TESSIAN

TESSIAN CUSTOMER STORY

Inbound and Outbound Email Security For an Enterprise-Level Investment Firm

INDUSTRY	EMPLOYEES	OFFICES	DEPLOYMENT
Professional Services	1,200+	USA, EMEA, Asia	Defender, Guardian, Enforcer

ABOUT JTC

Established in 1987, **JTC** is a global professional services firm specializing in corporate and client services.

With over 1,200 employees, the firm is publicly listed on the London Stock Exchange and FTSE 250 and has over $180 billion assets under administration (AUA).

JTC has been a Tessian customer since 2018.

> *“In the last 18 months, we’ve seen more sophisticated phishing attacks than ever, up at least 50% according to Tessian platform data. These are attacks that slip past other tools like secure email gateways (SEGs) and, without Tessian, they’d likely catch many employees out.“*

Adam Jeffries
CIO AT JTC GROUP

TESSIAN'S 3-YEAR IMPACT:

MINUTES

Tessian is deployed in minutes.

50%

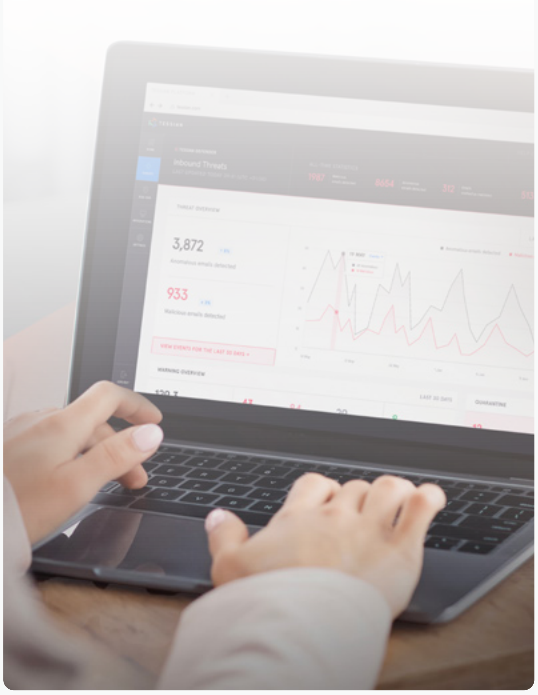
Over 50% increased visibility into phishing attacks.

TWO

Just 2 false positives over 3 years

- Adam and his team knew their current security stack couldn't effectively prevent accidental data loss via misdirected emails and misattached files
- In 2018, with GDPR coming into effect, the firm needed to mitigate email-related cyber risk
- While JTC had legacy phishing solutions in place and offered periodic training, advanced phishing attacks were still landing in inboxes, leaving employees as the last line of defense and the firm vulnerable
- Legacy Data Loss Protection (DLP) and spear phishing solutions needed to be intelligent enough to effectively prevent data loss or successful attacks, and the Total Cost of Ownership (TCO) needed to be low

JTC had seen a spike in advanced phishing attacks in the last 18 months.



Advanced spear phishing attacks like account takeover (ATO) prevented

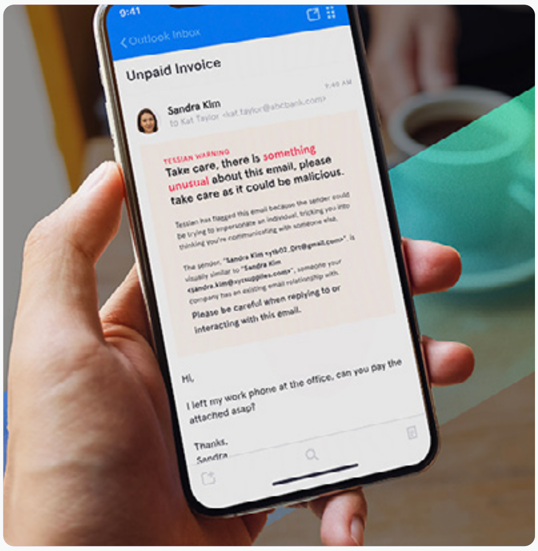
While JTC has been a customer since 2018, they've seen a spike in advanced phishing attacks in the last 18 months.

Bad actors have been taking advantage of fear culture from the pandemic and attacks have been far more targeted, with emails related to collaboration tools like Zoom and vaccine-related attacks. As Adam noted, it's easy to disguise malicious URLs in emails like these and get employees to click on them.

And, with the firm having been working remotely or in a hybrid work environment since early 2020, bad actors have been exploiting support communications, for example pretending to be the IT Helpdesk or HR department.

Finally, ATO attacks have become more and more frequent, and are virtually impossible for employees to spot.

