



Tessian Case Study



Premier

“Tessian’s technology has transformed our security protocol. We used to manually monitor for personal addresses so we could ensure sensitive emails weren’t being sent outside of our organization. This process was laborious and not particularly effective, as it only looked at one potential security threat. This is a much more comprehensive and effective system.”

---

**Kevin Strange**  
Head of IT

## Tessian Filters Deployed



### To Prevent Misdirected Emails →

**Guardian** uses stateful machine learning to automatically prevent highly sensitive emails being sent to the wrong recipients due to inadvertent human error.



### To Prevent Unauthorized Emails →

**Enforcer** uses stateful machine learning to automatically prevent highly sensitive emails being sent to unauthorized and personal email accounts.

---

**Premier Asset Management** is a fast-growing UK retail asset management group with a focus on delivering good investment outcomes for investors through relevant products and active management. Its range of investment strategies include multi-asset, equity and absolute return funds.

Enterprises face increased pressure to control, monitor and restrict the movement of their data. Premier Asset Management, a fast-growing UK retail asset management group, maximizes their resources to ensure they have the tools in place to do so.

Premier Asset Management cares about resource maximization. The UK firm aims to deliver good value to its clients through generating long-term investment outcomes, offering a range of strategies to produce either income, capital growth or a combination of both. Premier Asset Management turns to Tessian to provide effective, tailored solutions – all with high returns at a minimal cost.

Tessian's machine intelligent security platform protects against email-related data loss, while making the most effective and efficient use of resources. Its core technology is the Tessian Relationship Graph. By applying machine intelligent algorithms to historic email data, Tessian extracts metadata to learn about users' unique relationships with their contacts.

This mapping of baseline conversation patterns is then used to automatically detect inconsistencies and deviations from normal activity, which could signal a security threat. When abnormal activity occurs, the appropriate filters ensure that emails can be traced, redacted, kept confidential, or have appropriate access restrictions imposed on them – all without administrative burden.

Tessian Guardian and Enforcer filters perform real-time, automatic analysis of outbound emails, preventing information from being accidentally or deliberately sent outside the secure confines of an enterprise network.

Email security breaches can occur where there is malicious intent, such as when a person who is leaving a company sends client or competitive data to their personal account. However, these breaches can also occur when employees with good intentions send documents to their personal accounts to finish up work over the weekend.

Premier Asset Management depends on Enforcer to address these problems by preventing people from sending highly sensitive data to personal, or unauthorized, email accounts.

---

[Request a Demo](#)

[Talk to an Expert →](#)

Making email safe at:

 Investec

DACbeachcroft

CLYDE&CO

K&L GATES

 Intertrust

 BLM

fieldfisher

 Charles Russell  
Speechlys

Step toe

 大成 DENTONS

A&L Goodbody

Mishcon de Reya

 JTC

HILL DICKINSON

BRACEWELL

Horwich  
Farrelly

Kelley  
Drye

 QUILTER CHEVIOT  
INVESTMENT MANAGEMENT

 PREMIUM  
CREDIT

 BM  
BROOKS MACDONALD

rightmove 

 PRUDENTIAL

WILLIAM FRY

jmw

 havenpower

CVC

 arendt

CHOATE

ArmstrongWatson<sup>®</sup>  
Accountants, Business & Financial Advisers

 BMA



Tessian is building the world's first Human Layer Security platform to automatically secure all human-digital interactions within the enterprise. Today, our products use stateful machine learning to protect people using email and to prevent threats like spear phishing, accidental data loss due to misdirected emails, data exfiltration and other non-compliant email activity. We've raised \$60m from legendary security investors like Sequoia and Accel and have over 150 employees located in New York, San Francisco and London.

[tessian.com](https://tessian.com)