TESSIAN

Tessian Defender

Prevent Inbound Email Attacks that Bypass Legacy Email Security Solutions.

INBOUND EMAIL SECURITY

Tessian Defender intelligently protects against advanced email threats such as spear phishing, Business Email Compromise, Account Takeover while reducing security teams' workloads, and coaching end users about security threats in-the-moment.

How Do You Currently Manage The Threat Of Inbound Email Attacks?

Spear Phishing, Ransomware, Account Takeover, Business Email Compromise (BEC), Socially Engineered, and impersonation attacks are top of mind for security leaders. It's easy to see why.

CONSIDER THE STATISTICS...

#1

Phishing is #1 for all security incidents[1].

70%-90%

of all breaches involve social engineering, and 96% of phishing breaches came through email[2,3].

$1.8BN

Business Email Compromise has resulted in $1.8BN in losses[4].

92%

of malware is delivered by email[5].

Solution Highlights and Key Benefits

RISK-BASED APPROACH

Tessian emphasizes a behavioral risk-based approach, not a binary approach to classify threats. By using natural language processing (NLP) algorithms to perform a content X-ray that detects indicators of attack such as malicious intent, impersonation, compromise, and payloads, resulting in more accurate security decisions.

ENHANCED PROTECTION, EASY DEPLOYMENT

Tessian offers flexible deployment options for regardless of whether your email is in the cloud, on-premise, or a hybrid deployment. Tessian Defender includes API deployment for Microsoft Office 365. Defender Deploys in minutes and protects within hours.

LOW MANAGEMENT OVERHEAD

Tessian reduces the burden on your SecOps teams with automated triage, investigation and remediation and risk reporting. For Microsoft Office 365 customers there is no ongoing management beyond adding new users to directory groups.

IN-THE-MOMENT TRAINING

Tessian turns your employees into your biggest cyber asset with frictionless in-the-moment employee training. Powerful, yet non-intrusive end-user education with alerts helps organizations drive employees towards secure email behavior to reduce risks over time.

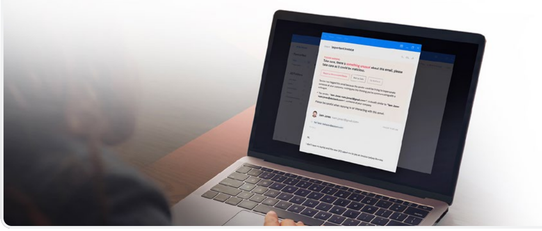
EMPLOYEE PROTECTION

Emails with the highest probability of being malicious are automatically quarantined. For emails with a lower probability of being malicious the end-user gets in-the-moment training banner with a defanged copy of the email (with attachment and URL links stripped) ensuring they don't click on URL or attachment before determining the email is safe.

Defender Product Differentiators

Email is typically the first to deliver initial malicious URLs, in the form of an exploit kit or phishing website, attachments in the form of payloads, or a starting point for social engineering attacks, such as in the case of business email compromise or credential phishing attacks.

Tessian Defender protects against advanced attacks using three proven and differentiated approaches - threat detection & prevention, education and awareness, and reducing the overall burden on security operations centers while improving security effectiveness.



INTELLIGENTLY STRENGTHEN EMAIL PROTECTION

Tessian Defender automatically protects against both known and unknown email attacks, including Account Takeover (ATO), Business Email Compromise (BEC), spear phishing, ransomware, and socially engineered attacks that bypass rule-based Secure Email Gateways, Microsoft 365 and Google Workspace security controls.

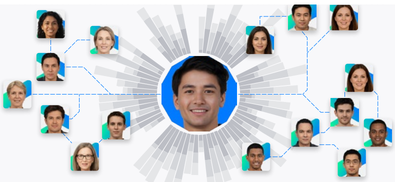
REDUCE BURDEN ON SECURITY TEAMS

Tessian Defender improves security behaviors of employees by alerting them in-the-moment and delivering contextual training when advanced threats are detected on email. Organizations can educate and empower users with this ongoing email security awareness and improve overall email risk posture

HELP SECURITY TEAMS WORK SMARTER, NOT HARDER

Tessian Defender significantly reduces the burden on SOC teams by decreasing incident response to email-related incidents and automating triage, investigation, remediation and risk reporting. Fully automated by machine learning, it requires no manual rules or policy configurations.

