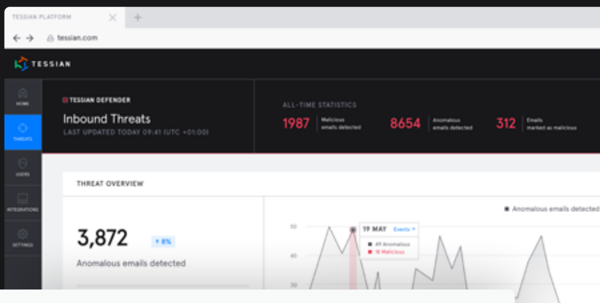
TESSIAN


Inbound Threats

1987 Malicious emails detected

8654 Anomalous emails detected

312 Emails marked as malicious

3,872 Anomalous emails detected

Tessian Defender

Prevent Inbound Email Attacks that Bypass Legacy Email Security Solutions.

INBOUND EMAIL SECURITY

Tessian Defender is a comprehensive inbound email security solution that automatically prevents a wide range of attacks that bypass Secure Email Gateways, while providing in-the-moment training to drive employees toward secure email behavior.

How do you currently manage the threat of inbound email attacks?

Phishing, spear phishing, business email compromise (BEC), and impersonation attacks are top of mind for security leaders. It's easy to see why.

CONSIDER THE STATISTICS...

95%
of all attacks on enterprise networks are the result of successful spear phishing[1].

22%
of breaches involve social engineering, and 96% of those breaches came through email[2].

$12.5BN
Spear phishing has cost global businesses $12.5bn in losses[3].

92%
of malware is delivered by email[4].

Solution Highlights and Key Benefits

RISK-BASED APPROACH

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 to release to the inbox.

FREE UP YOUR SOC

Defender massively reduces the burden on SOC teams to triage threats from other security tools, resulting in low ongoing admin.

CONTEXT-AWARE SECURITY

Defender uses 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.

IN-THE-MOMENT TRAINING

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

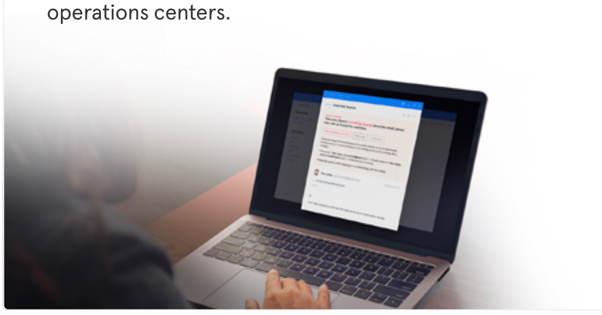
FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS

Defender deploys in minutes and automatically prevents data breaches through email within 24 hours of deployment, across all devices, desktop and mobile.

Defender Product Differentiators

Email is typically the first to deliver initial 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.

Defender covers these attacks using three proven and differentiated approaches - threat prevention, education and awareness, and reducing the overall burden on security operations centers.



PROTECT AGAINST KNOWN AND UNKNOWN EMAIL THREATS

Defender protects against both known and unknown email attacks, including Business Email Compromise (BEC), Account Takeover (ATO), spear phishing, and all impersonation attacks that bypass Secure Email Gateways, Microsoft 365, and G Suite.

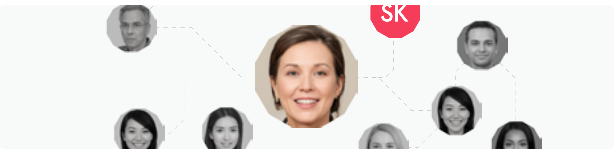
BUILD CONTINUOUS SECURITY AWARENESS

With Defender's in-the-moment training, organizations can educate and empower users to build continuous email security awareness.

AUTOMATE REPETITIVE TASKS

Defender removes the burden on the SOC and admins by automating repetitive tasks such as maintaining triage and review. This eliminates the need for human verification of email threats, reducing FTE requirements.

[1] IC3 [2] Verizon [3] FBI [4] Verizon



Threat Prevention

BEHAVIORAL INTELLIGENCE

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 defences 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 cyber attack kill chain to stop attacks.

CONTEXT-AWARE SECURITY

Unlike other email security solutions, Defender is **context-aware.** It uses 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. This, in turn, provides an alert that the end user will understand, helping them make the right decision. Defender takes proportional actions based on the risk level of the threat, warning users appropriately based on the severity of the risk.

BULK REMEDIATION

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. Defender also enables administrators to delete suspicious emails in users' inboxes directly from the portal.

AUTOMATED QUARANTINE

Defender automatically quarantines emails that the algorithm determines to be highly malicious.

Unpaid Invoice

Sandra Kim

TESSIAN WARNING

Take care, there is something unusual about this email, please take care as it could be malicio

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.

Reduce Admin Overhead

FREE UP YOUR SOC

Defender massively reduces the burden on SOC teams to triage threats from other security tools, resulting in low ongoing admin.

RISK-BASED APPROACH

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 to release to the inbox.

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.

FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS

Flexible deployment options and seamless integrations with existing email security controls and legacy Secure Email Gateways (SEG), add-ins, and G-Suite and API/O365 API. 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 →

Exchange   Office 365   G Suite   SGS   AICPA SOC

DUO   splunk>   Radar   exabeam

ALIEN VAULT   RAPID7   RSA

Defender Coverage

When we say comprehensive, we mean comprehensive. 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

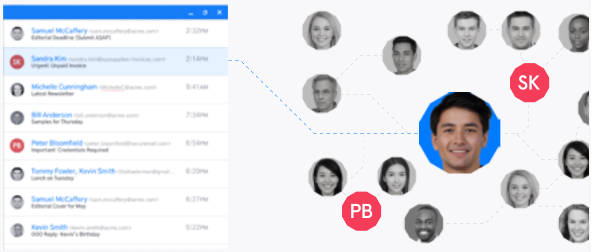
Domain Lookalike
Display Name Lookalike
Exact Domain Spoof

Attack Type Coverage → Attack Outcome

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

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

How Defender Works



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

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

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.

