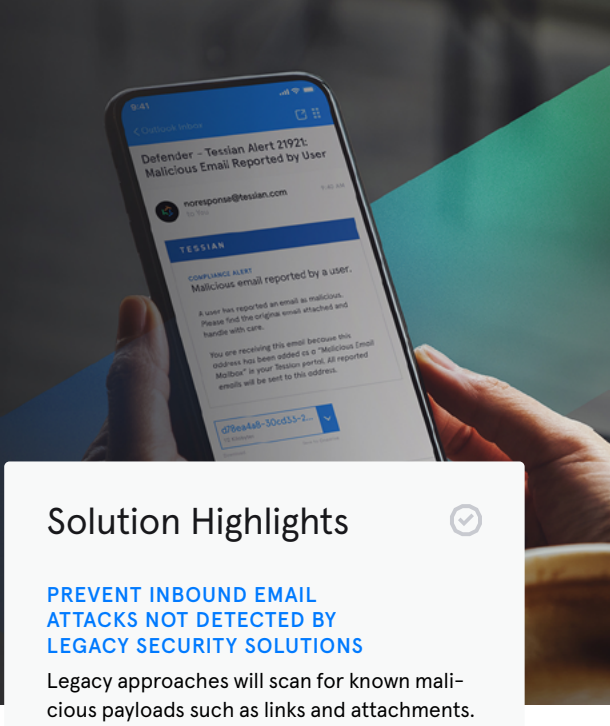
TESSIAN

TESSIAN PRODUCT AND INTEGRATIONS

Tessian Human Layer Security for Microsoft Office 365



Tessian's Human Layer Security platform is designed to enhance the rule-based and sandbox approaches of Microsoft 365 Defender (ATP), to detect and stop *newer* and *previously unknown* attacks from external sources, domain, brand, and service impersonations, **and** data loss by internal users.

Why are O365 accounts so vulnerable to attacks?

Exchange Online/Outlook - the cloud email application for Microsoft Office 365 users - has always been a breeding ground for phishing, malware, and very targeted data breaches.

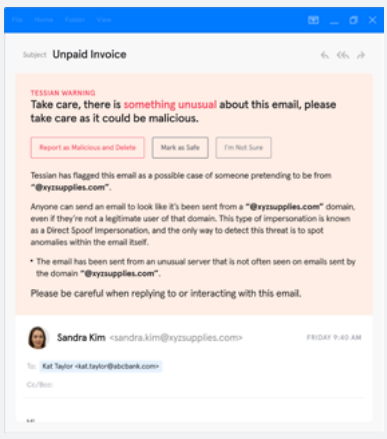
Though Microsoft has been ramping up its O365 email security features with Advanced Threat Protection (ATP) as an additional layer to Exchange Online Protection (EOP), both tools have failed to meet expectations because of their inability to stop newer and more innovative social engineering attacks, business email compromise (BEC), and impersonations.

One of the biggest challenges with ATP in particular is its time-of-click approach, which requires the user to click on URLs within emails to activate analysis and remediation.

Is O365 ATP enough to protect my email?

Microsoft O365's native security controls can provide basic protection against bulk phishing scams, spam, malware and domain spoofing. They are best at broad-based, high-volume and low-effort attacks. However, this protection is baseline protection.

For example, Tessian Defender can be used successfully with Microsoft EOP, to cover phishing, spear phishing and account takeover attacks, while EOP handles bulk spam and phishing attacks. In this cast, the best combination is Defender + Microsoft ATP to provide optimal layered protection against advanced email attacks.



Solution Highlights

PREVENT INBOUND EMAIL ATTACKS NOT DETECTED BY LEGACY SECURITY SOLUTIONS

Legacy approaches will scan for known malicious payloads such as links and attachments. This leaves these defenses vulnerable to zero-day threats, or attacks without payloads. Tessian will inspect the context of the email to determine indicators of an attack, notify the user, therefore not giving an opportunity of malware slipping through or the user to click. This moves Tessian up the kill chain to stop attacks.

RISK-BASED APPROACH

Tessian emphasizes risk-based protection, not a binary approach to classifying threats, which significantly reduces the burden on security ops teams.

CONTEXT-AWARE SECURITY

Tessian uses natural language processing (NLP) algorithms to perform a content x-ray that detects indicators of attack such as malicious intent, impersonation, compromise, and payloads, resulting in more accurate security decisions.

IN-THE-MOMENT TRAINING

Non-disruptive *in-the-moment training and awareness* is provided to employees through contextualized, easy to understand warning messaging.

FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS

Tessian deploys in minutes and automatically prevents data breaches through email within 24 hours of deployment, across all devices, desktop and mobile.

DID YOU KNOW?

Malicious URLs consistently bypass ATP. Attackers use automation to make small, random modifications to existing malware signatures and use transformation techniques to bypass these native O365 security tools.

Office O365 ATP was developed as an overlay security architecture for Exchange Online Protection (EOP), which is the native security tool for O365 mail. Though ATP offers good baseline features against inbound threats such as malware and spam, it lacks the depth of functionality for customers looking to build a comprehensive email security strategy.

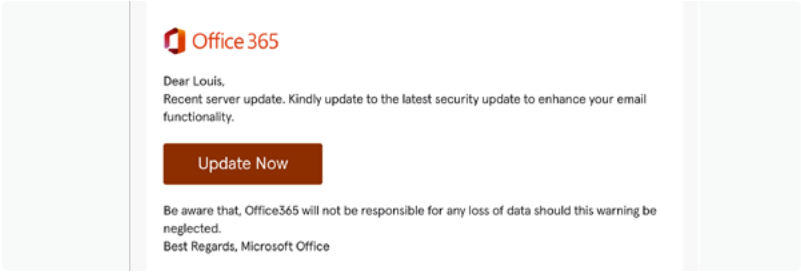
Microsoft uses ML to detect suspicious patterns of data access. However, a lot of its anti-phishing capabilities are dependent on EOP's policy-based filters and ML is limited to the cloud. As with any other data-driven tool, ATP relies on historical knowledge of cyberattacks to detect new ones.

For missed phishing emails, it puts the onus on the trained user to identify phishing attacks and report them back to Microsoft. While it does offer some situational education, organizations still spend time and effort in training end users.

Microsoft acts as an outsourced SOC team by analyzing threats internally, and offers little transparency to its customers in the detailed reporting of threats. The forensics reporting features are at a high level and lack depth.

But, Here's the Problem...

Email attacks have mutated to become more sophisticated and targeted, and hackers exploit user behavior to launch targeted and highly damaging campaigns on people and organizations. Attackers use automation to make small, random modifications to existing malware signatures and use transformation techniques to bypass these native O365 security tools. Unsuspecting - and often untrained - users fall prey to socially engineered attacks that mimic O365 protocols, domains, notifications, and more.



This is an email impersonation attack. The hacker has crafted a believable email, prompting the user to update his or her security controls. But, the link won't lead the user to a genuine page. Instead, they will be led to a look-a-like page where hackers may gain unauthorized access to the user's account. This is often a credential harvesting page. Stolen credentials can then be used to gain access to the account.

It is because such loopholes exist in O365 email security that Microsoft continues to be one of the most impersonated brands in the world.

What are the consequences of a compromised account?

With approximately 180 million O365 active email accounts, organizations could find themselves at risk of a data loss or a breach, which means revenue loss, damaged reputation, customer churn, disrupted productivity, regulatory fines, and penalties for non-compliance. This means they need to quickly move beyond relying on largely rule and reputation-based O365 email filters to more dynamic ways of detecting and mitigating email-originated risks.

How Tessian Enhances O365 Email Security

By dynamically analyzing current and historical data, communication styles, language patterns, and employee project relationships both within *and* outside the organization, Tessian generates contextual employee relationship graphs to establish a baseline normal behavior. By doing this, Tessian turns both your employees and the email data into an organization's biggest defenses against inbound and outbound email threats.

Conventional tools focus on just securing the machine layer – the network, applications, and devices. By uniquely focusing on the *human* layer, Tessian can make clear distinctions between legitimate and malicious email interactions and warn users in real-time to reinforce training and policies to promote safer behavior.

Often, customers ask us which approach is better: the conventional, rule-based approach of Microsoft's native tools, or Tessian's powered by machine learning. **The answer is, each has their unique place in building a comprehensive email security strategy for O365.** But, no organization that deals with sensitive, critical, and personal data can afford to overlook the benefits of an approach based on machine learning and behavioral analysis.

A layered approach that leverages the tools offered by O365 for high-volume attacks, reinforced with next-gen tools for detecting the unknown and evasive ones, would be your best bet. A very short implementation time coupled with the algorithm's ability to 'learn' from historical email data over the last year - all within 24 hours of deployment - means Tessian could give O365 users just the edge they need to combat modern day email threats.