[1] Tessian [2] KnowBe4 [3] Verizon [4] FBI [5] Verizon



Threat Prevention

BEHAVIORAL INTELLIGENCE

Tessian Defender's behavioral intelligence leverages at least 12 months of historical data that includes the company's emails, company network, as well as Tessian's Global Threat Network, to detect all indicators of attack including impersonation, compromise, payloads and intent.

PREVENT INBOUND EMAIL ATTACKS NOT DETECTED BY LEGACY SOLUTIONS

Legacy approaches will scan for known malicious payloads such as links and attachments.This leaves these defenses vulnerable to zero-day threats, or attacks without payloads. Tessian will inspect the context of the email to determine indicators of an attack, notify the user, therefore not giving an opportunity of malware slipping through or the user to click. This moves Tessian up the stack to stop attacks.

CONTEXT-AWARE SECURITY

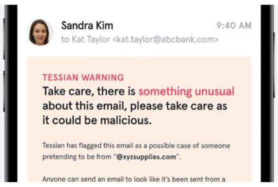
Unlike other email security solutions, Tessian Defender is context-aware. It uses natural language processing (NLP) to perform a content X-ray that detects indicators of attack such as malicious intent, impersonation, compromise, and payloads, resulting in more accurate security decisions. Tessian Defender takes proportional actions based on the risk level of the threat, warning users appropriately based on the severity of the risk.

AUTOMATED ADMIN QUARANTINE & SOFT QUARANTINE

Tessian Defender automatically quarantines emails with the highest probability of being malicious. For emails with a lower probability Soft Quarantine gives the end user in-the-moment security notification and a defanged copy of the email protecting the user from clicking on a URL or attachment until they've determined the email is safe.

BULK REMEDIATION

Tessian Defender allows admins to bulk-remediate malicious emails in 1-click. By identifying attacks (burst attacks), admins can delete the entire campaign from users' inboxes with one click. Tessian Defender also enables administrators to delete suspicious emails in users' inboxes directly from the portal



Sandra Kim 9:40 AM
to Kat Taylor <kat.taylor@abcbank.com>

TESSIAN WARNING
Take care, there is something unusual about this email, please take care as it could be malicious.

Tessian has flagged this email as a possible case of someone pretending to be from "@xyzsupplies.com".

Anyone can send an email to look like it's been sent from a

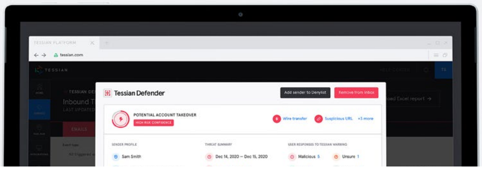
Education and Awareness

IN-THE-MOMENT TRAINING

Non-disruptive in-the-moment training and awareness is provided to employees through contextualized, easy to understand warning messaging.

RISK TRENDS DOWNWARD

Risk will quickly trend downward as users learn more about security through in-the-moment warnings, becoming better at spotting attacks and lowering click-through rates on identified threats.



TESSIAN PLATFORM
tessian.com
TESSIAN
Inbound T
LAST UPDATED
EMAILS
Tessian Defender
Add sender to Denylist
Remove from Inbox
POTENTIAL ACCOUNT TAKEOVER
HIGH RISK CONFIDENCE
Wire transfer
Suspicious URL
+3 more
SENDER PROFILE
Sam Smith
THREAT SUMMARY
Dec 14, 2020 – Dec 15, 2020
USER RESPONSES TO TESSIAN WARNING
Malicious 5
Unsure 1

Reduce Admin Overhead

RISK-BASED APPROACH

Tessian Defender emphasizes risk-based protection, not a binary approach to classifying threats, which significantly reduces the burden on security ops teams. In-the-moment warnings take further burdens off the SOC reducing the amount of email to triage.

