Email security is no longer limited to securing an organization’s own email platform and its users. There is a growing trend where attackers gain access to the email account of a trusted sender (a customer, a business partner, or a supplier), impersonate the sender and use it to conduct fraudulent activities. This is called Account Takeover (ATO) and it is one of the pathways to Business Email Compromise (BEC).

External ATO attacks have repeatedly demonstrated that rule-based threat detection tools and email authentication (DMARC, DKIM, SPF) are ineffective in detecting and stopping them. This is because these emails originate from trusted external accounts and exploit the trust between business entities and individuals.

ATO threats call for a differentiated approach for detecting:

1. Anomalous geophysical location, time, IP, email client; impossible to travel locations and unusual reply-to addresses
2. Anomalous email sending patterns: Emails sent to an unusual number of recipients, to unusual recipients, and at unusual times
3. Suspicious email payloads by spotting language that conveys intent with NLP
4. Suspicious URLs (machine learning to identify URL match patterns)
5. Suspicious attachments (machine learning to identify common red flags)

**New Defender Features**

**MACHINE LEARNING-POWERED ANOMALY DETECTION**
Tracks user behavior and detects even the most subtle anomalies that might signal an attack at the first instance of an attempt.

**MODELING**
The Tessian ML algorithm continuously analyzes and learns from email communications across its global network to build profiles / models of companies and their employees to understand what their normal email communication looks like. This helps catch the most subtle ATO attacks.

**RAPID REMEDIATION**
Real-time alerts of ATO events to dedicated mailboxes. Explainable machine learning helps SOC teams understand quickly why an email has been classified as malicious. By aggregating similar events and grouping emails from the same compromised account, Tessian allows administrators to clawback/delete multiple events with a single click.

**END-USER EDUCATION**
Best-in-class email security starts with continuous and contextual employee education. Tessian delivers this with simple, in-the-moment alerts that educate users on secure email behavior.

**Tessian Defender** offers automated protection against external account takeover threats.