Solution Highlights

THREAT DETECTION

Tessian Defender can detect and stop a variety of inbound threats such as services, brand, vendor, internal, and executive impersonations, preventing a broad spectrum of fraudulent activities (invoice/wire/crypto frauds), thefts (credentials/IP/PII), gift card and bribery attacks, and system compromise (servers, databases, control systems, etc).

EDUCATION AND AWARENESS

The Tessian HLS platform provides contextual, in-the-moment warnings. In addition, you have the ability to automatically warn and educate users on unusual looking emails with configuration options.

FORENSIC TOOLS

Historical analysis shows what threats were received in the past year that got past existing defenses. Tessian's machine learning acquires significant behavioral inputs within 24 hours of deployment.

The Tessian O365 Integration

Tessian today aims to provide a necessary additional layer of security on top of Microsoft's inbuilt functionality – rather than acting as a like-for-like alternative.

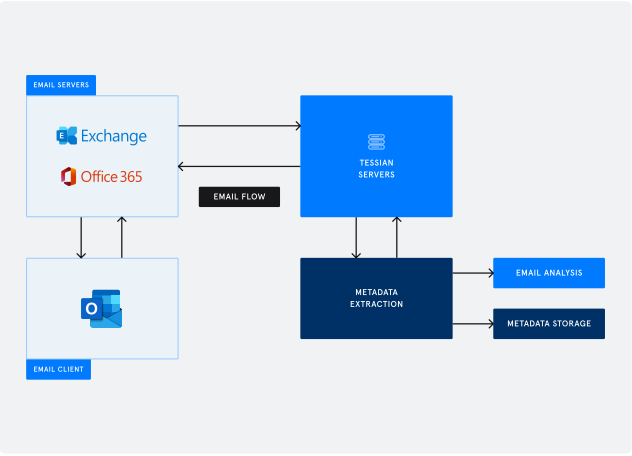
Tessian's platform is built to work alongside either Microsoft, Google or a SEG and leverages Microsoft's Graph APIs to provide additional value to customers. Tessian partners with Microsoft in a number of ways (including Graph API development), and continue to actively develop integration capabilities, including:

- O365 API Integration to sync historical email data
- Microsoft Active Directory integration to sync user group data into Tessian
- O365 Azure Directory integration to sync organizational groups and roles into Tessian
- O365 API integration to view full email body via the Tessian Platform (Defender)
- Ongoing work to integrate closely with Microsoft Azure Information Protection (AIP)/Microsoft Information Protection (MIP) and use data to inform Tessian's predictions.

The Tessian integrations for O365 allows Tessian to connect to part of your O365 domain that you give it access to. This allows Tessian, for instance, to analyze your users' mailboxes and detect the spear phishing emails they received that weren't blocked by your existing email security, or to detect past data exfiltration attempts.

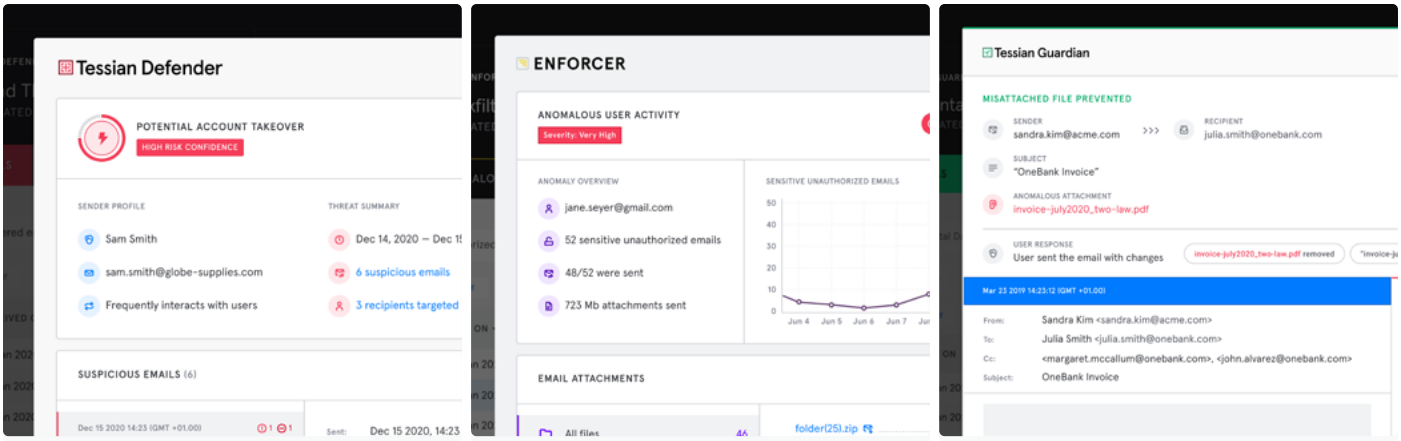
Once you've specified which of your users' mailboxes you wish Tessian to analyze, the Tessian integrations will upload copies of emails that the specified users sent and received in the past 12 months, to Tessian's servers.