NO MORE TIME-CONSUMING, RIGID POLICIES

There is no need for admin teams to maintain a complex set of rules or establish pre-defined policies or configurations.Tessian Defender reduces the burden on SOC teams to triage threats from other security tools, resulting in low ongoing administration.

FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS

Flexible deployment options and seamless integrations with existing email security controls and legacy Secure Email Gateways (SEG), G-Suite via connectors, add-ins and M365 APIs. Tessian Defender deploys in minutes and automatically prevents data breaches through email within 24 hours of deployment, across all devices, desktop and mobile. See all Tessian Integrations →

Tessian Defender Coverage

When we say comprehensive, we mean comprehensive. Tessian Defender prevents all inbound attacks that lead to some nasty outcomes - such as ransomware and zero-day attacks.

Impersonated Party → Impersonation Method

INTERNAL
Executive
Colleague

EXTERNAL
Vendor
Supplier
Brand
Service

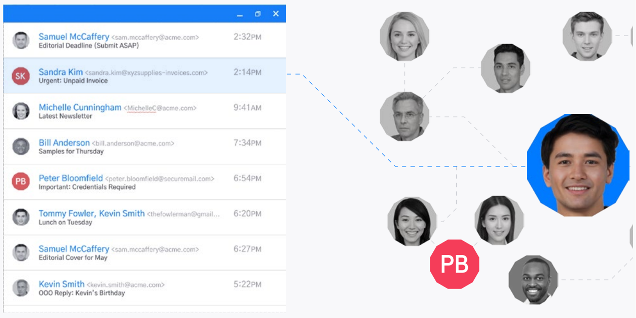
Domain Lookalike
Display Name Lookalike
Exact Domain Spoof

Attack Type Coverage → Attack Outcome

Account Takeover
Business Email Compromise (BEC)
Spear Phishing
Social Engineering
Whaling Attack
Executive Spoofing

Ransomware
Zero-day Attacks
Cypto fraud
PII Theft
Data Theft
IP and Sensitive Data Loss
Credential Loss/Harvesting
Reputational Damage
Organization Downtime

How Tessian Defender Works



Samuel McCaffery <sam.mccaffery@acme.com> 2:32PM
Editorial Deadline (Submit ASAP)

SK Sandra Kim <sandra.kim@xyzsupplies-invoices.com> 2:14PM
Urgent: Unpaid Invoice

Michelle Cunningham <MichelleC@acme.com> 9:41AM
Latest Newsletter

Bill Anderson <bill.anderson@acme.com> 7:34PM
Samples for Thursday

PB Peter Bloomfield <peter.bloomfield@securemail.com> 6:54PM
Important: Credentials Required

Tommy Fowler, Kevin Smith <thefowlerman@gmail... 6:20PM
Lunch on Tuesday

Samuel McCaffery <sam.mccaffery@acme.com> 6:27PM
Editorial Cover for May

Kevin Smith <kevin.smith@acme.com> 5:22PM
OOO Reply: Kevin's Birthday

BEHAVIORAL ANALYSIS

Detect all indicators of inbound email attacks.

Tessian Defender's behavioral intelligence leverages at least 12 months of historical data that includes the company's emails, company network, as well as Tessian's Global Threat Network, to detect all indicators of inbound email attacks.

By using these broad range of signals from relationship graphs, deep inspection of the email content, and previous user behavior, Tessian can identify all inbound email attacks including:

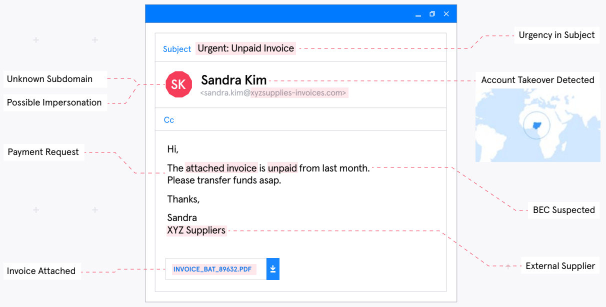
- Account Takeover →
- Business Email Compromise (BEC) →
- All Impersonation Attacks →
- Spear Phishing →
- Social Engineering →
- Whaling Attacks →

DEEP INSPECTION OF EMAIL CONTENT

Identify inbound email threats in real-time.

