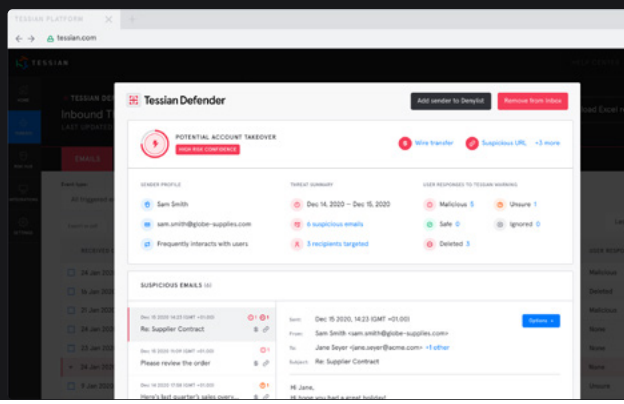
TESSIAN

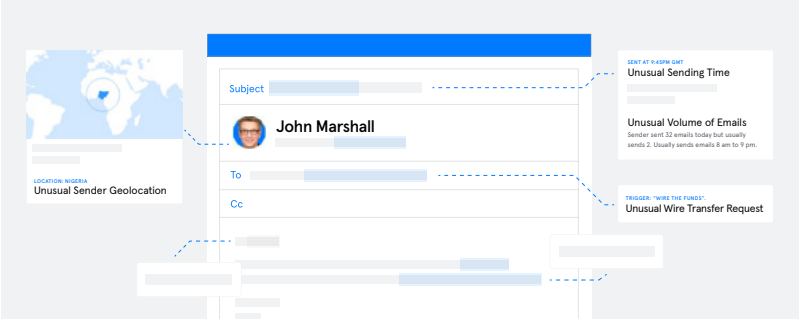
Tessian Defender

INBOUND EMAIL SECURITY SOLUTIONS

Stop Account Takeover with Tessian Defender

Automatically prevent advanced threats originating from compromised third-party supplier, partner and vendor email accounts.





What is External Account Takeover?

Email security is no longer limited to securing an organization's own email platform and its users. In External Account Takeover attacks gain access to the email account of a trusted external counterparty (a customer, a business partner or a supplier), and use it to send email attacks. External Account Takeovers (ATO) are one of the pathways to Business Email Compromise (BEC).

According to Gartner:

- Impersonation and Account Takeover attacks are increasing and causing direct financial loss, as users place too much trust in the identities associated with incoming email and are inherently vulnerable to deception and social engineering.
- The adoption of cloud office systems from Microsoft and Google continues to grow, forcing security and risk management leaders to evaluate the native capabilities offered by products.
- There is no single technology solution to business email compromise (BEC) attacks. Solutions need to be a combination of technology and user education.

Solution Highlights

AUTOMATED THREAT DETECTION

Tessian takes a behavioral based approach to prevent threats. It learns normal behaviors from peoples historical email interactions, and combines this behavioral intelligence of each individual end user,, security intelligence and machine learning to accurately detect even subtle anomalies and prevent ATO attacks.

RAPID REMEDIATION

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

IN-THE-MOMENT SECURITY COACHING

Non-disruptive in-the-moment coaching is provided to employees through contextualized, easy to understand educational alerts guiding them to take the right security decision.

FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS

Defender deploys in minutes and automatically prevents data breaches through email within 24 hours of deployment, across all devices, desktop and mobile. Tessian deployment options protect your cloud, on-premise, or hybrid email deployments.

ACCOUNT TAKEOVER RISKS

Why Account Takeover Attacks Are So Hard to Detect

The battle against phishing has now extended to supply chain networks, third-party business partners, and customers. Bad actors use these trusted third-party accounts to identify their targets and learn relationships as well as communication patterns to maximize their success rates when launching malicious email attacks.

A majority of organizations **remain completely exposed and vulnerable against these highly sophisticated attacks** for a number of reasons:

ATO attacks are extremely difficult to detect.

ATO attacks are sent from legitimate email accounts. As a result, the emails are more 'authentic' than other phishing attacks. Attackers gain access to the sender's email communication history to craft highly sophisticated attacks or continue an ongoing conversation. ATO attacks are thus highly convincing for end users and therefore dangerous.

Legacy systems are not developed to detect ATO cases.

Account Takeover emails will pass email authentication checks like SPF and DMARC which many incumbent tools and SEGs often heavily rely on. Moreover, legacy systems have proved inadequate to detect sophisticated attacks, particularly zero-payload threats.

