Tessian has blocked this email because it includes unauthorized recipient(s).

This is not permitted by your organization.

OK

Tessian Enforcer

OUTBOUND EMAIL PROTECTION

Automatically Stop Sensitive Data Exfiltration Over Email.

64% of employees admitted to forwarding work emails to their personal accounts.[1]

Whether it's an employee negligently sending emails to insecure personal email accounts to work on at home or a disgruntled employee maliciously stealing company intellectual property for personal gain while exiting the company, data exfiltration is a major problem in today's business environment.

Traditional approaches to prevent data exfiltration on email rely on manual data classification, a litany of pre-defined rules blacklists and retrospective incident investigation. Tackling the problem of data exfiltration by manually maintaining blacklists in a world of innumerable new

freemail and personal domains is a losing game. Relying on machine based RegEx classification for sensitive content detection or human-in-the-loop quarantine leads to false positives, false negatives and significant administrative burden.

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 analyses 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-situ training.

Key Features

ENTERPRISE GRADE SECURITY
Tessian is used by world leading organizations across healthcare, finance, legal and technology and holds the highest standards of security certification.

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.

AUTOMATIC MAPPING
Automatically maps every employee's business and non-business (personal) email accounts.

FIT TO YOUR INTERNAL POLICIES
Block emails, warn users, or silently track data exfiltration events.

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

TESSIAN HLS INTELLIGENCE BUILT-IN
Provides insights, automated intelligence and detailed reports of email data exfiltration 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

Key Benefits

EFFECTIVE DATA EXFILTRATION PREVENTION

- Automatic protection using machine learning. No pre-defined rules or blacklists required.
- Prevent email data exfiltration events that are impossible to detect with legacy DLP controls.
- Instant visibility into high risk data exfiltration events, trends, and threat actors to take immediate remedial actions.

- Safeguard your intellectual property, comply with customer confidentiality agreements and eliminate the risk of reputational damage.
- Meet GDPR, CCPA, and other mandatory data protection regulations.
- Reinforce security awareness and data protection policies through in-situ training.

Security and Compliance Teams:

- Prevent breaches due to data exfiltration on email before they happen (rather than investigate incidents after a breach)
- Get visibility into and quantify data breaches prevented due to data exfiltration and must-have insights to trend down the organization's risks of data exfiltration
- Significantly reduce your security team's investigation workload with automated intelligence behind security events detected by Tessian
- Machine learning system and mapped non-business email accounts are always up to date through continual analysis of your email network

- No behaviour change required for employees, minimal end user disruption and zero admin for security teams

IT Teams:

- Integration to 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 security controls
- Invisible to the end-user until potential data exfiltration is detected

## How Tessian Enforcer Tackles the Problem of Data Exfiltration Over Email:

Automatically detect non-business email accounts with historical email data.

Tessian analyzes historical email data to understand normal content, context and communication patterns, enabling a comprehensive mapping of every employee's business and non-business email contacts. Relationship graphs are continuously updated as email behavior changes over time after Tessian is deployed.


Perform real-time analysis of emails before they're sent to detect data exfiltration.

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.
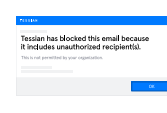
Automatically detect and prevent data exfiltration over email.

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. Employee interactions are also logged for inspection in the Tessian dashboard.
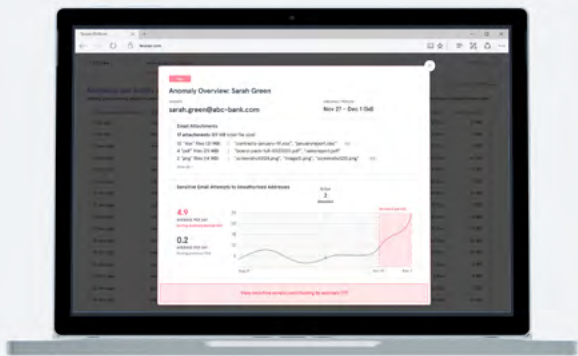
Get visibility into breaches prevented and quickly take remedial actions with Tessian HLS Intelligence

Built within the Tessian HLS Platform, Security teams can seamlessly access insights and intelligence behind security events that significantly reduce manual incident investigation time and allow for rapid response to data exfiltration threats. View threat actors, quantify 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 data exfiltration.

TESSIAN

Human Layer Security

TESSIAN.COM