

# Microsoft + Tessian: Comprehensive Email Security



SEGs are redundant and do not offer protection against advanced social engineering based attacks. Microsoft and Tessian together offer comprehensive email security to replace your SEG.

## The Problem: SEGs are no longer fit for purpose in an increasingly complex threat environment

Secure Email Gateways (SEGs) are considered legacy IT technology. With the move of email to the cloud, enterprises have access to native SEG capabilities, including threat intelligence, in Microsoft 365. Enterprises integrate SEGs into their environments to improve email security, for spam filtering, as well as for malicious URL and attachment protection.

SEGs typically offer the following features:

- Malware protection
- Spam protection
- Basic phishing protection
- Attachment sandboxing
- URL rewriting/ Time of click protection
- Link following/URL tracking
- Email data loss prevention (DLP)
- Archiving

*"What we saw after our Proof of Value with Tessian was exciting, but also quite scary. We saw things that we didn't actually know were happening. Suddenly we had transparency and could see the true scope of the issues we had on email. But, we also saw how employee behavior changes with Tessian."*

**Cas de Bie**  
CIO at Cordaan



## Key Shortcomings of SEGs:

### IN-LINE, STATIC RULE BASED APPROACH

The in-line gateway approach of SEGs renders them sitting ducks, unable to address any risk that bypasses the gateway. SEGs are particularly ineffective at protecting against advanced social engineering based attacks such as CEO impersonation, account takeover (ATO), business email compromise (BEC), spear phishing or insider threat detection.

### NO ZERO DAY PROTECTION

SEGs are notoriously unable to safeguard against zero day attacks because the threat engine relies on known threats only.

### POINT OF FAILURE RISK

SEGs represent a point of failure risk in your IT environment. On-premise SEG appliances are often housed in the same server rack or on the same premises as your email exchange server, which makes SEGs vulnerable to downtime and disaster events.

### HIGH RESOURCE ALLOCATION AND UTILIZATION, WITH DECLINING EFFECTIVENESS

Maintaining SEGs requires dedicated staffing resources to maintain the DNS and MX records, and to triage email threats through post-event threat hunting and forensics. The retroactive nature of threat detection in the current context of ransomware is accelerating the declining effectiveness of SEGs.

### BUSINESS INTERRUPTION AND HIGH USER FRICTION

Business interruption (i.e. broken email flow due to SEG misconfiguration) is a leading customer complaint. So too is the high user friction that SEGs generate by incorrectly blocking legitimate incoming email.

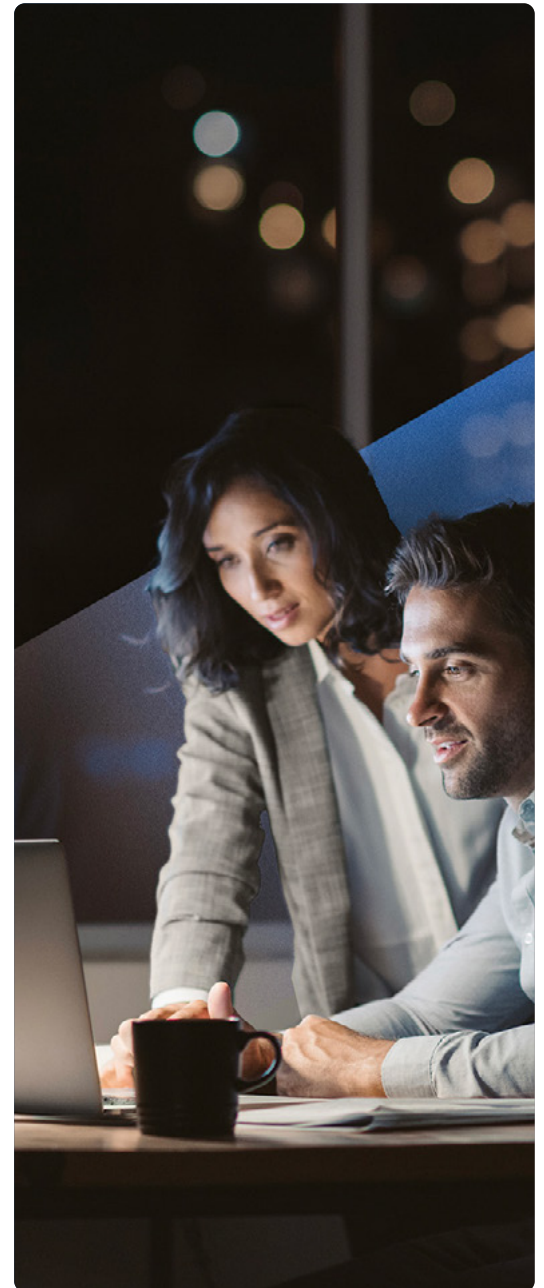
Sitting in-line as the gateway for all received and sent emails in the enterprise, a significant responsibility rests on the effectiveness of SEGs to ensure the integrity of email communication. SEGs prove to be relatively effective at spam filtering and the blocking of unsophisticated phishing attempts.

