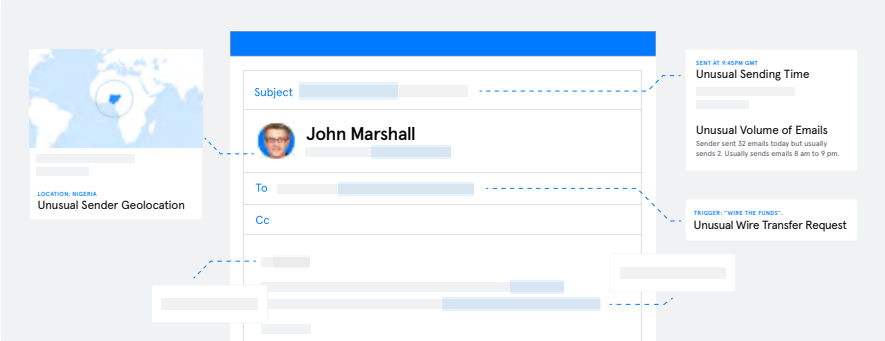
TESSIAN

Tessian Defender

DEFENDER UPGRADE

Stop External Account Takeover with Tessian Defender

Detect and prevent risks originating from compromised email accounts in third-party partner/vendor/customer networks.



Email security is no longer limited to securing an organization's own email platform and its users. There is a growing trend where attackers gain access to the email account of a trusted sender (a customer, a business partner, or a supplier), impersonate the sender and use it to conduct fraudulent activities. This is called Account Takeover (ATO) and it is one of the pathways to Business Email Compromise (BEC)

External ATO attacks have repeatedly demonstrated that rule-based threat detection tools and email authentication (DMARC, DKIM, SPF) are ineffective in detecting and stopping them. This is because these emails originate from trusted external accounts and exploit the trust between business entities and individuals

ATO threats call for a differentiated approach for detecting:

- Anomalous geophysical location, time, IP, email client; impossible to travel locations and unusual reply-to addresses
- Anomalous email sending patterns: Emails sent to an unusual number of recipients, to unusual recipients, and at unusual times
- Suspicious email payloads by spotting language that conveys intent with NLP
- Suspicious URLs (machine learning to identify URL match patterns)
- Suspicious attachments (machine learning to identify common red flags)

TESSIAN DEFENDER offers automated protection against external account takeover threats.

New Defender Features

MACHINE LEARNING-POWERED ANOMALY DETECTION

Tracks user behavior and detects even the most subtle anomalies that might signal an attack at the first instance of an attempt.

MODELING

The Tessian ML algorithm continuously analyzes and learns from email communications across its global network to build profiles / models of companies and their employees to understand what their normal email communication looks like. This helps catch the most subtle ATO attacks.

RAPID REMEDIATION

Real-time alerts of ATO events to dedicated mailboxes. Explainable machine learning helps SOC teams understand quickly why an email has been classified as malicious. By aggregating similar events and grouping emails from the same compromised account, Tessian allows administrators to clawback/ delete multiple events with a single click.

END-USER EDUCATION

Best-in-class email security starts with continuous and contextual employee education. Tessian delivers this with simple, in-the-moment alerts that educate users on secure email behavior.

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

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.