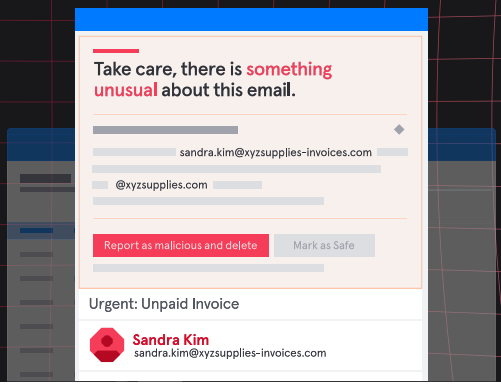
TESSIAN



Tessian Defender

FOR INBOUND EMAIL

Prevent email security threats that are impossible to detect with legacy email security controls.

Impersonation is today's biggest security threat. Loss to Business Email Compromise attacks exceeded $26 billion in the past three years.[1]

Today's email attacks are increasingly being designed to bypass Secure Email Gateways (they contain no url or attachment, they are targeted not bulk in nature and leverage both internal and external contact impersonation techniques). As a result, unsafe emails are reaching employees' inboxes on an increasing basis and leading to significant financial losses, credential theft and data breaches. Even savvy employees can fall victim to the modern tactics used by attackers.

Tessian Defender automatically prevents business email compromise, spear phishing and other targeted email attacks. Powered by Tessian's proprietary Human Layer Security Engine, Defender analyses millions of data points for every inbound email and detects anomalies that indicate security threats. Tessian Defender captures attacks that evade secure email gateways and legacy security controls. These include zero-payload attacks that include no URL or attachment, look-alike impersonations of internal employees and trusted external counterparties – vendors, suppliers, customers, contractors and more, and difficult-to-detect domain spoof manipulations.

Key Benefits

EFFECTIVE PROTECTION AGAINST TODAY'S BIGGEST SECURITY THREAT

- Automatically prevent Business Email Compromise, spear phishing and other targeted email attacks that bypass Secure Email Gateways and legacy email security controls.
- Machine learning system continually analyses email network and adapts to prevent never-before-seen threats.
- Automated blacklisting using shared threat intelligence from Tessian threat intel network future proofs your defense.
- Enhance your static phishing simulations with in-situ security awareness and training via contextual warning banners.
- Prevent catastrophic financial loss, credential theft and data breaches.

Key Features

ENTERPRISE GRADE SECURITY

Tessian is used by world leading organizations across healthcare, finance, legal and technology and holds the highest standards of security certification.

POWERED BY MACHINE LEARNING

Provides continuous, adaptive email security.

REAL-TIME ANALYSIS OF EMAILS

Uses our proprietary Human Layer Security Engine that detects anomalies in real-time based on insights from relationship graphs, external data sources, email content and user behavior.

ADVANCED PROTECTION

Detects even the most advanced domain, sub-domain and display name impersonations.

CONTEXTUAL WARNING MESSAGES

Real-time contextual warning banners provide clear and precise guidance on why emails look unsafe. Contextual explanations for anomalies detected allowing security teams to investigate threats easily.

TESSIAN HLS INTELLIGENCE BUILT-IN

Provides insights, automated intelligence on data breaches enabling rapid investigation. Remediation tools allow to mitigate and lower inbound attacks.

- Quarantine, post delivery email claw back, single-click domain blacklisting
- Automated domain blacklisting via Tessian's threat intel network

COMPREHENSIVE PROTECTION

Secures all inbound 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

[1] FBI Internet Crime Complaint Center Estimate

EFFORTLESS FOR SECURITY, IT, AND COMPLIANCE TEAMS

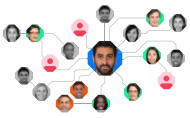
Security and Compliance Teams:

- Machine learning system continually evolves to automatically prevent new threats.
- Get visibility into inbound attacks organization faces and data breaches prevented.
- Significantly eliminate manual incident investigation and respond to threats faster with automated threat intelligence and robust remediation tools.
- Minimal disruption to employees.

IT Teams:

- Integration to 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 and security controls
- Invisible to the end-user until potential threats are detected

How Tessian Defender Protects from Advanced Impersonation Attacks:



Establish employee relationship graphs with historical email data.

