TESSIAN

PROTECT YOUR PEOPLE

Human Layer Security Platform Overview

Tessian is the world's only Human Layer Security platform that automatically stops data breaches and security threats caused by employees on email.

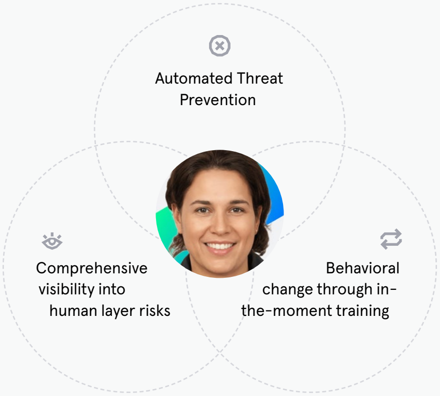
How are you preventing Human Layer Security threats?

Human error is the primary root cause of data breaches over email. To prevent today's email threats, security controls must understand human behavior, and security and IT teams must have clear visibility into their human layer threats.

Tessian uses machine learning technology to uniquely address the risks posed by employees. We do this by:

Providing comprehensive visibility into your human layer risks.	Automatically detecting and preventing threats like accidental data loss, data exfiltration, and advanced phishing attacks (that legacy solutions can't detect).	And more importantly, we change behavior: we continuously drive your employees toward secure email behavior through contextual, in-the-moment training.

All of these together continually reduce security threats at the human layer and strengthen your organization's security posture. This is all done with no disruptions to your employees' productivity. Tessian deploys within minutes, learns within hours and starts protecting in a day.


Automated Threat Prevention
Comprehensive visibility into human layer risks
Behavioral change through in-the-moment training

Platform Benefits

AUTOMATED THREAT PREVENTION AND REMEDIATION

Contextual machine learning (ML) understands human behavior on email, can predict normal and abnormal email activity, and can start preventing the most advanced threats within 24 hours of deployment. No pre-configuration required.

HOLISTIC VIEW OF HUMAN BEHAVIOR

Tessian maps employee email activity and builds unique security identities for every individual. Tessian dashboards and analytics surface these insights and give full visibility into threats you've never been able to detect before. Now you can predict and preempt security risks caused by unsafe human behavior.

MAKE PEOPLE YOUR STRONGEST DEFENSE

Tessian warnings act as in-the-moment training for employees, continuously educating them about threats, reinforcing your policies, and nudging them toward safe behavior. Take the right educational interventions and targeted remedial actions at scale.

EFFORTLESS AND NON-DISRUPTIVE

Easy to deploy, to manage, and to integrate with any email environment and enterprise security applications. You can set it and forget it, or partner with Tessian's dedicated team of security experts to optimize for your environment. Tessian is invisible to employees until they need it.

TESSIAN HUMAN LAYER SECURITY PLATFORM MODULES:

PEOPLE MAKE MISTAKES →

TESSIAN GUARDIAN
Accidental Data Loss
Prevent misdirected emails and misattached files.

PEOPLE BREAK THE RULES →

TESSIAN ENFORCER
Data Exfiltration
Prevent unauthorized emails.

TESSIAN ARCHITECT
Intelligent Policies and Custom Protection
Advance your Data Loss Prevention strategy with Automatic and Custom Policies.

OUTBOUND DATA LOSS

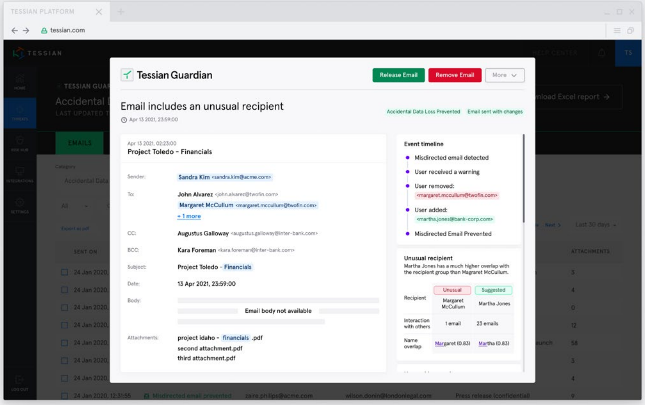
PEOPLE CAN BE TRICKED →

TESSIAN DEFENDER
Impersonation Attacks
Prevent spear phishing, BEC, and other impersonation attacks.

