REPORT REPRINT

Tessian uses AI and machine learning to address the human side of phishing and email attacks

FEBRUARY 18 2020

By Garrett Bekker

The company is one of several new takes on data loss prevention that look to leverage new capabilities in AI, machine learning and natural language processing to deliver more effective DLP to prevent human error in emails. We see Tessian as both complementary and competitive to traditional DLP offerings, and thus a potential partner as well as acquisition.

451 Research®
Now a Part of
S&P Global Market Intelligence

Introduction

Tessian is one of several new takes on data loss prevention (DLP) – dare we say 'next-gen'? – that we have chronicled in recent reports (Armorblox, Code42) that look to leverage new capabilities in AI, machine learning and natural language processing (NLP) to deliver more effective DLP. While security has historically focused on the machine layer, Tessian cites data that show that 88% of data breaches are due to human error. To that end, Tessian has developed what it calls the world's first human layer security platform to prevent human error in emails.

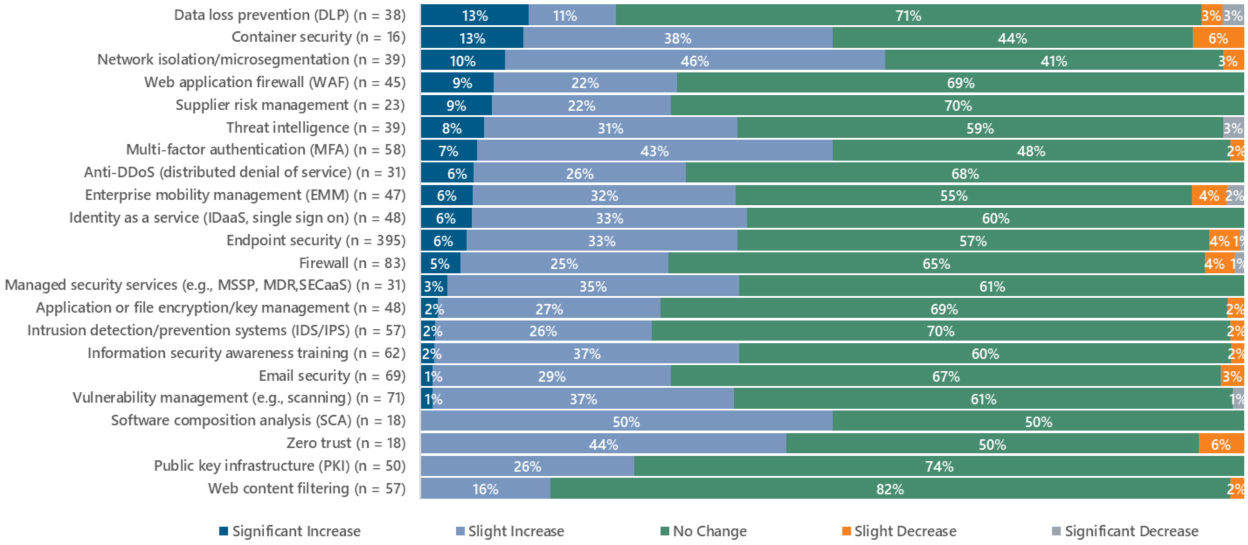
451 TAKE

As we have argued in other recent reports, we believe the DLP market is ripe for change and are encouraged by the emergence of new perspectives that can address new DLP use cases. Candidly, AI and machine learning are becoming almost commonplace in security, and we suspect that will also be true of legacy DLP and data classification vendors in time. In that sense, we see Tessian as both complementary and competitive to traditional DLP offerings, and thus a potential partner as well as a potential acquisition. AI and ML also present problems with respect to competitive differentiation – how to tell when one application of AI or ML is more effective than another? Early market traction and high-profile backing would suggest that Tessian is on the right track.

Context

According to research from 451 Research's Voice of The Enterprise (VoTE) Information Security, Workloads & Key Projects survey, DLP was ranked at the top of the list of over 20 security categories that are expected to see a 'significant' increase in spending in the next 12 months, by 13% of respondents. Unfortunately, however, DLP technology has developed a reputation as much for inaccuracy, false positives and poor performance as it has for protecting data.

Figure 1: How will your spending on the following change in the next 12 months?



Source: 451 Research, Voice of The Enterprise (VoTE) Information Security, Workloads & Key Projects, Q1 2019

London-based Tessian (fka CheckRecipient) was founded in 2013 by CEO Tim Sadler, CTO Ed Bishop and head of client-side engineering Tom Adams, all of whom attended Imperial College London and served brief stints as financial analysts before forming Tessian. The company currently has 180 employees in London and San Francisco. Most of its 250 customers range from SMB to enterprise, the largest of which has over 10,000 users. Average deal sizes hover around $50,000, although larger deals can range from $500,000-$1m and are trending upwards as Tessian pursues several deals north of 100,000 seats. Tessian has raised a total of $60m from blue-chip VCs such as Sequoia ($42m series B in 2019) and Accel Partners ($13m series A with Balderton).