But due to the increasing sophistication of social engineering based attacks, the position and relevance of SEGs as the principal email security solution is rapidly diminishing. Advanced attacks are able to circumvent the static, rule-based defenses of SEGs. Once a threat has effectively circumvented the gateway, the threat actor is significantly closer to accessing an enterprise's crown jewels.

Threat actors are able to bypass SEGs because of the reliance on threat intelligence, which relies on known lists and signatures of already discovered threats. SEGs do not offer any protection against zero day attacks, and in fact represent a key point of failure in the growing security challenge of email delivered ransomware. Insider threat management is also limited. SEG's also do not offer Email DLP, and are therefore unable to protect you from misdirected email, the wrong attachment being emailed out, or sensitive data from being exfiltrated via email.

The legacy nature of SEGs has been carried into the cloud, too. Relaying Microsoft 365 email through a SaaS SEG solution increases the risk of business interruption due to the overly manual process of changing MX records to ensure email is routed to the correct server. Changing MX records also publicly discloses what email security solution is in use. The static nature also requires continuous maintenance and is ill-suited to organizations that require dynamic scaling. The archiving capability of SEGs is made further redundant by cloud hosted productivity suites like Microsoft 365 providing archiving natively. **Simply stated, SEGs are no longer fit for purpose in an increasingly complex threat environment.** This is why enterprises are consolidating their email security stack and selecting next-gen solutions that enhance Microsoft 365's native capabilities – enabling comprehensive protection through a defense in depth approach.

Enterprises might not be aware of the SEG redundancy in their IT environments. The typical enterprise is running a SEG in parallel to Microsoft 365 or some other cloud hosted productivity suite.