INBOUND EMAIL SECURITY

HUMAN LAYER RISK HUB
Human Layer Risk Management, Made Easy
Deep visibility into risk levels and drivers.

HLS INTELLIGENCE
Insights, Investigation and Remediation
Intelligence to investigate, remediate, and reduce human layer risks.



Tessian Guardian

Release Email | Remove Email | More

Email includes an unusual recipient

Apr 13 2021, 23:59:00

Accidental Data Loss Prevented   Email sent with changes

Apr 13 2021, 02:23:00
Project Toledo - Financials

Sender: Sandra Kim <sandra.kim@acme.com>
To: John Alvarez <john.alvarez@twofin.com>
Margaret McCullum <margaret.mccullum@twofin.com>
+ 1 more
CC: Augustus Galloway <augustus.galloway@inter-bank.com>
BCC: Kara Foreman <kara.foreman@inter-bank.com>
Subject: Project Toledo - Financials
Date: 13 Apr 2021, 23:59:00
Body: Email body not available
Attachments: project idaho - financials .pdf
second attachment.pdf
third attachment.pdf

Event timeline
- Misdirected email detected
- User received a warning
- User removed: <margaret.mccullum@twofin.com>
- User added: <martha.jones@bank-corp.com>
- Misdirected Email Prevented

Unusual recipient
Martha Jones has a much higher overlap with the recipient group than Margaret McCullum.

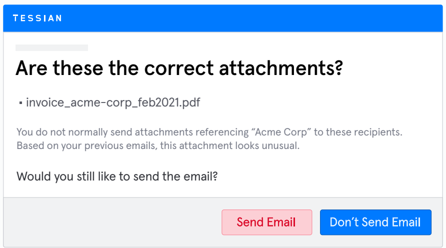
	Unusual	Suggested
Recipient	Margaret McCullum	Martha Jones
Interaction with others	1 email	23 emails
Name overlap	Margaret (0.83)	Martha (0.83)

Tessian Guardian

OUTBOUND DATA LOSS

Tessian Guardian is the industry's only solution that automatically prevents accidental data loss from misdirected emails and misattached files (sending wrong attachments over email).

Guardian compares millions of data points for every outbound email and detects anomalies that indicate whether the email is being sent to the wrong person or if a wrong document is being attached and alerts the user before the email is sent.



TESSIAN

Are these the correct attachments?

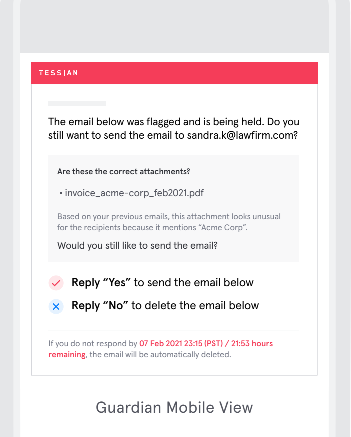
- invoice_acme-corp_feb2021.pdf

You do not normally send attachments referencing "Acme Corp" to these recipients. Based on your previous emails, this attachment looks unusual.

Would you still like to send the email?

Send Email | Don't Send Email

Guardian Desktop View



TESSIAN

The email below was flagged and is being held. Do you still want to send the email to sandra.k@lawfirm.com?

Are these the correct attachments?

- invoice_acme-corp_feb2021.pdf

Based on your previous emails, this attachment looks unusual for the recipients because it mentions "Acme Corp".

Would you still like to send the email?

✓ Reply "Yes" to send the email below

✕ Reply "No" to delete the email below

If you do not respond by 07 Feb 2021 23:15 (PST) / 21:53 hours remaining, the email will be automatically deleted.