> *"Traditional training and awareness can only go so far. That's where we look at technology solutions like Tessian to help us close the gap."*
>
> Adam Jeffries
> CIO AT JTC GROUP



9:41

< Outlook Inbox

Unpaid Invoice

9:40 AM

Sandra Kim
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 because the sender could be trying to impersonate an individual, tricking you into thinking you're communicating with someone else.

The sender, "Sandra Kim <ytb02_Drt@gmail.com>", is visually similar to "Sandra Kim <sandra.kim@xyzsupplies.com>", someone your company has an existing email relationship with.

Please be careful when replying to or interacting with this email.

Hi,

I left my work phone at the office, can you pay the attached asap?

Thanks,
Sandra

With Tessian, JTC have been able to detect and prevent these threats.

Tessian Defender uses machine learning (ML), anomaly detection, behavioral analysis, and natural language processing (NLP) to detect a variety of signals, including unusual sender characteristics, anomalous email sending patterns, malicious payloads, and deep content inspection.

When unsafe emails are detected, employees receive in-the-moment alerts with clear, simple explanations of potential risks. These warnings provide helpful context around why the email was flagged, reinforce phishing awareness training, and help improve security culture.

Preventing human error while protecting sensitive data

Before deploying Tessian, JTC's security stack just could not effectively prevent accidental data loss via misdirected emails and misattached files. And, with GDPR coming into effect, the firm needed to mitigate that type of risk.

With Tessian Guardian, they've been able to successfully prevent a significant number of misdirected emails, and have even received a "thank you" from senior stakeholders who have been saved from inadvertently sending sensitive content to the incorrect recipients.

So, how does Tessian Guardian do it?

When an email is being sent, Guardian's ML algorithm uses deep content inspection, natural language processing (NLP), and heuristics to detect anomalies such as:

- ↗ **Counterparty anomalies:** The email or attachment is related to a company that isn't typically discussed with the recipients.
- ↗ **Name anomalies:** The email or attachment is related to an individual who isn't typically discussed with the recipients.
- ↗ **Context anomalies:** The email or attachment looks unusual based on the email context.
- ↗ **File type anomalies:** The attachment file type hasn't previously been shared with the receiving organization.

> *"Although it sounds like a throw away comment, when people ask me about Tessian, my response is 'it does what it says on the tin'. Tessian Guardian effectively prevents misdirected emails, helps us remain compliant, and consistently educates users. It's staggering actually, when you first deploy it. I thought "Blimey, we've stopped all of these misdirected emails!!?". You do start to ask yourself, what was happening in the years and months prior, before implementing Tessian?"*
>
> Adam Jeffries
> CIO AT JTC GROUP

Shining a light on workarounds and data exfiltration attempts, without disrupting employees

In March 2020, when employees started working from home, JTC wanted to ensure employees complied with the company policies in place to protect sensitive data.

There were very real challenges presented as they moved so quickly into a ‘work from home’ model and needed to adjust company policies and implement new IT policies. For example, preventing employees from printing remotely.

There were occasions where employees found this particularly restrictive, and would look to find ways around the policy. They would attempt to email documents to their personal email addresses.

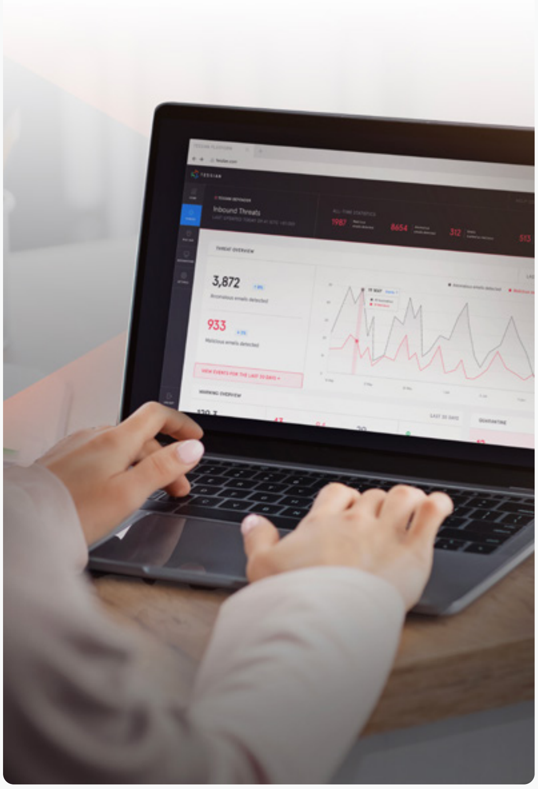
This was a huge concern to JTC. When information is on someone’s personal device, there’s no MFA or encryption. It’s a big threat vector and compliance risk.

