 24 hours of deployment based on Tessian's learning from pre-existing historical email.

SECURES ALL ENTERPRISE EMAIL ENVIRONMENTS

Exchange Office 365 G Suite

EFFORTLESS FOR SECURITY, IT, AND COMPLIANCE TEAMS

Security and Compliance Teams:

- Prevent data breaches from misdirected emails and misattached files before they happen (rather than investigate incidents after a breach)
- Proactively stop the exposure of sensitive data arising from misdirected emails and wrong attachments.
- Guardian helps organizations stay compliant and avoid regulatory fines
- Machine learning system is always up to date through continual analysis of your email network
- Get visibility into data breaches prevented due to misdirected emails and misattached files, helping to trend down your organization's data loss risks

IT Teams:

- Integration with your existing email stack in minutes
- No ongoing maintenance or configuration needed
- No MX record changes
- Layers on top of all existing Secure Email Gateways and email security controls
- Invisible to the end-user until potential misdirected emails or wrong attachments are detected

How Tessian Guardian Tackles the Problem of Misdirected Emails:

Establish employee relationship graphs with historical email data.

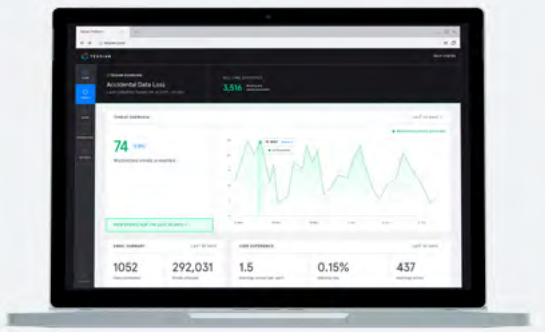
Tessian analyzes historical email data to understand normal content, context, and communication patterns for every single employee in your organization. Relationship graphs are continuously updated as email behavior changes over time.

Perform real-time analysis of emails before sending and detect anomalies.

Tessian's Human Layer Security Engine analyzes all outbound emails in real-time and uses machine intelligence to automatically predict accidental data loss on email based on insights from the relationship graph, external data sources, deep inspection of the email content, and previous user behavior.

Automatically prevent accidental data loss and misdirected emails.

As misdirected emails are detected, employees are alerted in real-time with clear, simple explanations and precise reasons for anomalies. This way, they can correct the recipient(s) before the email is sent. Employee interactions are also logged for inspection in the Tessian dashboard.



Get visibility into breaches prevented and quickly take remedial actions with Tessian HLS Intelligence.

Built within the HLS platform, security teams can seamlessly access insights and automated intelligence behind security events and significantly reduce incident investigation time and delays in mitigation efforts. Quantify the risk, compare trends, benchmark against peers and more. Tessian API integrations allow security teams to centralize and orchestrate events from your SIEM/SAOR platforms. Learn More →

See how you can turn your email data into your biggest defense against misdirected emails.

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 and Balderton and has offices in San Francisco and London.