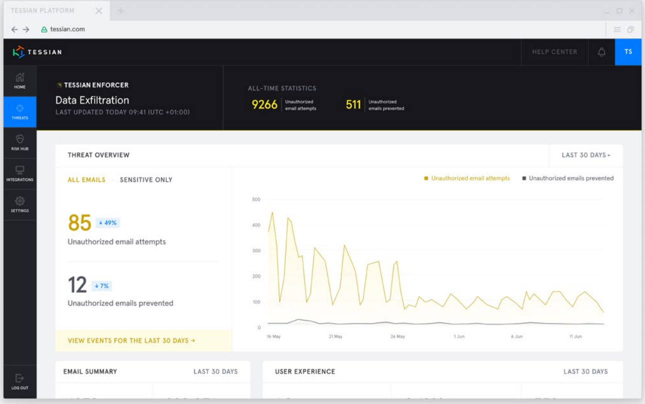
Guardian Mobile View

Tessian Enforcer

OUTBOUND DATA LOSS

Tessian Enforcer is the industry's first solution that uses machine learning to automatically prevent data exfiltration via email to employee personal, unauthorized and non-business accounts.

Powered by Tessian's proprietary Human Layer Security Engine, Enforcer analyzes millions of data points for every outbound email and detects anomalies that indicate data exfiltration before it leaves your organization. Tessian Enforcer notification messages can be customized to reinforce security awareness and data protection policies through in-the-moment training.



TESSIAN ENFORCER
Data Exfiltration
LAST UPDATED TODAY 09:41 (UTC +01:00)

ALL-TIME STATISTICS
9266 Unauthorized email attempts
511 Unauthorized emails prevented

THREAT OVERVIEW   LAST 30 DAYS

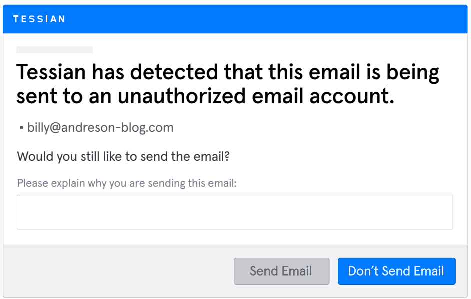
ALL EMAILS   SENSITIVE ONLY

85 ↓ 49%
Unauthorized email attempts

12 ↓ 7%
Unauthorized emails prevented

VIEW EVENTS FOR THE LAST 30 DAYS →

EMAIL SUMMARY   LAST 30 DAYS
USER EXPERIENCE   LAST 30 DAYS



TESSIAN

Tessian has detected that this email is being sent to an unauthorized email account.

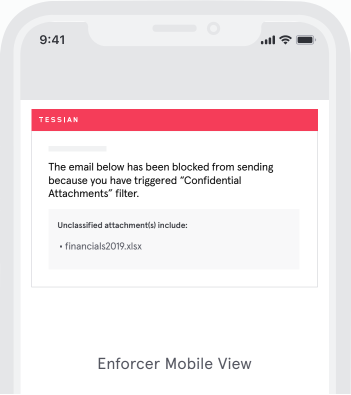
- billy@andreson-blog.com

Would you still like to send the email?

Please explain why you are sending this email:

Send Email | Don't Send Email

Enforcer Desktop View



9:41

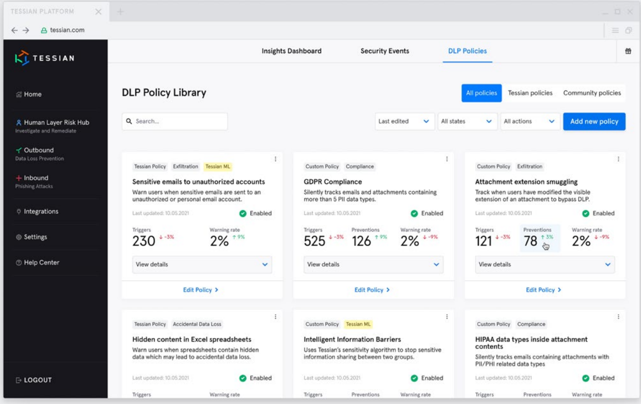
TESSIAN

The email below has been blocked from sending because you have triggered "Confidential Attachments" filter.