Products

Tessian DLP applies 'stateful' machine learning techniques to historical email messages (headers, body and attachments) to understand relationships and establish normal behavior profiles that can be used to distinguish between safe and unsafe emails. Like some other emerging DLP vendors, Tessian's focus is on finding abnormal human behavior to protect sensitive data, and as such relies on machine learning to find anomalies rather than trying to discover data using regex searches, fingerprinting or optical character recognition (OCR), as many existing data discovery and DLP tools do. Architecturally, Tessian relies on both agents and gateway appliances to analyze data, similar to most existing DLP tools.

While the latter are good at finding personally identifiable information (PII) like credit card, driver's license and social security numbers, finding and blocking actions such as employees sending files to a personal email account are surprisingly challenging and are quickly out-of-date, so predefined rules are not that effective. Tessian prides itself on the depth of its data analysis – for example, Tessian can scan every email header sent historically to a domain or map all IP chains. From a content analysis perspective, Tessian can determine when it may be unusual for an invoice to be sent to a certain person, for example.

Tessian's Human Layer Security portfolio consists of four main products that address multiple use cases, both outbound (accidental and malicious data exfil) and inbound (anti-phishing and advanced impersonation attacks) threats.

Tessian Defender was developed for phishing emails and advanced impersonation attacks, which are notoriously hard to detect. While a standard secure email gateway (SEG) blocks known attacks by scanning links and attachments and applying predefined rules, Defender can check the metadata in the headers and wording within the body content to find subtle differences in usage that could indicate a fraudulent user. Defender is intended to alert on only high-level attacks rather than to send frequent warnings.

Tessian Guardian is all about preventing accidental leakages of data via misaddressing. For example, if a sender makes a typo and the email client auto fills the wrong name, Guardian can look at the user's history of communications and if the address looks unusual relative to historical context, Guardian can hold the email and send a message to the sender confirming the recipient's address – 'Did you really mean to send this to John Doe'? Tessian Enforcer is meant to prevent users from intentionally sending sensitive data out to unauthorized, non-business recipients via emails, such as a client list by someone leaving the company. Enforcer can stop emails from going out to certain addresses and can also put employees on whitelists or blacklists.

Tessian Constructor is a rules-based offering that comes with all Tessian products and lets admins create blacklists, whitelists and also create custom email filters.

Competition

Tessian's most likely competition will come from traditional DLP vendors such as Broadcom (Symantec/Vontu), McAfee, Forcepoint and Digital Guardian, as well as smaller or regional players like CoSoSys, Clearswift and GTB Technologies. Newer entrants such as Armorblox, Altitude Networks, Code42 and MessageControl also have new takes on DLP that generally look to apply new techniques such as AI, machine learning, NLP and natural language understanding (NLU) to traditional DLP and email security use cases.

Armorblox has attempted to draw on its ability to leverage NLP and NLU to analyze actual message content as opposed to common methods that focus on scanning email links, attachments and header information. Altitude Networks' Cloud-Native DLP is designed to control unauthorized access to and sharing of cloud data in cloud collaboration apps like Box or Dropbox by leveraging AI and machine learning to analyze metadata to both identity false positives and discover attacks that existing tools might miss. Chicago-based MessageControl also applies AI to address social engineering and employee errors and combat unintended data exfiltration.

After several years of dabbling in DLP, former backup vendor Code42 has now fully embraced DLP with an offering that leverages its capabilities around data retention and retrieval to better focus on protection (i.e., detection and response) and insider threats as opposed to standard DLP prevention (active blocking). Code42 can investigate activities like corporate changes (M&A) or departing employees to look for abnormal file activity, such as somebody moving files, saving files where they shouldn't, accessing files they shouldn't or taking sensitive data with them when they leave.

SWOT Analysis

STRENGTHS

Tessian can detect subtle impersonation attacks and prevent human errors that are difficult to detect with standard DLP techniques such as regex searches, fingerprinting or OCR.

WEAKNESSES

Tessian works across email platforms only. and does not yet cover collaboration platforms like Box or Dropbox.

OPPORTUNITIES

We see Tessian as potentially complementary to traditional DLP offerings as well as competitive, and thus could be a potential partner as well as a potential acquisition.

THREATS

Many established and emerging security vendors have incorporated AI and machine learning into their offerings, and we suspect that will also be true of traditional DLP and data classification vendors.