Companies have no control or visibility over the security of their counterparties.

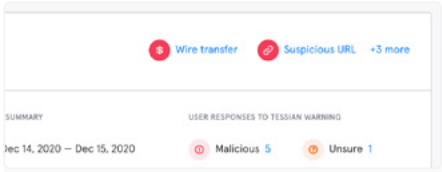
CISOs can try to protect their organizations from attackers, but can't control security measures that their suppliers/clients implement. This means that a company's external network presents an important vulnerability.

Email credential theft is detected too late in the breach cycle.

A key challenge for CISOs is to anticipate, identify, and remediate potential attacks. Without the ability to identify sophisticated social engineering threats, organizations today learn about these attacks only after they have been breached.

SOLUTION DIFFERENTIATORS

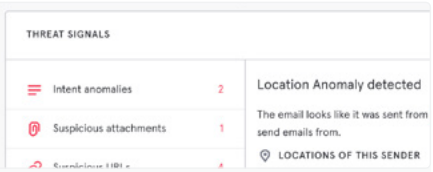
How Defender Detects ATO Cases



Detect Suspicious Payloads

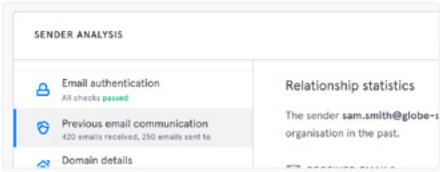
Defender detects suspicious payloads in emails with Natural Language Processing (NLP) to detect:

1. Whether suspicious intents, URLs, or attachments are usual for the sender.
2. Machine-learning models to identify malicious URLs and attachments.



Anomalous Sender Characteristics

Defender uses a variety of signals and detects anomalous sender characteristics like if the sender sent from an unusual location, if the sender used an unusual email client, an unusual reply-to address, or if a bad actor is attempting to make a new email look like a reply to an existing email.



Anomalous Email Sending Patterns

Defender detects anomalies in email relationship patterns, by analyzing signals like if a sender sends to never-seen-before recipients, sends an unusually high number of emails or at an unusual time.

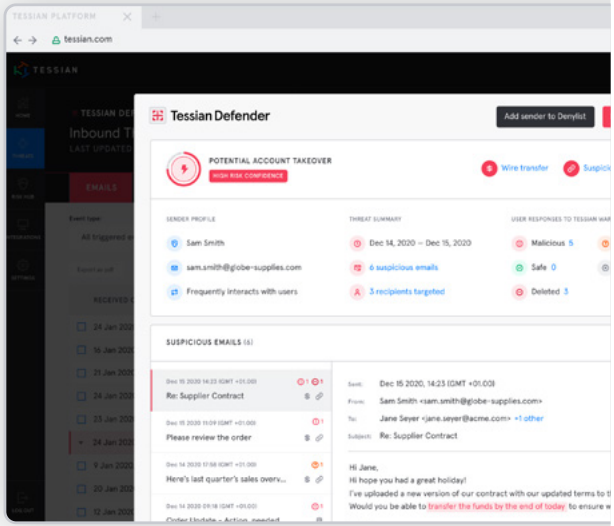
STOP ACCOUNT TAKEOVER WITH TESSIAN DEFENDER

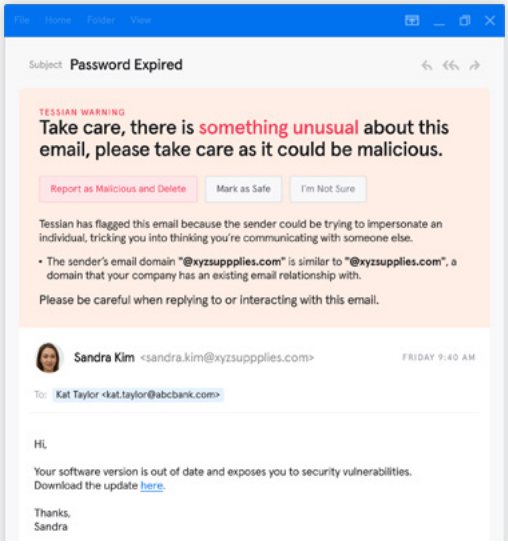
Account Takeover detection is automatically enabled by default for all customers and there is no configuration required.