Unclassified attachment(s) include:

- financials2019.xlsx

Enforcer Mobile View



TESSIAN PLATFORM

tessian.com

TESSIAN

Home

Human Layer Risk Hub
Investigate and Remediate

Outbound
Data Loss Prevention

Inbound
Phishing Attacks

Integrations

Settings

Help Center

LOGOUT

Insights Dashboard | Security Events | DLP Policies

DLP Policy Library

All policies | Tessian policies | Community policies

Search...

Last edited | All states | All actions | Add new policy

Tessian Policy · Exfiltration · Tessian ML
Sensitive emails to unauthorized accounts
Warn users when sensitive emails are sent to an unauthorized or personal email account.
Last updated: 10.05.2021 · Enabled
Triggers 230 ↓ -3% · Warning rate 2% ↑ 9%
View details
Edit Policy >

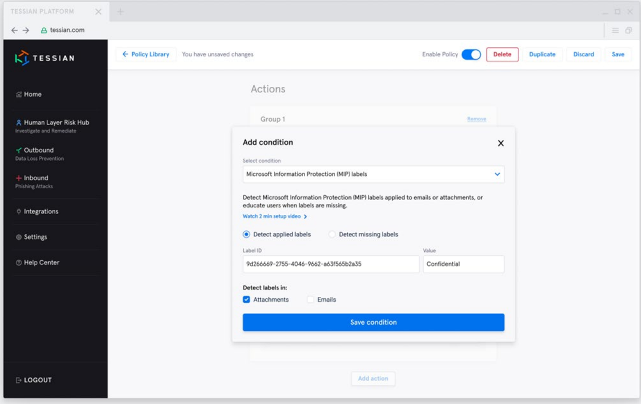
Custom Policy · Compliance
GDPR Compliance
Silently tracks emails and attachments containing more than 5 PII data types.
Last updated: 10.05.2021 · Enabled
Triggers 525 ↓ -3% · Preventions 126 ↑ 9% · Warning rate 2% ↓ -9%
View details
Edit Policy >

Custom Policy · Exfiltration
Attachment extension smuggling
Track when users have modified the visible extension of an attachment to bypass DLP.
Last updated: 10.05.2021 · Enabled
Triggers 121 ↓ -3% · Preventions 78 ↑ 3% · Warning rate 2% ↓ -9%
View details
Edit Policy >

Tessian Policy · Accidental Data Loss
Hidden content in Excel spreadsheets
Warn users when spreadsheets contain hidden data which may lead to accidental data loss.
Last updated: 10.05.2021 · Enabled
Triggers · Warning rate

Custom Policy · Tessian ML
Intelligent Information Barriers
Uses Tessian's sensitivity algorithm to stop sensitive information sharing between two groups.
Last updated: 10.05.2021 · Enabled
Triggers · Preventions · Warning rate

Custom Policy · Compliance
HIPAA data types inside attachment contents
Silently tracks emails containing attachments with PII/PHI related data types
Last updated: 10.05.2021 · Enabled
Triggers · Preventions · Warning rate



TESSIAN PLATFORM

tessian.com

TESSIAN

Home

Human Layer Risk Hub
Investigate and Remediate

Outbound
Data Loss Prevention

Inbound
Phishing Attacks

Integrations

Settings

Help Center

LOGOUT

← Policy Library · You have unsaved changes

Enable Policy · Delete · Duplicate · Discard · Save

Actions

Group 1 · Remove

Add condition

Select condition: Microsoft Information Protection (MIP) labels

Detect Microsoft Information Protection (MIP) labels applied to emails or attachments, or educate users when labels are missing.