Tessian Enforcer – which can automatically classify and detect unauthorized email addresses – helped JTC manage this risk with just two false positives in over 3 years.

Better still, the JTC Information Security team were able to set specific rules within the platform to automatically block employees attempting to send sensitive information to a personal account.

TWO

Tessian helped JTC manage data exfiltration with just two false positives in over 3 years.



Taking a more targeted approach with in-the-moment warnings and threat insights

In addition to detecting and preventing threats, Tessian also provides threat insights that help JTC's security team make more informed decisions about their security strategy.

For example, with the Risk Hub, JTC can hone in on three things related specifically to spear phishing attacks:

They can identify those people who seem to be getting targeted more frequently than others. From there, they can help them understand the risk, and encourage them to be extra cautious with what information they share online (for example, their email address), and vigilant when it comes to inspecting potential threats that land in their inbox.

They can also identify those people who aren't engaging with the warning messages when a spear phishing attack is detected. Instead of doing firm-wide, generalized security awareness, they can create more targeted programs, and identify employees who may need some extra help.

Finally, they can actually see how behavior changes over time. If an employee wasn't engaging with Tessian warning messages, but started to after receiving more targeted training, the Information Security team can actually see and quantify the impact of their efforts.

"Traditional training and awareness can only go so far. That's where we look at technology solutions like Tessian to help us close the gap."

Adam Jeffries
CTO AT JTC GROUP

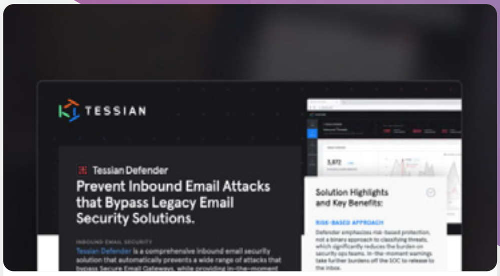
"Tessian uses very advanced technology. The old-fashioned way is to use rule-based tools. You have a human being attempting to think of every angle and then setting up rules to combat them,. With Tessian, this is all done using advanced technology, machine learning, which is far more flexible, targeted, and adapted. It allows us to avoid a huge administrative burden and mistakes being made."

Adam Jeffries
CIO AT JTC GROUP

Learn More About How Tessian Prevents Human Error on Email.

Tessian's mission is to secure the human layer by empowering people to do their best work, without security getting in their way.

LOOKING FOR MORE RESOURCES?



TESSIAN

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

Solution Highlights and Key Benefits:

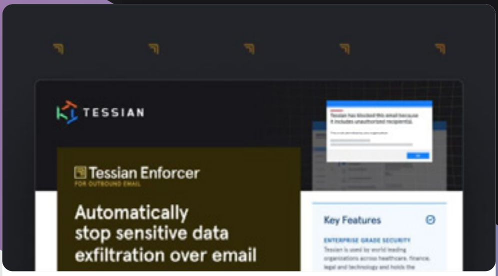
RISK-BASED APPROACH

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.

PRODUCT DATASHEET

Tessian Defender – Prevent Inbound Email Attacks that Bypass Legacy Email Security Solutions.

LEARN MORE →



TESSIAN

Tessian Enforcer

FOR OUTBOUND EMAIL

Automatically stop sensitive data exfiltration over email

Tessian has blocked this email because it includes unauthorized recipient(s).

Key Features

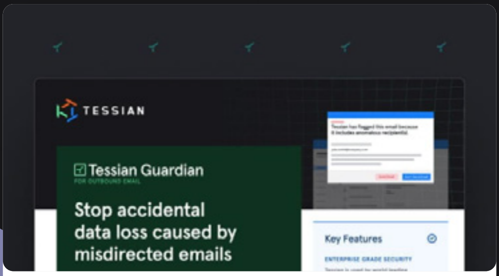
ENTERPRISE GRADE SECURITY

Tessian is used by world leading organizations across healthcare, finance, legal and technology and holds the

PRODUCT DATASHEE

Tessian Enforcer – Automatically Stop Sensitive Data Exfiltration Over Email.

LEARN MORE →



TESSIAN

Tessian Guardian

FOR OUTBOUND EMAIL

Stop accidental data loss caused by misdirected emails

Tessian has flagged this email because it includes anomalous recipient(s).

Key Features

ENTERPRISE GRADE SECURITY

Tessian is used by world leading

PRODUCT DATASHEET

Tessian Guardian – Stop Accidental Data Loss Caused by Misdirected Emails and Misattached Files.

LEARN MORE →

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.

Oct 2021