TESSIAN

Defend

Rules Don't Stop Advanced Email Threats

For attackers, phishing links and malware are no longer effective means of breaching organizations through email. Instead, they're bypassing email security rules by impersonating employees and business partners in order to intercept payments and sensitive data. Highly targeted BEC and spear phishing attacks, using the latest techniques in personalization and scale are now today's norm.

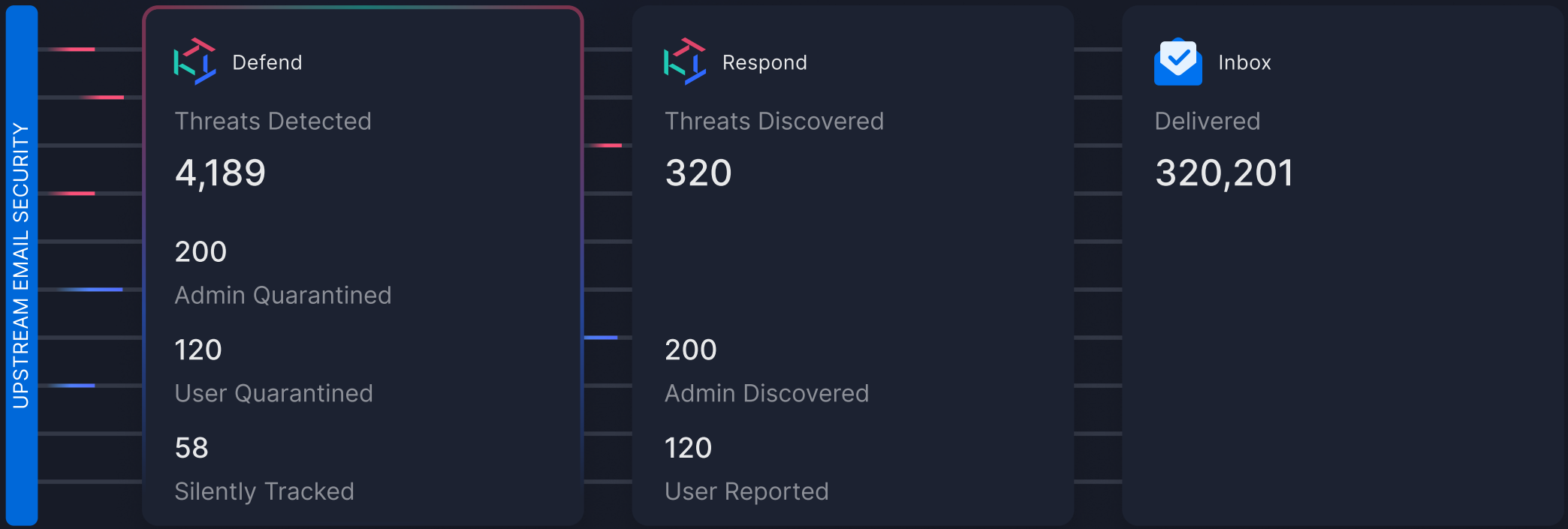
Tessian Uses AI to Stop Advanced Email Threats

Tessian AI detects sophisticated, targeted email threats, and is purpose built to stop attacks that can't be caught with signatures or rules. It uses an ensemble model consisting of multiple machine learning models including:

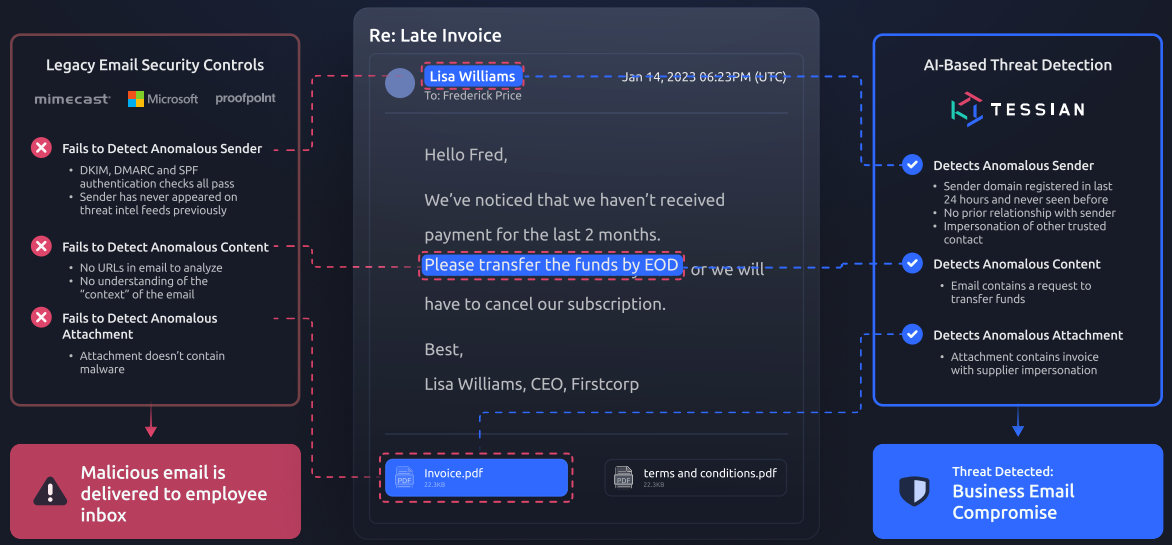
- Deep learning
- Large language models
- Natural language processing

Defend Against Advanced Phishing Attacks

- Business Email Compromise
- QR Code & Image Attacks
- Vendor Account Takeover
- Internal Account Takeover
- Employee Impersonation
- Account Takeover
- Credential Theft
- Financial Fraud
- Domain Spoof
- Ransomware
- Malware
- +More



Allowing Tessian to stop email security threats that legacy solutions can't



"Tessian provides an AI approach to phishing which is much more effective than Mimecast and O365"

Trusted by World Leading Organizations

BlackRock · Evercore · Investec · affirm · RAND Merchant Bank · APEX · ICE NYSE · REALPAGE · cordaan

Tessian Intelligence Ensemble

CONTENT ANALYSIS

Tessian LLMs and hundreds of data points within each email are used to determine if the email is safe, malicious, or needs review

BEHAVIORAL ANALYSIS

Thousands of learned events over email create a strong foundation for normal vs. abnormal communications.

THREAT NETWORK ANALYSIS

Third party threat feeds and data from our customer network are leveraged to stop attacks in minutes



Email Platforms

Integrations

splunk> · KnowBe4 · okta · sumo logic

Deployment

API · COM Add-in · Gateway