Watch 2 min setup video >

● Detect applied labels ○ Detect missing labels

Label ID: 9d266669-2755-4046-9662-a63f565b2a35

Value: Confidential

Detect labels in:

☑ Attachments □ Emails

Save condition

Add action

Tessian Architect

INTELLIGENT EMAIL DLP POLICY ENGINE

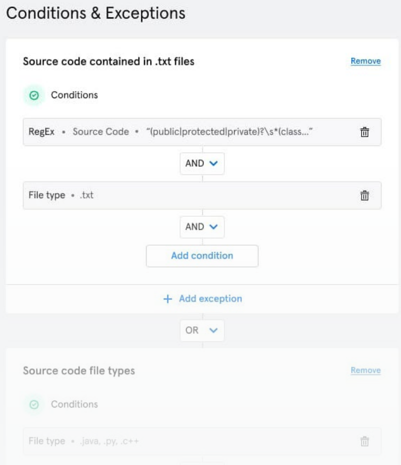
Tessian Architect is a powerful policy engine for real-time email data loss prevention.

It features a combination of the classic elements of DLP policies, as well as intelligent policies that provide custom protection against sensitive data loss.

- Build Intelligent DLP Policies Combining Rules And Machine Learning
- Integrate With Data Classification Tools, Such As Microsoft Information Protection (Mip)
- Choose From A Library Of Prebuilt Policies Or Adopt Best Practices From The Tessian Community

Architect adds deeper capabilities to Tessian's best-in-class Email DLP platform which is the only solution that offers complete protection against any form of data loss through email, whether it's accidental data loss and sensitive data exfiltration to unauthorized parties.

DLP POLICY CAPABILITIES



Conditions & Exceptions

Source code contained in .txt files · Remove

Conditions

RegEx • Source Code • "(public|protected|private)?\s*(class..."

AND

File type • .txt

AND

Add condition

+ Add exception

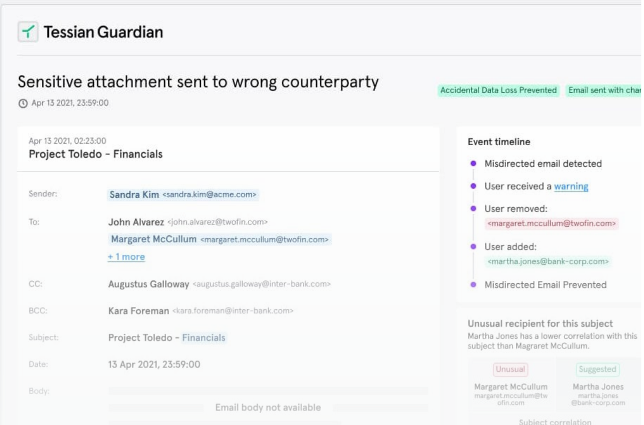
OR

Source code file types · Remove

Conditions

File type • .java, .py, .c++

Customize Rules and Exceptions



Tessian Guardian

Sensitive attachment sent to wrong counterparty

Accidental Data Loss Prevented · Email sent with char

Apr 13 2021, 23:59:00

Apr 13 2021, 02:23:00
Project Toledo - Financials

Sender: Sandra Kim <sandra.kim@acme.com>

To: John Alvarez <john.alvarez@twofin.com>
Margaret McCullum <margaret.mccullum@twofin.com>
+ 1 more

CC: Augustus Galloway <augustus.galloway@inter-bank.com>

BCC: Kara Foreman <kara.foreman@inter-bank.com>

Subject: Project Toledo - Financials

Date: 13 Apr 2021, 23:59:00

Body: Email body not available

Attachments: project idaho - financials .pdf
second attachment.pdf

Event timeline
- Misdirected email detected
- User received a warning
- User removed: <margaret.mccullum@twofin.com>
- User added: <martha.jones@bank-corp.com>
- Misdirected Email Prevented

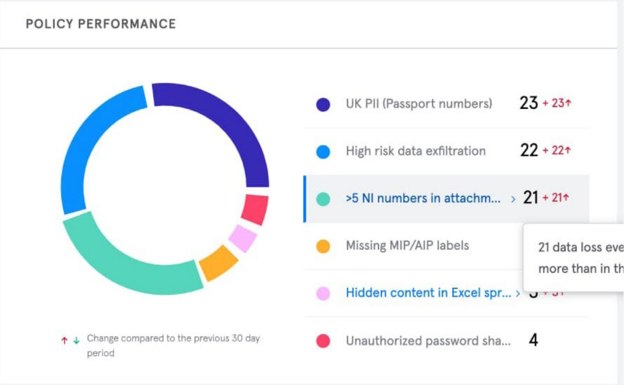
Unusual recipient for this subject
Martha Jones has a lower correlation with this subject than Margaret McCullum.