There, metadata required for analysis is extracted from the emails. This metadata includes email headers, URLs, phrases indicating malicious intent, and attachment names. Tessian saves this metadata and never stores exact copies of the full email. Tessian's algorithms then analyze the extracted email metadata to produce a threat report.



TESSIAN HUMAN LAYER SECURITY PLATFORM

Explore the Human Layer Security Platform Modules



PREVENT INBOUND EMAIL ATTACKS

Tessian Defender

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 training to drive employees toward secure email behavior.

LEARN MORE →

STOP DATA EXFILTRATION

Tessian Enforcer

Automatically prevent data exfiltration over email. Whether it's careless, negligent or malicious, Enforcer automatically detects data exfiltration and non-compliant activities on emails. No rules required.

LEARN MORE →

AUTOMATICALLY PREVENT DATA LOSS

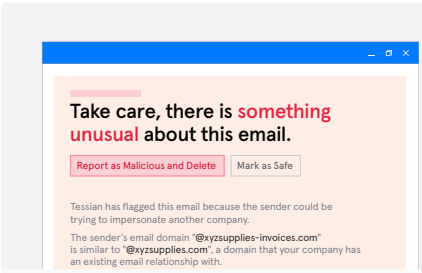
Tessian Guardian

Stop accidental data loss from misdirected emails and misattached files before they happen. Ensure the right email is shared with the right person and prevent data breaches that are impossible to detect with legacy DLP controls.

LEARN MORE →

TESSIAN FOR SECURITY AWARENESS TRAINING

In-the-Moment Training to Stop Email Attacks and Data Loss Where They Start.

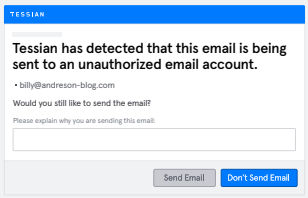


PREVENT INBOUND EMAIL ATTACKS

Tessian Defender

When unsafe emails are detected, employees can either receive in-the-moment alerts with clear, simple explanations of potential risks or emails can be directly quarantined for inspection and approval by Security Analysts.

LEARN MORE →

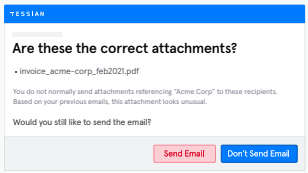


STOP DATA EXFILTRATION

Tessian Enforcer

Real-time warnings are shown to employees when data exfiltration threats are detected. Warning triggers can be tailored to suit your company's security policies and workflow requirements; employees can be warned, emails can be blocked, or activity can be silently tracked.

LEARN MORE →



AUTOMATICALLY PREVENT DATA LOSS

Tessian Guardian

As misdirected emails and incorrect attachments are detected, employees are alerted in real-time with clear, simple explanations and precise reasons for anomalies and correct recipients are suggested. This way, they can correct the recipient(s) and review attachments before the email is sent.

LEARN MORE →

FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS:

Exchange · Office 365 · G Suite · splunk> · Radar · exabeam · SGS · AICPA SOC · DUO · ALIEN VAULT · RAPID7 · RSA

TRUSTED BY ENTERPRISE CUSTOMERS ACROSS ALL INDUSTRIES:

EVERCORE · arm · PRUDENTIAL · REALPAGE · affirm · Schroders · rightmove · Investec · GRAPHCORE · sanne · K&L GATES · cordaan · DENTONS · fieldfisher · ERT · CLYDE&CO · BRACEWELL · gubra · Intertrust · ManGroup plc

See Tessian in Action.

Book a demo and see first hand how Tessian's Human Layer Security Platform detects inbound and outbound email attacks that bypass legacy email security solutions.

REQUEST A DEMO →

TESSIAN | Human Layer Security

TESSIAN.COM

Tessian's mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error – like data exfiltration, accidental data loss, business email compromise and phishing attacks – with minimal disruption to employees' workflow. As a result, employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like Sequoia, Accel and Balderton and has offices in San Francisco and London.

May 2021