Tessian Cloud Email Security Platform analyzes all inbound emails in real-time and uses machine intelligence to automatically predict whether an incoming email is malicious. Using a broad range of signals from relationship graphs, Tessian performs deep inspection of the email content, and previous user behavior.

Legacy approaches will scan for known malicious payloads such as links and attachments. This leaves these defenses vulnerable to zero-day threats, or attacks without payloads. Tessian will instantly inspect the context of the email to determine indicators of an attack, and protect your organization from highly targeted email based attacks.



Subject Urgent: Unpaid Invoice

SK Sandra Kim
<sandra.kim@xyzsupplies-invoices.com>

Cc

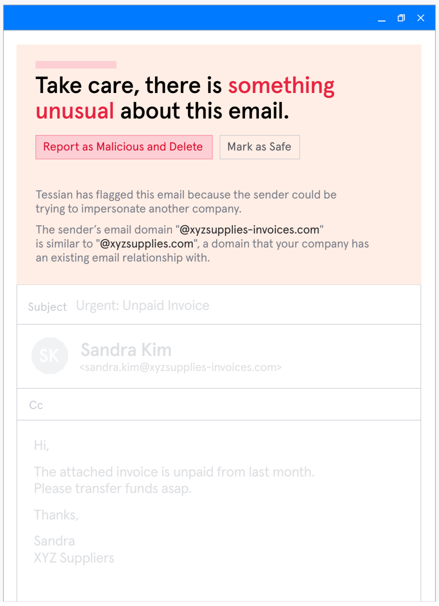
Hi,

The attached invoice is unpaid from last month.
Please transfer funds asap.

Thanks,

Sandra
XYZ Suppliers

INVOICE_BAT_89632.PDF



Take care, there is something unusual about this email.

Report as Malicious and Delete | Mark as Safe

Tessian has flagged this email because the sender could be trying to impersonate another company.

The sender's email domain "@xyzsupplies-invoices.com" is similar to "@xyzsupplies.com", a domain that your company has an existing email relationship with.

Subject Urgent: Unpaid Invoice

SK Sandra Kim
<sandra.kim@xyzsupplies-invoices.com>

Cc

Hi,

The attached invoice is unpaid from last month.
Please transfer funds asap.

Thanks,

Sandra
XYZ Suppliers

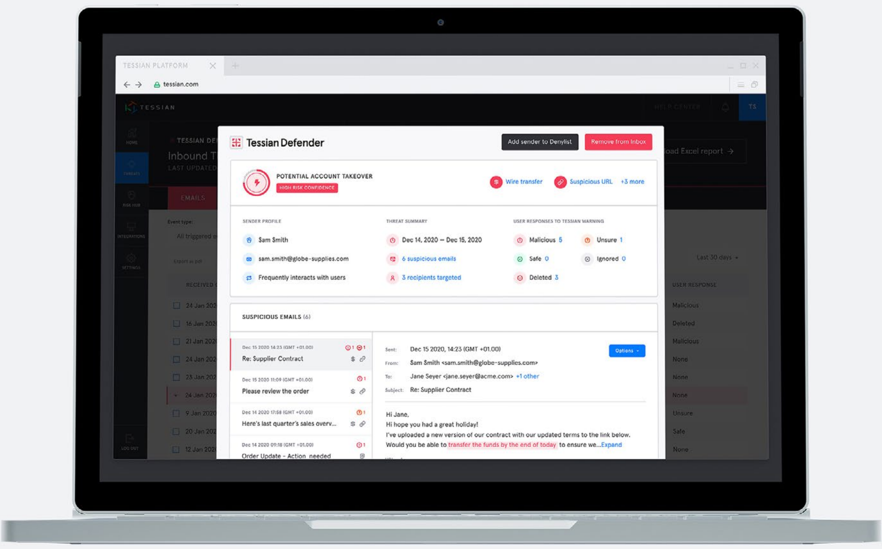
CONTINUOUS SECURITY AWARENESS TRAINING

In-the-moment training to stop email attacks where they start.

