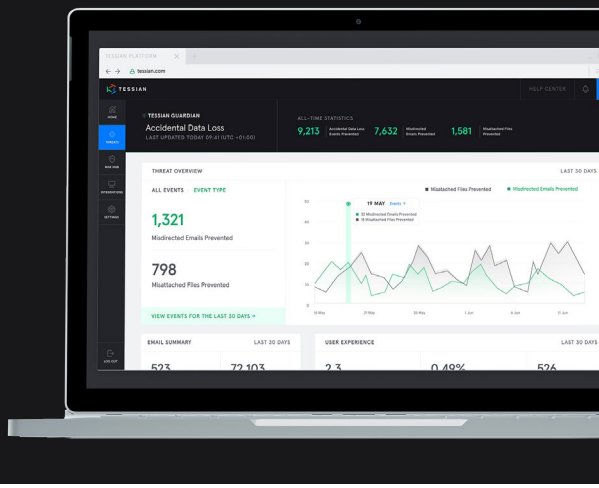
TESSIAN



Tessian Guardian

Stop Accidental Data Loss From Misdelivery or Misdirected Emails

Misdirected emails or email misdelivery is the number one data security incident reported to data protection regulators across the world. Every day, inadvertent human mistakes 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. And it is a huge burden on the security teams. According to a recent Ponemon study, it takes security teams almost 48 hours to detect and remediate an incident caused by employee negligence or error on email.

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).

Tessian uses a behavioral-based approach to detecting accidental data loss on emails. Using behavioral intelligence modeling and machine learning, it analyzes millions of data points for every outbound email and automatically detects anomalies that indicate whether an 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, Tessian Guardian only shows warning notifications to employees when anomalies are detected and provides suggestions to correct their mistakes before email is sent . Tessian Guardian keeps notification rates low and prevents employee's mistakes from turning into security incidents.

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 information 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 behavior change required for employees; minimal end user disruption and zero admin for security teams

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

REAL-TIME ANALYSIS OF EMAILS
Using Behavioral Intelligence Modeling and machine learning

DETECTS AND PREVENTS MISDIRECTED EMAILS
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.

DETAILED SECURITY EVENTS AND AUTOMATED REPORTS
Detailed security events and automated 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

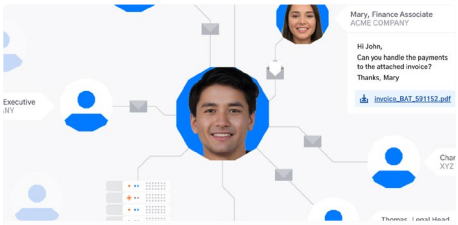
SECURITY AND COMPLIANCE TEAMS:

- Prevent data breaches from misdirected emails and misattached files before they happen (rather than investigate incidents after a breach)
- Reduce the volume of accidental data loss incidents from misdirected emails and wrong attachments that SOC teams need to investigate and remediate. .
- 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:

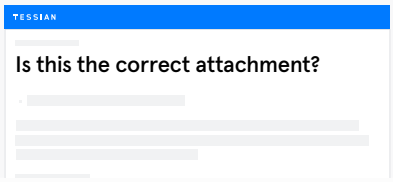
- Integration with your existing email stack in minutes
- No ongoing maintenance or configuration needed
- No MX record changes
- Layers on top of all existing Secure Email Gateways, Microsoft 365, Google Workspace and Exchange
- Invisible to the end-user until potential misdirected emails or wrong attachments are detected

How Tessian Guardian Tackles the Problem of Misdirected Emails and Misattached Files



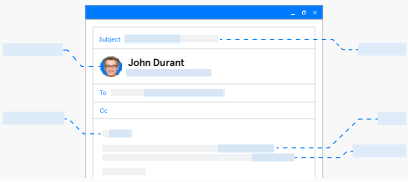
Establish a behavioral intelligence model with historical email data.

Tessian analyzes historical email data to understand content, context, and communication patterns for every single employee in your organization. Behavioral Intelligence models are continuously learning as email behavior changes over time.



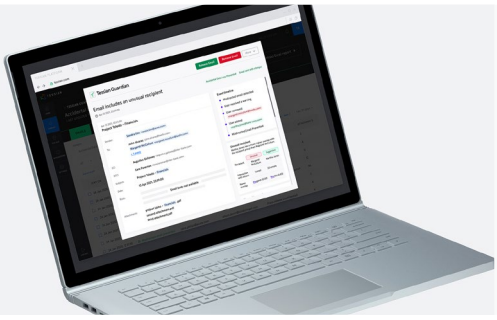
Perform real-time analysis of emails before sending and detect anomalies.

Tessian analyzes all outbound emails in real-time for accidental data loss. Use machine learning and behavioral intelligence modeling 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 from misdelivery or misdirected emails.

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



Get visibility into breaches prevented and remediate with speed.

Tessian allows security teams to seamlessly access insights and automated intelligence for every security event. This significantly reduces incident investigation time and delays in mitigation efforts. Quantify risk, compare trends, benchmark against peers, and more. Use Tessian's cloud open API integrations allow security teams to centralize and orchestrate events from their SIEM/SOAR platforms. Learn More →

See Tessian in Action.

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

REQUEST A DEMO →

TESSIAN

Tessian Cloud Email Security intelligently prevents advanced email threats and protects against data loss, to strengthen email security and build smarter security cultures in modern enterprises.