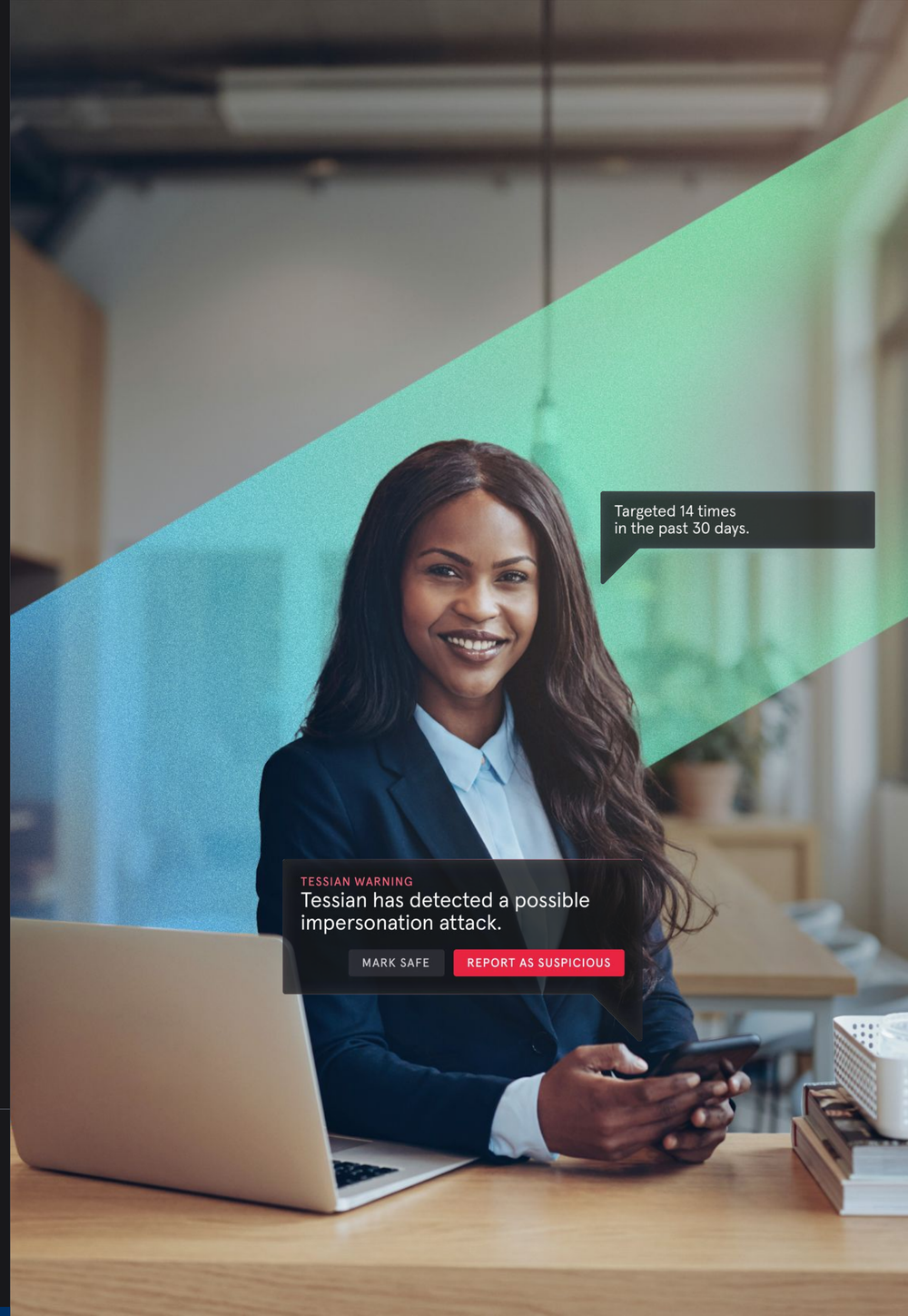
TESSIAN

To Prevent Spear Phishing, Look for Impersonation

There's never been a more urgent time to comprehensively address the spear phishing crisis. In this report, we outline impersonation as the root issue, and illustrate how machine learning is the only effective way to detect all forms of impersonation attackers are using today.



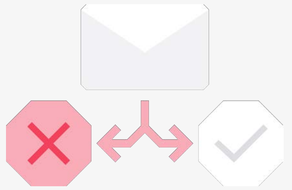
Why are spear phishing attacks still successful when enterprises supposedly have protection in place?

The three methods used by legacy Secure Email Gateway providers to combat phishing provide ‘machine layer’ protection, which is easily bypassed by sophisticated attacks.

The first two are reasonably effective at blocking malware and bulk phishing attacks, respectively. **They are not, however, effective at stopping targeted spear phishing attacks.**

Inspecting URLs & attachments for malicious payloads.