Unusual: Margaret McCullum, margaret.mccullum@twofin.com
Suggested: Martha Jones, martha.jones@bank-corp.com

Subject correlation

Financials: never exchanged with this recipient
Financials: exchanged 23 times with this recipient

Prevent Sensitive-labeled Content from Leaving the Organization



POLICY PERFORMANCE

UK PII (Passport numbers) 23 + 23↑

High risk data exfiltration 22 + 22↑

>5 NI numbers in attachm... › 21 + 21↑

Missing MIP/AIP labels

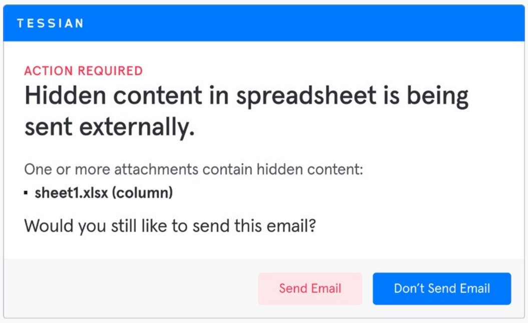
Hidden content in Excel spr... ›

Unauthorized password sha... 4

21 data loss eve
more than in th

↑ ↓ Change compared to the previous 30 day period

DLP Policy Performance Analysis



TESSIAN

ACTION REQUIRED

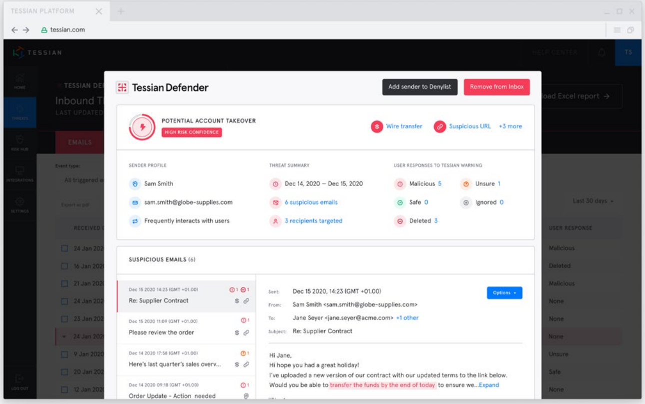
Hidden content in spreadsheet is being sent externally.

One or more attachments contain hidden content:
- **sheet1.xlsx (column)**

Would you still like to send this email?

Send Email · Don't Send Email

Detect Hidden Content in Excel Spreadsheets



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

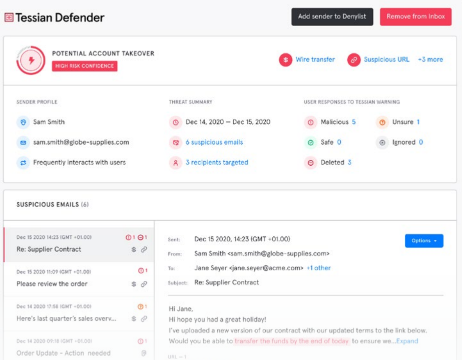
Hi Jane,
Hi hope you had a great holiday!
I've uploaded a new version of our contract with our updated terms to the link below.
Would you be able to transfer the funds by the end of today to ensure we...Expand

Tessian Defender

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 (SEGs), while providing in-the-moment training to drive employees toward secure email behavior.

- Protect against both known and unknown email attacks, including business email compromise, account takeover, spear phishing, and all impersonation attacks that bypass SEGs, M365, and G Suite.
- With Defender's in-the-moment training, organizations can educate and empower users to build continuous email security awareness.
- Remove the burden on your Security Operations Center 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.