When unsafe emails are detected, employees can either receive in-the-moment alert notifications with clear, simple explanations of potential risks or emails can be directly quarantined for inspection and approval by Security Analysts. Emails with the highest probability of being malicious are automatically quarantined for SecOps to investigate. For emails with a lower probability of being malicious, Tessian Defender uses in-the-moment training notifications to turn your employees into your biggest cyber asset providing them with clear, simple explanations of potential risks.

Non-disruptive in-the-moment training and awareness is provided to employees through contextualized, easy to understand warning messages.

Risk trends downward as users learn more about security through in-the-moment warnings, becoming better at spotting attacks and lowering click-through rates on identified threats.


Tessian Defender

Add sender to Denylist | Remove from Inbox

POTENTIAL ACCOUNT TAKEOVER
HIGH RISK CONFIDENCE

Wire transfer · Suspicious URL · +3 more

SENDER PROFILE	THREAT SUMMARY	USER RESPONSES TO TESSIAN WARNING	
Sam Smith	Dec 14, 2020 – Dec 15, 2020	Malicious 5	Unsure 1
sam.smith@globe-supplies.com	6 suspicious emails	Safe 0	Ignored 0
Frequently interacts with users	3 recipients targeted	Deleted 3	

SUSPICIOUS EMAILS (6)

- Dec 15 2020 14:23 (GMT +01.00) — Re: Supplier Contract
- Dec 15 2020 11:09 (GMT +01.00) — Please review the order
- Dec 14 2020 17:58 (GMT +01.00) — Here's last quarter's sales overv...
- Dec 14 2020 09:18 (GMT +01.00) — Order Update - Action needed

Sent: Dec 15 2020, 14:23 (GMT +01.00)
From: Sam Smith <sam.smith@globe-supplies.com>
To: Jane Seyer <jane.seyer@acme.com> +1 other
Subject: Re: Supplier Contract

Options

Hi Jane,
Hi hope you had a great holiday!
I've uploaded a new version of our contract with our updated terms to the link below.
Would you be able to transfer the funds by the end of today to ensure we...Expand

MITIGATE AND REMEDIATE

Granular visibility to quickly prevent, mitigate and remediate inbound email attacks.

The Tessian Cloud Email Security Platform allows security teams to seamlessly access insights, intelligence, and tools that significantly reduce manual incident investigation time and allow for rapid response to impersonation threats. With Tessian security teams can:

- → Granular visibility into risk levels and drivers within the organization. Readily view top threats, top targeted users, and detailed breakdown of anomalous events detected by Tessain Defender.
- → Automated triage, investigation, remediation and risk reporting reduces SOC burden, team burnout and frees up time for other important tasks. Low false positives eliminates alert fatigue
- → Remediate with speed. Quarantine, clawback unsafe emails from users' inboxes, or update blocklists to prevent similar threats with a single click.
- → Fully automate SOC workflows and integrate with your SIEM, SOAR, IAM, ITSM, SEG or Phishing Training vendor to enhance security insights and orchestrate your workflows.
- → Quantify risks, compare trends, and influence employees to adopt a secure behavior. Benchmark impersonation risk levels against industry peers

TRUSTED BY ENTERPRISE CUSTOMERS ACROSS ALL INDUSTRIES:

Evercore · arm · Herbert Smith Freehills · RealPage · affirm
Investec · Graphcore · sanne · K&L Gates · PeaceHealth
MSCI · ERT · Man Group plc · Bracewell · Rand Merchant Bank
Clyde&Co · Intertrust · rightmove · GoCardless · Schroders

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.