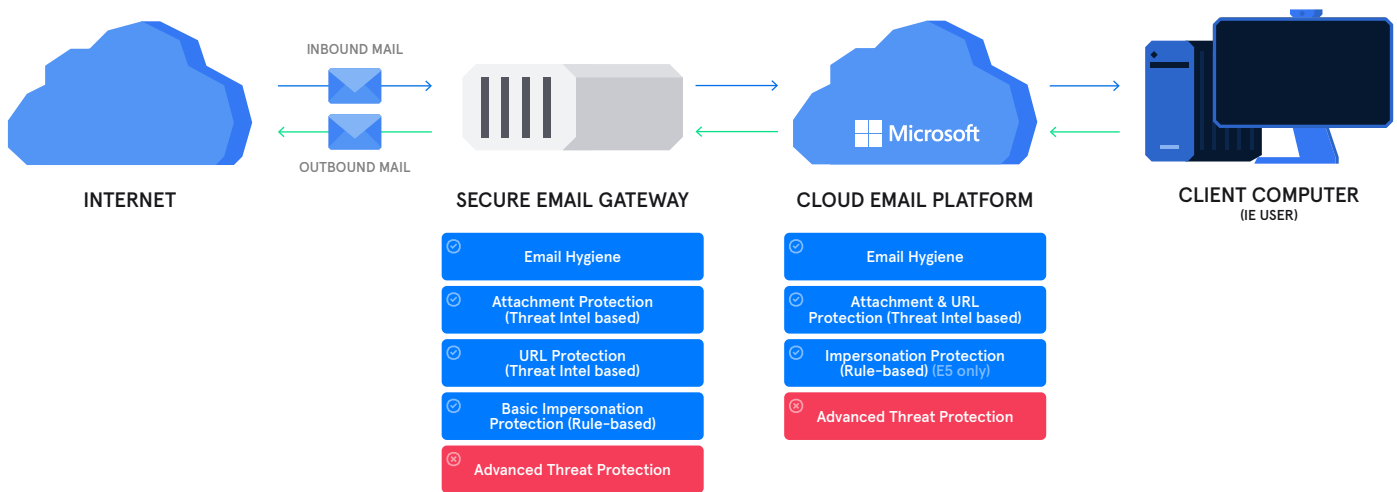


### Microsoft 365 with the E5 licensing includes the following capabilities:

- ✓ ANTI-MALWARE PROTECTION
- ✓ BASIC PHISHING PROTECTION
- ✓ ANTI-SPAM PROTECTION
- ✓ INSIDER RISK MANAGEMENT
- ✓ PROTECTION FROM MALICIOUS URLS AND FILES IN EMAIL AND OFFICE DOCUMENTS (SAFE DOCUMENTS, SAFELINKS AND SAFE ATTACHMENTS)
- ✓ MESSAGE ENCRYPTION VIA ISSUED PKI
- ✓ AUDIT LOGGING
- ✓ QUARANTINE
- ✓ EXCHANGE ARCHIVING

SEG + MICROSOFT

# Microsoft Email Security



## TESSIAN DIFFERENTIATORS

### Advanced Threat Protection

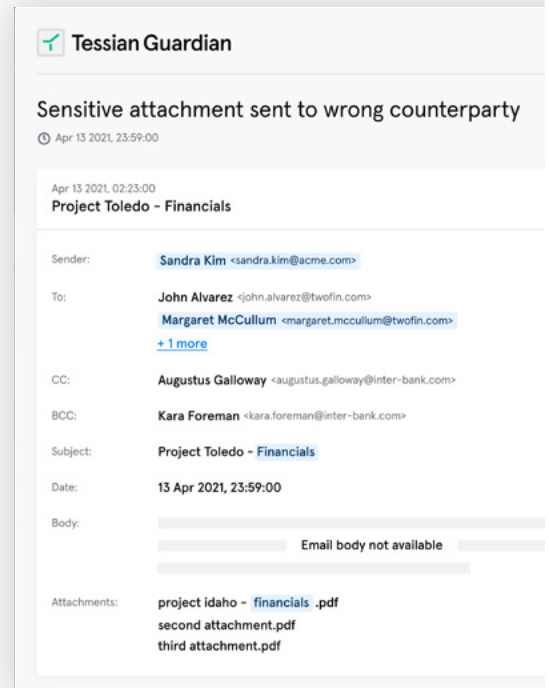
Tessian's capabilities include:

- Advanced Spear Phishing Protection
- Advanced Attachment and URL Protection
- Internal Impersonation & CEO Fraud
- Advanced Spoof Detection
- Counterparty & Vendor Impersonation
- Brand Impersonation
- Account Takeover
- Invoice Fraud
- Bulk Remediation
- Automated Quarantine
- Threat Intelligence

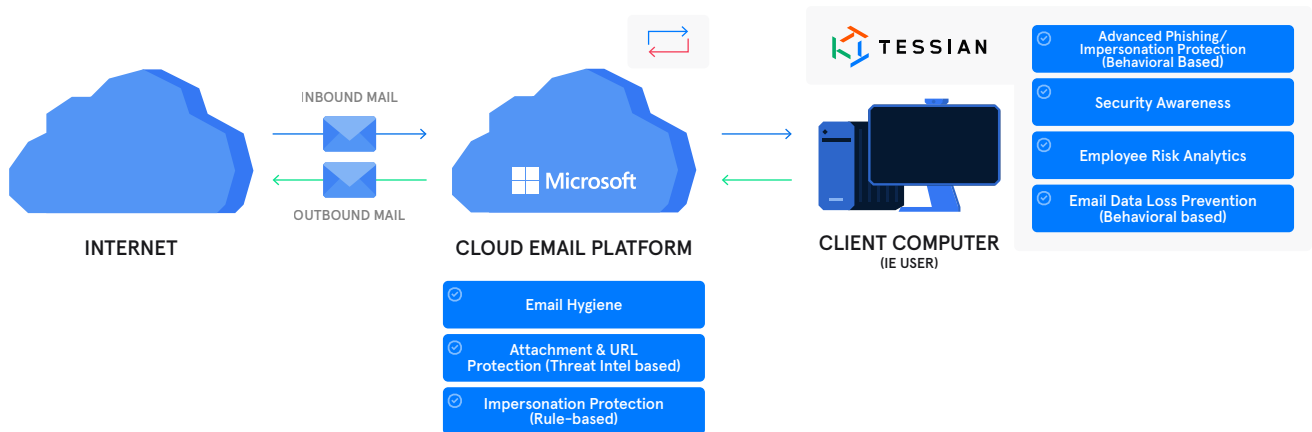
Other benefits include significant reduction of the SOC burden through automated triage and reporting. And, with Tessian's no black-box approach to threat intelligence, customers get a detailed view on why a particular email was quarantined.