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 · 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

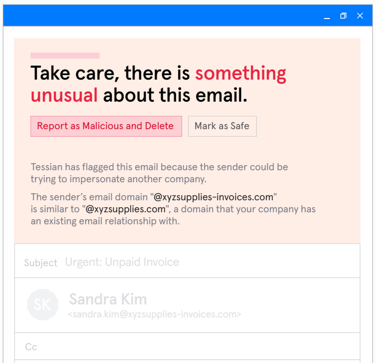
SUSPICIOUS EMAILS (6)

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

Quickly view and remediate account takeover attacks.



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,

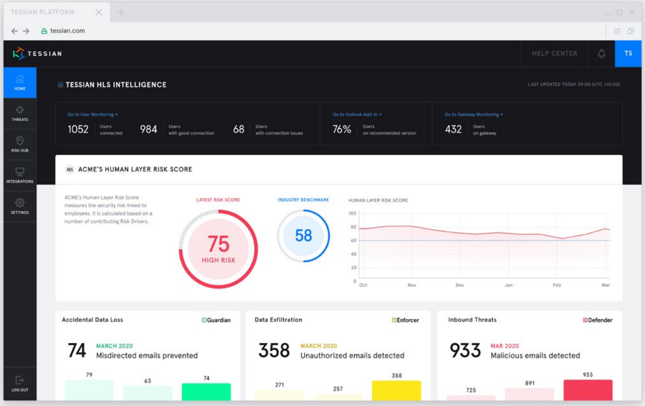
In-the-moment warnings educate employees about malicious emails.

Tessian HLS Intelligence

INVESTIGATE AND REMEDIATE

With Tessian HLS Intelligence, security teams can now readily view curated security events prevented by Tessian with detailed threat breakdowns, make informed prioritization decisions, and respond to threats faster while benchmarking risks against industry peers.

- Insights: Automated insights by inbound and outbound threat categories where you can view top threats and trends, and benchmark against peers.
- Investigation: Detailed event logs and threat breakdown, curated event priorities, and API integrations to connect to your SIEM/SOAR platforms.
- Remediation: Quarantine and post-delivery protection, automated domain blacklisting from shared threat intelligence, and rule-free, single-click domain blacklisting.



TESSIAN HLS INTELLIGENCE

LAST UPDATED TODAY 09:00 (UTC +01:00)

Go to User Monitoring → 1052 Users connected · 984 Users with good connection · 68 Users with connection issues
Go to Outlook Add-In → 76% Users on recommended version
Go to Gateway Monitoring → 432 Users on gateway

ACME'S HUMAN LAYER RISK SCORE

ACME's Human Layer Risk Score measures the security risk linked to employees. It is calculated based on a number of contributing Risk Drivers.

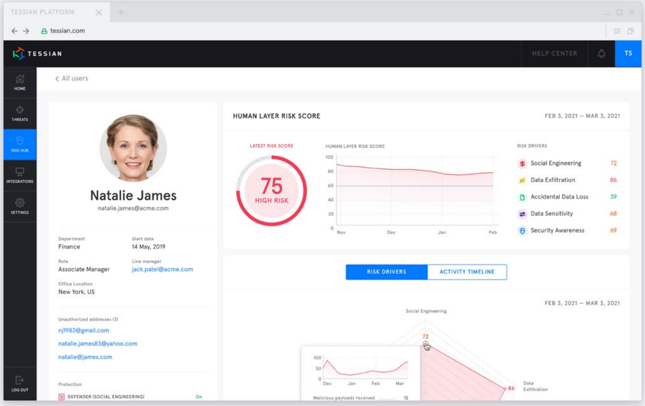
LATEST RISK SCORE: 75 HIGH RISK
INDUSTRY BENCHMARK: 58