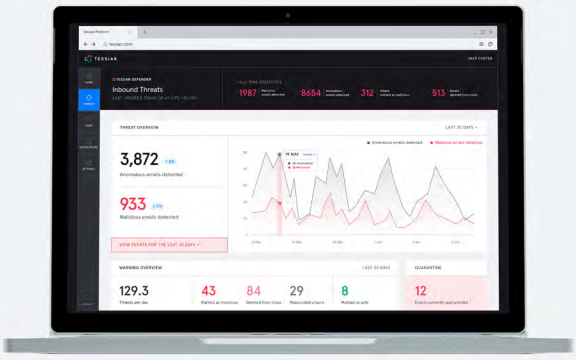
Tessian analyzes historical email data to understand normal content, context, and communication patterns, enabling a comprehensive mapping of every employee's trusted email relationships (both within and outside your organization). Relationship graphs are continuously updated as email behavior changes over time after Tessian is deployed.

Perform real-time analysis of inbound emails and detect anomalies.

Tessian's Human Layer Security Engine analyzes all inbound emails in real-time and uses machine intelligence to automatically predict whether the email looks unsafe based on insights from the relationship graph, external data sources, deep inspection of the email content, and previous user behavior.

Automatically prevent targeted email attacks.

When unsafe emails are detected, employees can either be alerted in-situ with clear, simple explanations of potential risks or emails can be directly quarantined for inspection and approval by Security teams.



Get visibility into breaches prevented and quickly take mitigation actions with Tessian HLS Intelligence

Built within the Tessian HLS Platform, Security teams can seamlessly access insights, automated threat intelligence behind security events, and remediation tools that significantly reduce manual incident investigation time and allow for rapid response to impersonation threats. Auto blacklist unsafe domains, block similar threats, view attack types, quantify risks, compare trends, benchmark against peers and more. Tessian API integrations allow security teams to centralize and orchestrate events from your SIEM/SAOR platforms. Learn More →

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

REQUEST DEMO →

CONTACT US

TESSIAN | Human Layer Security

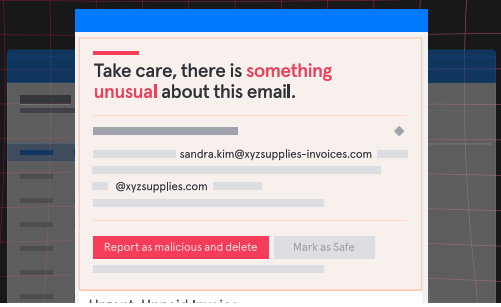
TESSIAN.COM

Tessian builds technology to empower people to work safely, without security getting in their way. Tessian's Human Layer Security platform automatically protects your employees on email - where they spend 40% of their time - from risks like business email compromise, phishing, data exfiltration and misdirected emails. We've raised $60M from legendary security investors like Sequoia and Accel and located in San Francisco and London.

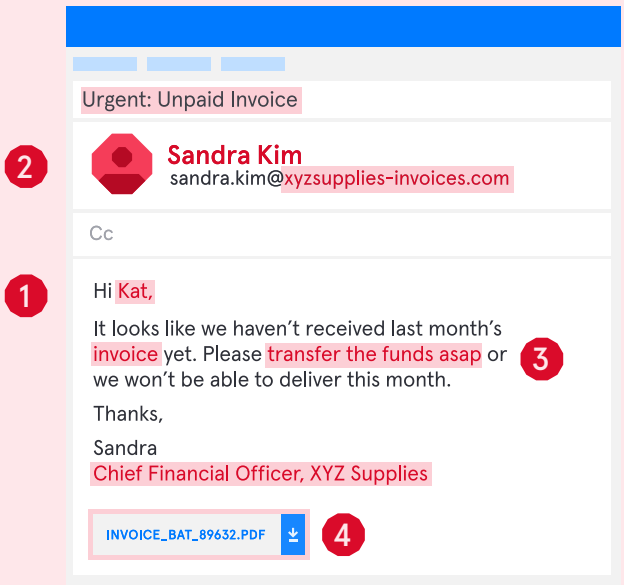
TESSIAN

Tessian Defender

FOR INBOUND EMAIL



Breaking down spear phishing and advanced impersonation attacks



Phishing relies on the impersonation of trusted entities, is typically bulk in nature, and isn't personalized. Spear phishing is highly targeted, sophisticated, and convincing, making them hard to catch. Typical components include:

1 TARGET

Attackers may focus on high-ranking executives or members of certain crucial departments.