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:

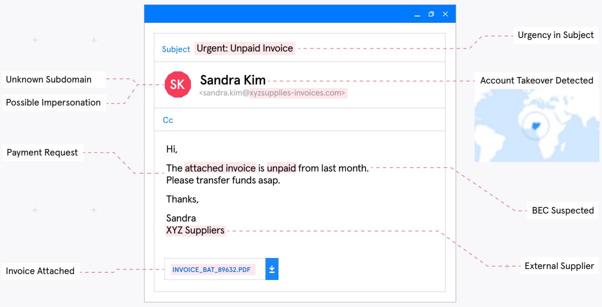
- Account Takeover →
- Business Email Compromise (BEC) →
- All Impersonation Attacks →
- Spear Phishing →
- Social Engineering →
- Whaling Attacks →

DEEP INSPECTION OF EMAIL CONTENT

Identify inbound email threats in real-time.

Tessian's Human Layer Security (HLS) Engine 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 defences 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.



Subject Urgent: Unpaid Invoice

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

Cc

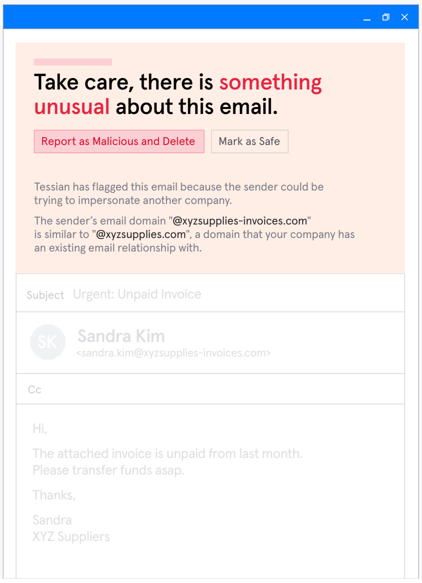
Hi,

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

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

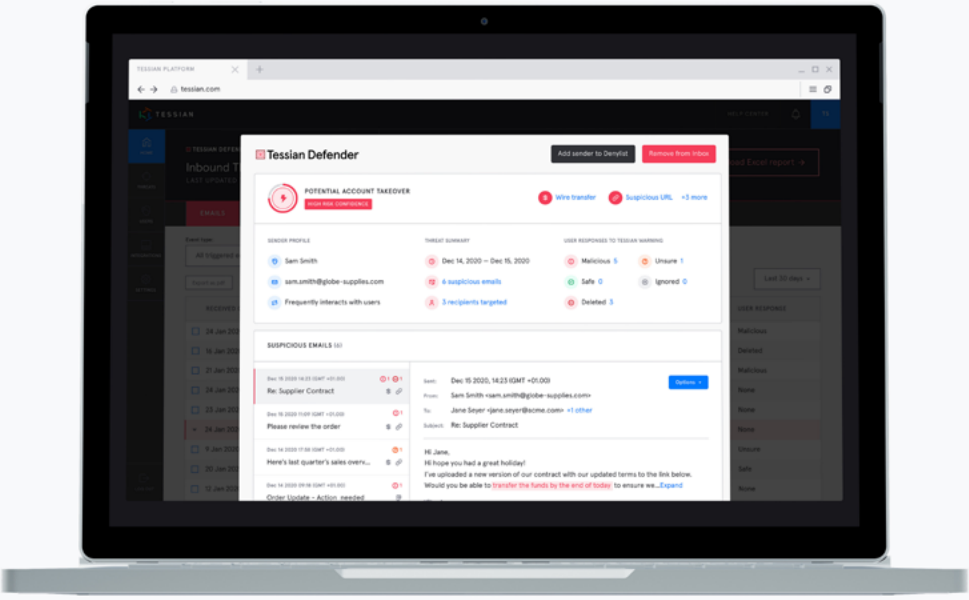
CONTINUOUS SECURITY AWARENESS TRAINING

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

When unsafe emails are detected, employees can either receive in-the-moment alerts with clear, simple explanations of potential risks or emails can be directly quarantined for inspection and approval by Security Analysts.

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.



POTENTIAL ACCOUNT TAKEOVER
HIGH RISK CONFIDENCE

SENDER PROFILE
Sam Smith
sam.smith@globe-supplies.com
Frequently interacts with users

THREAT SUMMARY
Dec 14, 2020 – Dec 15, 2020
6 suspicious emails
3 recipients targeted

USER RESPONSES TO TESSIAN WARNING
Malicious 5
Unsure 1
Safe 0
Ignored 0
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

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.

Built within the Tessian Human Layer Security Platform, HLS Intelligence 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 HLS Intelligence, security teams can:

- Readily view top threats, top target users, and detailed breakdown of anomalous events detected by Tessian Defender.
- Remediate with speed. Quarantine, clawback unsafe emails from users' inboxes, or update blacklists to prevent similar threats with a single click
- Future proof defenses using shared threat intelligence and automatically block blacklisted domains across the Tessian ecosystem. No rules needed.
- Quantify risks, compare trends, and influence employees to adopt a secure behaviorBenchmark impersonation risk levels against industry peers.

TRUSTED BY ENTERPRISE CUSTOMERS ACROSS ALL INDUSTRIES:

Evercore arm Prudential RealPage Outperform affirm Schroders rightmove

Investec Graphcore sanne K&L Gates cordaan Dentons

fieldfisher ERT Clyde&Co Bracewell gubra Intertrust Man Group plc

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.