In addition to the advanced inbound protective capability, Tessian offers advanced outbound protection including email data loss prevention:

- Insider threats
- Misdirected emails
- Misattached files



# Simplified Email Security Stack, Comprehensive Protection



## THE SOLUTION

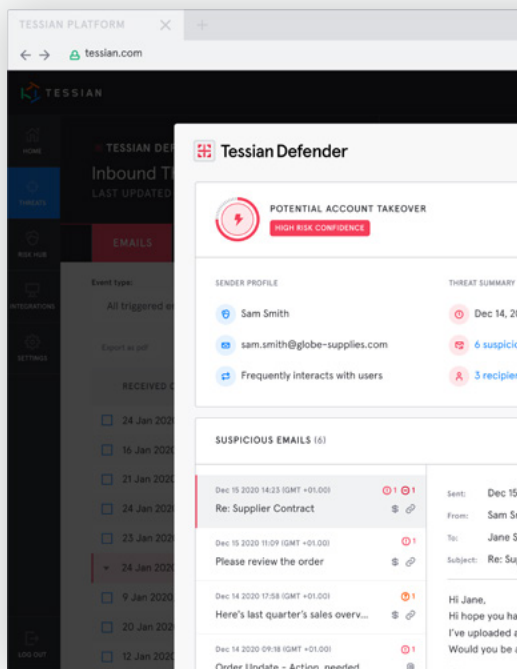
### Tessian + Microsoft

Microsoft alone does not guarantee against advanced email threats. Just like SEGs, significant gaps remain in Microsoft's ability to protect against advanced social engineering campaigns that can result in BEC, ATO, or zero day attacks.

This is where behavioral cybersecurity solutions like Tessian come into the fold, with its advanced, always-on threat detection and prevention capability. Through machine learning Tessian is able to build a contextual relationship of all end-user email behavior. From this the solution is able to understand normal email behavior by conducting a deep inspection of content using natural language process (NLP) and behavioral analysis. Tessian's algorithm is then able to detect and prevent threats that Microsoft or SEGs have failed to detect – all within 5 days of deployment.

Unlike the static nature of SEGs, Tessian is able to dynamically detect anomalous email behavior, whether it be inbound (i.e. advanced spear phishing attacks, CEO impersonation) or internal (i.e. insider threats) as it happens. With each threat detected and blocked, the algorithm and threat defenses become more resilient. We call this dynamic security.

Realize defense-in-depth and comprehensive protection by leveraging Microsoft with Tessian.

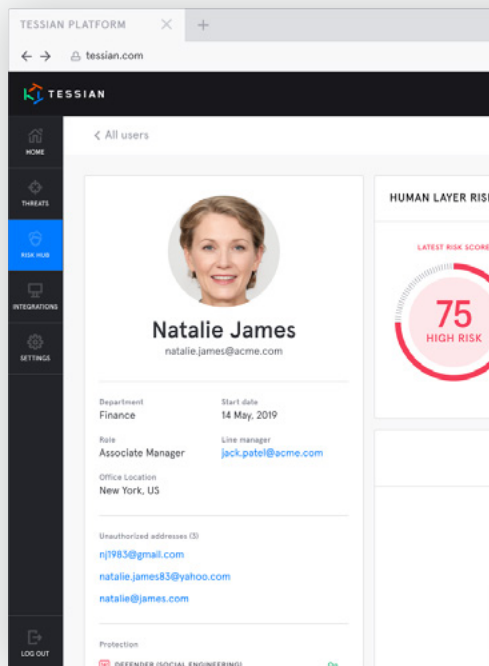


*"After so many years using Mimecast, we knew its strengths and weaknesses and we had identified a clear gap. We wanted to fill that gap in the least intrusive way possible. After evaluating various tools, Tessian was a no-brainer."*

**Associate Director of Information Security**  
Biopharmaceutical Company







## THREAT VISIBILITY AND INTELLIGENT RISK MITIGATION

### Gain visibility into your Human Layer risks

Threat visibility and intelligent risk mitigation are core features of the Tessian platform.