2 SENDER IDENTITY

Successful attackers invariably impersonate colleagues, customers, or third-party suppliers.

3 INTENT

Requests for action exploit organizational pressures or personal relationships to maximize urgency and time sensitivity.

4 PAYLOAD

Payload of a spear phishing attack might be a corrupt file, a malicious link, or no payload at all, making them even harder to detect.

Traditional Methods vs Tessian

(AN EXAMPLE)

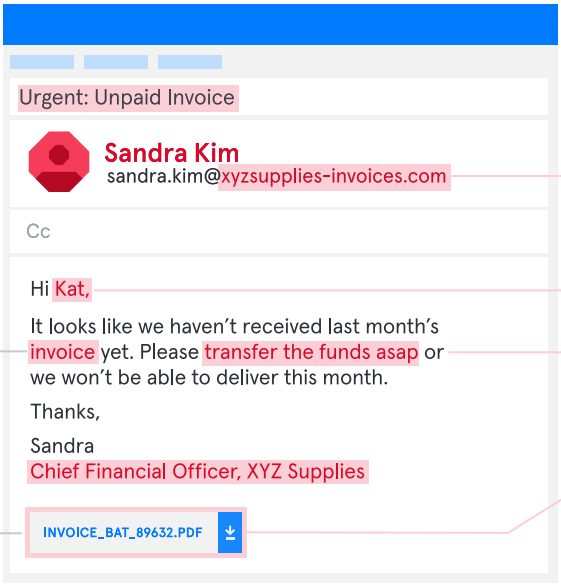
TYPICAL ANALYSIS BY TRADITIONAL METHODS:

Sender domain is an impersonation of an external counterparty. Domain is not blacklisted.

Email contains no URLs

Attached file is not malware

Impersonation attack: UNDETECTED



Tessian Defender

TESSIAN'S PROTECTION AGAINST BUSINESS EMAIL COMPROMISE, SPEAR PHISHING AND OTHER TARGETED EMAIL ATTACKS:

Domain and display name impersonates a trusted vendor.

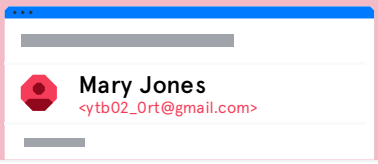
Sender has no prior relationship with the company.

Language indicates social engineering. Intents detected: high urgency, wire transfer request.

Potentially fraudulent invoice detected.

Impersonation attack: PREVENTED

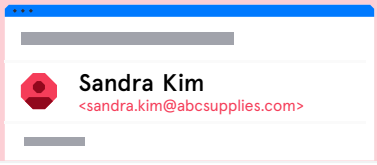
Tessian can detect both internal and external look-alike impersonations making it an essential layer of security for MS Exchange, O365 and G Suite environments



Display name impersonations

The *from:* display name appears legitimate, but the *from:* address is different.

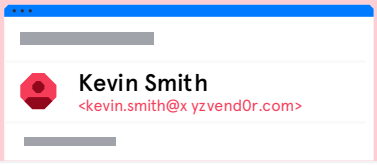
Mary Jones <ytb02_0rt@gmail.com>
or worse
Mary Jones <mary.jones.contractor@gmail.com>



Direct impersonation

The *display name* and *from:* address exactly match the legitimate individual and the domain:

Sandra Kim <sandra.kim@abcsupplies.com>



Domain impersonations

The *from:* address spoofs the legitimate *domain name* or uses spoof subdomains:

Kevin Smith <kevin.smith@xyzvendor-invoice.com>
Kevin Smith <kevin.smith@xyzvendor-secured-email.com>
or
Kevin Smith <kevin.smith@xyzvend0r.com>

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

REQUEST DEMO →

CONTACT US

TESSIAN | Human Layer Security

TESSIAN.COM

Tessian builds technology to empower people to work safely, without security getting in their way. Tessian's Human Layer Security platform automatically protects your employees on email - where they spend 40% of their time - from risks like business email compromise, phishing, data exfiltration and misdirected emails. We've raised $60M from legendary security investors like Sequoia and Accel and located in San Francisco and London.