GRANULAR THREAT VISIBILITY

Rapid Remediation

Tessian identifies attack campaigns and groups them together to save security teams time and resources when evaluating and remediating ATO threats. Admins can clawback emails, quickly delete and remediate events in bulk with a single click.





SECURITY AWARENESS TRAINING

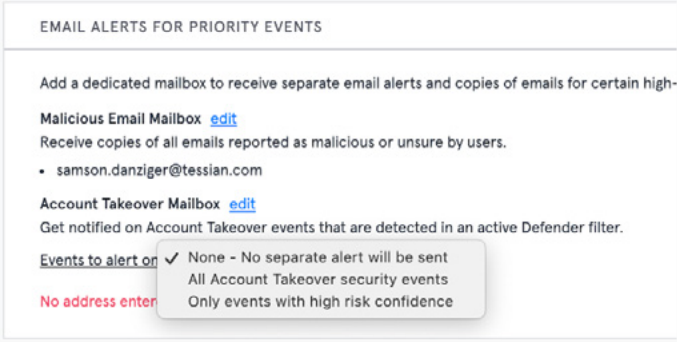
In-the-moment Security Coaching

Emails with high probability of being an ATO attack are automatically quarantined for admin review. For those emails with a lower probability employees receive a contextual, in-the-moment coaching banner alerting the end user of potential threats and guiding them to safely self-remediate, saving Security team's time and building a better risk posture for your employees.

NEXT GENERATION DETECTION

Security Alerts

Admins can separately enable alerts for potential ATO attacks. If configured, admins will receive the compliance alert email for each corresponding ATO in the specified mailbox (in the same format as today's compliance alerts). Alerts include a link to the ATO case viewer in the portal for swift evaluation and remediation.



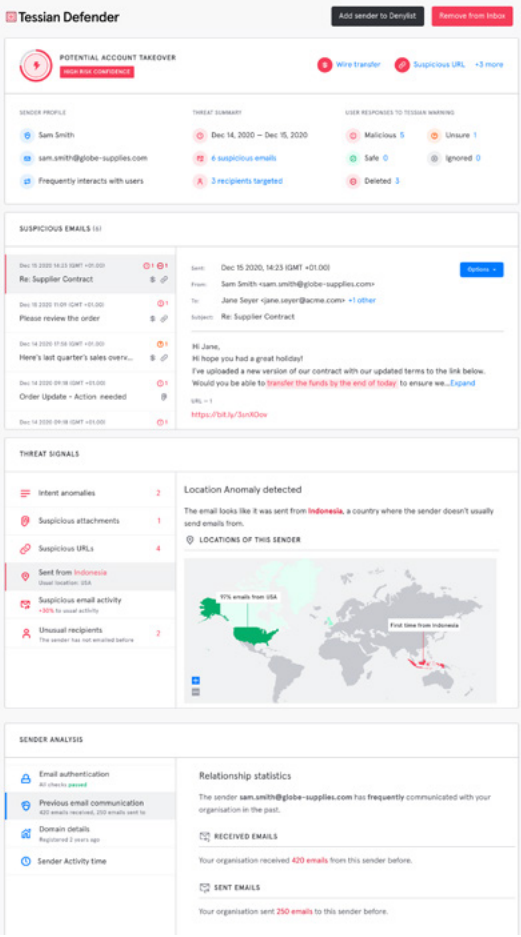
How ATO Events Appear in the Security Events Table.

Admins are able to examine the ATO event using a new ATO case viewer. The case viewer consists of key components to help admins effectively evaluate and remediate potential ATO threats:

The viewer is centered around the sender and aggregates all anomalies detected that look like an ATO attack

A list of all individual emails by this sender where the ATO algorithm triggered

Additional intelligence Tessian has about the sender to help admins make an informed decision



SEAMLESSLY INTEGRATE WITH ALL EMAIL ENVIRONMENTS

Exchange Office 365 G Suite

SEAMLESSLY INTEGRATE INTO YOUR SECURITY STACK

KnowBe4 okta SECURONIX sumo logic splunk>

TRUSTED BY ENTERPRISE CUSTOMERS ACROSS ALL INDUSTRIES:

EVERCORE arm HERBERT SMITH FREEHILLS REALPAGE affirm Schroders rightmove

Investec GRAPHCORE sanne K&L GATES PeaceHealth GOCARDLESS

MSCI ERT CLYDE&CO BRACEWELL RAND MERCHANT BANK Intertrust ManGroup plc

See Tessian in Action.

Automatically stop data breaches and security threats caused by employees on email.

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.