In order to protect against threats within organizations, Security and Risk Management leaders need visibility into key areas of risk. They need to know:

- What kinds of threats are the highest risk in your organization?
- Which departments and employees are most at-risk or likely to make a mistake?
- Where and how can you improve your security stack and improve safer email behavior?

Tessian provides unique insights with enriched risk profiles at the user, department, and company level. With increased visibility into risk areas and drivers, Security and Risk Management teams are able to prioritize mitigation actions and present results to company executives and board members, as evidence of technology reducing risk, not simply reporting it.

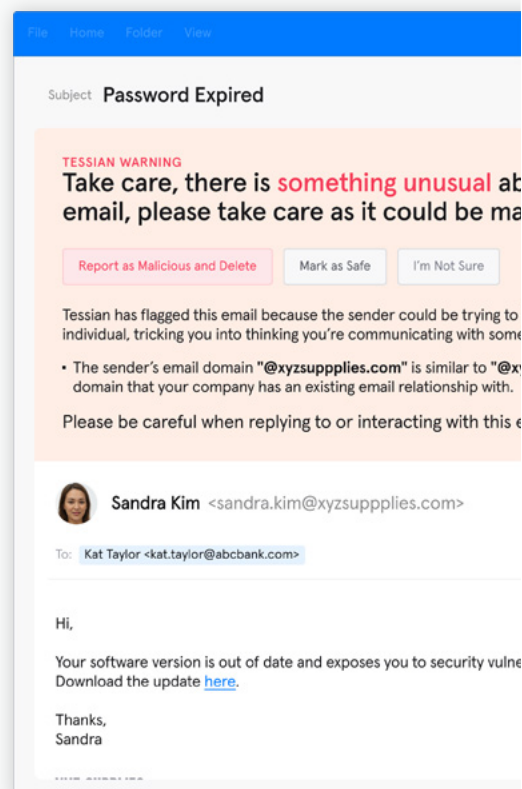
## SECURITY AND AWARENESS TRAINING

### In-the-moment contextual security awareness training


































The context-aware cybersecurity capability of Tessian extends to providing in-the-moment security awareness training to employees. When Tessian discovers malicious emails inbound or outbound, it displays contextual warning messages in a simple user friendly way with precise flag reasons to end-users educating them why the email has been identified as malicious.























The real-time security notifications help employees become better at identifying these threats over time, which improves the security posture of the company. While most organizations experience an average of **30%** click through rate on simulated phishing exercises, Tessian clients see a **less than 5% click through rate** after deployment.

And because Tessian warns users only when true events are detected, employees are protected, without disruption to their day-to-day work, enabling clients to remain agile while staying safe.

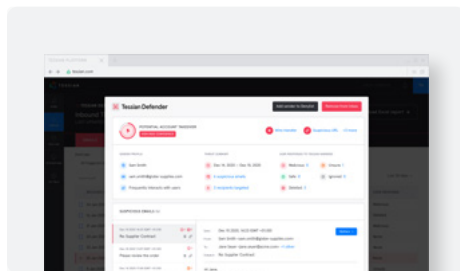


## Secure Email Gateway Replacement Matrix

|   |  |    |    |
|---|---|---|---|
| KEY   | SEG Protection  | M365 Protection   | Tessian Protection  |
| Capability                                      | SEG ONLY  | TESSIAN + M365  | TESSIAN + SEG + EXCHANGE  |
| <b>Email Filtering</b>                          |   |   |   |
| Sender Reputation & Authentication              | YES   |    |    |
| Spam  | YES   |    |    |
| Custom Routing Rules                            | YES   |    |    |
| <b>Attachment &amp; URL Protection</b>          |   |   |   |
| Malware Attachment Scanning                     | VARIES  |   | VARIES  |
| Time-of-click URL Protection                    | VARIES  |    | VARIES  |
| URL & Attachment Analysis (Threat Intelligence) | PARTIAL   |  +  |  +  |
| URL & Attachment Analysis (Behavioral)          | NO  |    |    |
| <b>Impersonation Attacks</b>                    |   |   |   |
| Internal Impersonation & CEO Fraud              | VARIES  |  +  |    |
| Counterparty & Vendor Impersonation             | LIMITED   |    |    |
| Brand impersonation                             | LIMITED   |  +  |    |
| Advanced Spoof Detection                        | VARIES  |    |    |
| Account Takeover                                | NO  |    |    |
| Invoice Fraud                                   | NO  |    |    |
| Credential Theft                                | NO  |    |    |