Accidental Data Loss — Guardian: 74 MARCH 2020 Misdirected emails prevented

Data Exfiltration — Enforcer: 358 MARCH 2020 Unauthorized emails detected

Inbound Threats — Defender: 933 MAR 2020 Malicious emails detected

Tessian Human Layer Risk Hub



TESSIAN PLATFORM

tessian.com

Natalie James
natalie.james@acme.com

Department: Finance
Start date: 14 May, 2019
Role: Associate Manager
Line manager: jack.patel@acme.com
Office Location: New York, US

Unauthorized addresses (3)
nj1983@gmail.com
natalie.james83@yahoo.com
natalie@james.com

Protection
DEFENDER (SOCIAL ENGINEERING) On

HUMAN LAYER RISK SCORE FEB 3, 2021 – MAR 3, 2021

LATEST RISK SCORE: 75 HIGH RISK

RISK DRIVERS
Social Engineering 72
Data Exfiltration 86
Accidental Data Loss 39
Data Sensitivity 68
Security Awareness 69

FEB 3, 2021 – MAR 3, 2021

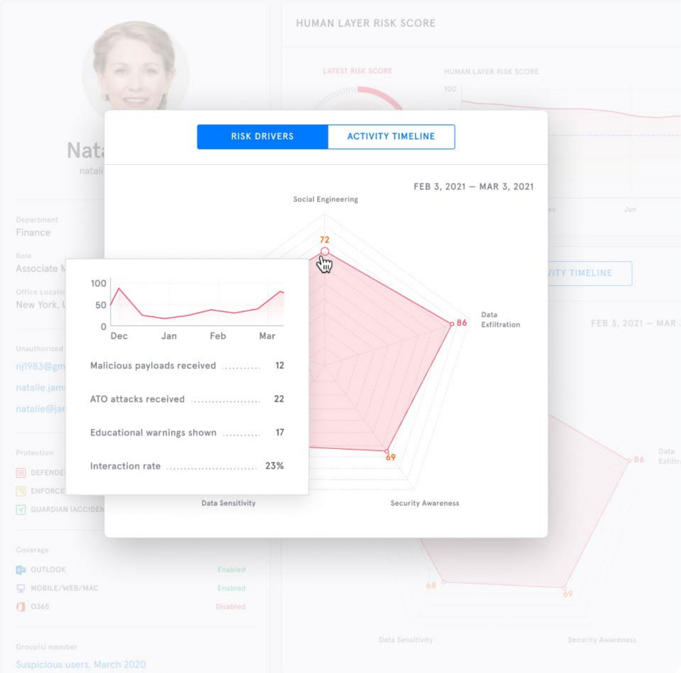
INVESTIGATE AND REMEDIATE

Tessian's Human Layer Risk Hub enables security and risk management leaders to deeply understand their organization's email security posture by providing granular visibility and reporting into individual user risk levels and drivers.

With the Human Layer Risk Hub, SRM leaders will be able to quantify risk levels, pinpoint their high risk user groups, perform targeted remediation at scale, measure impact and demonstrate progress in lowering risks posed by employees.

THE HUMAN LAYER RISK HUB OFFERS:

- Unified Risk View: Email security, training, and risk analytics are offered all in one platform. It delivers a broad spectrum of risk analytics across outbound and inbound email threats and hard to solve problems such as accidental data loss, data exfiltration and advanced phishing attacks, with laser focus on the human layer.
- Unique Risk Insights: Enriched individual risk profiles that are modeled with a broad range of signals from email usage patterns, relationship graphs, security decisions in real time as well as from historical emails. Because of this unique data modeling, Tessian provides a profile that is contextually rich from day 1 of deployment.
- Defensible Audit: Detailed reporting and audit logs provide defensible proof against data breaches. If risk is identified, Tessian's Human Layer Risk Hub enables you to formally document all associated events such as exposure, owner, mitigation decisions and actions.



Malicious payloads received 12
ATO attacks received 22
Educational warnings shown 17
Interaction rate 23%

TESSIAN PROTECTS ENTERPRISE ORGANIZATIONS JUST LIKE YOURS:

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 · Man Group plc

See Tessian in Action.

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

REQUEST A DEMO →

TESSIAN

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 March Capital, Sequoia, Accel, and Balderton.