|   |  |     |    |
|---|---|--|---|
| KEY                                       | SEG Protection  | M365 Protection  | Tessian Protection  |
| Capability                                | SEG ONLY  | TESSIAN + M365   | TESSIAN + SEG + EXCHANGE  |
| <b>Security Awareness</b>                 |   |  |   |
| In-The-Moment Phishing Banners            | VARIES  |    |    |
| In-The-Moment DLP Warning Pop-Ups         | VARIES  |     |    |
| <b>Data Loss Protection</b>               |   |  |   |
| Misdirected Email & Attachment Prevention | NO  |     |    |
| Personal Email Detection & Prevention     | NO  |     |    |
| Custom Email DLP Policies                 | VARIES  |    |    |
| Document Classification                   | VARIES  |    | VARIES  |
| Email Encryption                          | VARIES  |   | VARIES  |
| Large File Send                           | VARIES  |   | VARIES  |
| <b>Employee Risk Analytics</b>            |   |  |   |
| Frequently Phished Users                  | VARIES  |   |  |
| Mistake Prone Users                       | NO  |   |  |
| Insider Threat Detection                  | VARIES  |  |  |

## Explore the Human Layer Security Platform

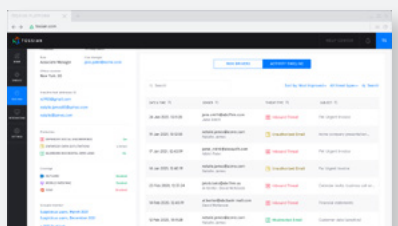


### INBOUND EMAIL SECURITY

Tessian offers comprehensive inbound email security and automatically prevents a wide range of attacks that bypass Secure Email Gateways (SEGs) including Account Takeover (ATO), Business Email Compromise (BEC), and other advanced spear phishing attacks, all while providing in-the-moment training to drive employees toward secure email behavior.

Tessian removes the burden on the SOC and admins by automating repetitive tasks such as maintaining triage and review. This eliminates the need for human verification of email threats, reducing FTE requirements.

[LEARN MORE →](#)

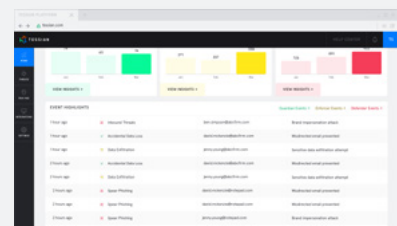


### EMAIL DATA LOSS PREVENTION (DLP)

Tessian stops accidental data loss from misdirected emails and misattached files, and ensures the right email is shared with the right person. Tessian also automatically prevents data exfiltration over email, whether it's an employee sending sensitive information to less secure, personal accounts or a bad leaver maliciously exfiltrating information for personal gains.

And, with automatic and custom policy capabilities, and real-time visibility into data loss events, security leaders can ensure compliance, without cumbersome, manual rules found in traditional DLP solutions.

[LEARN MORE →](#)



### THREAT VISIBILITY

Tessian's Human Layer Risk Hub enables security and risk management leaders to deeply understand their organization's email security posture by providing granular visibility and reporting into individual user risk levels and drivers.

With the Human Layer Risk Hub, SRM leaders will be able to quantify risk levels, pinpoint their high risk user groups, perform targeted remediation at scale, measure impact and demonstrate progress in lowering risks posed by employees.

[LEARN MORE →](#)

### FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS:



### TRUSTED BY ENTERPRISE CUSTOMERS ACROSS ALL INDUSTRIES:



## See Tessian in Action.

Automatically stop data breaches and security threats caused by employees on email.



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 March Capital, Sequoia, Accel, and Balderton.