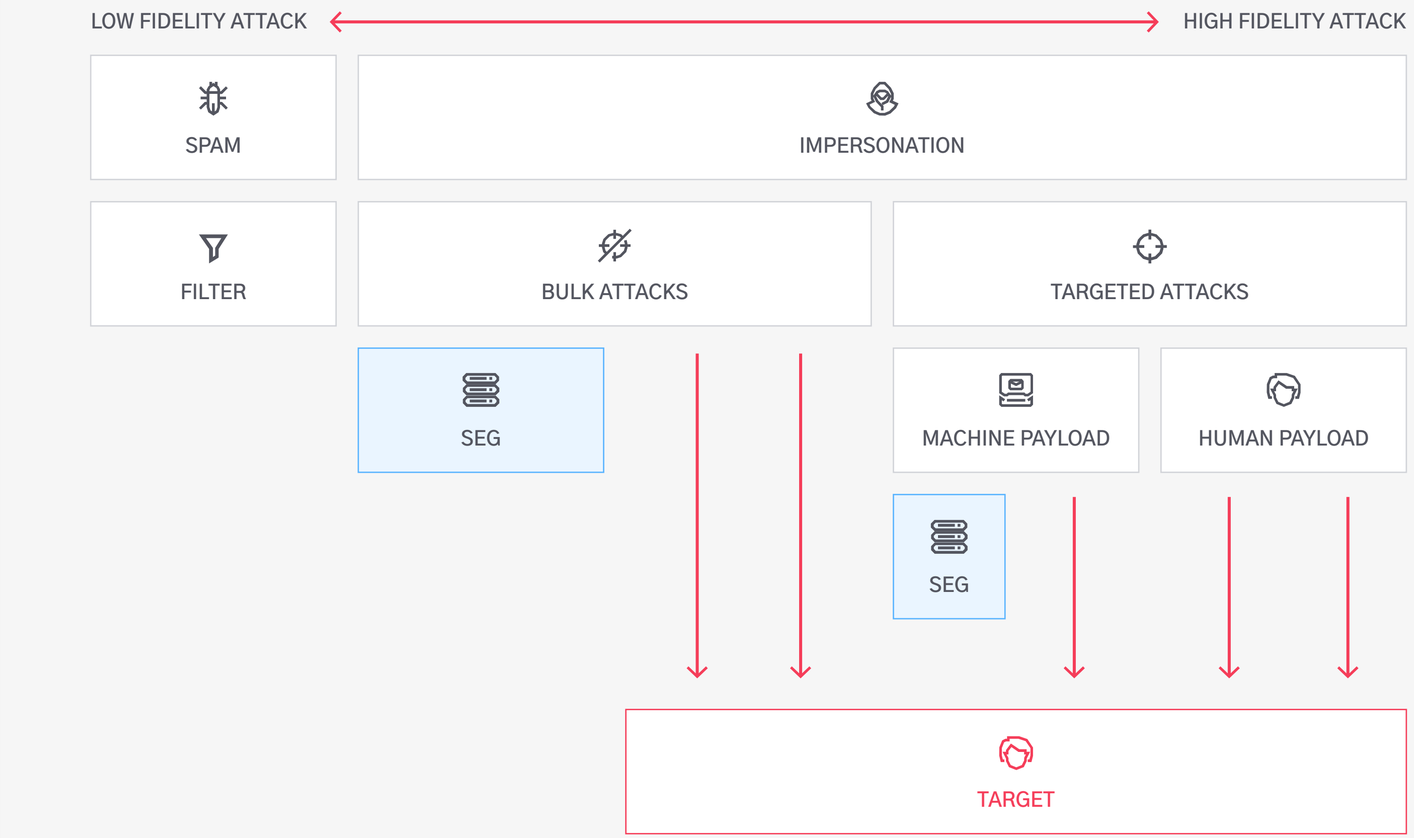
Creating blacklists of known bulk phishing attacks.



Relying on in-built rule-based impersonation detection.

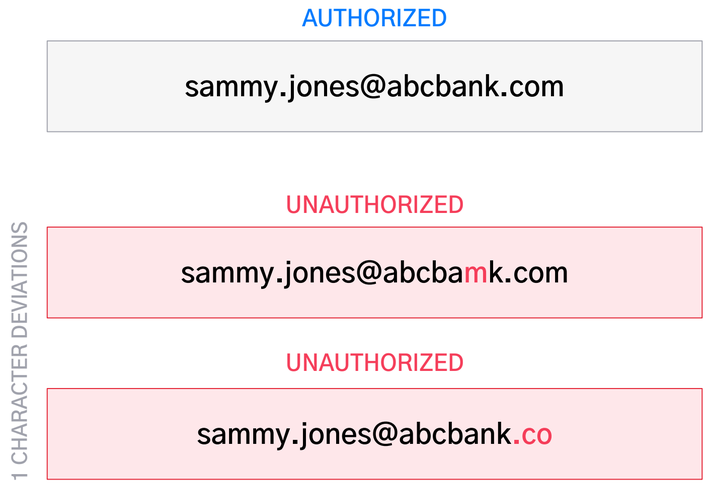
Targeted attacks are sophisticated. They don't necessarily contain a malicious payload, a term which describes typical phishing markers like malicious URLs and attachments.

Rather, targeted attacks are written in a deliberate fashion to elicit a certain action from the recipient; for example "please wire payment to this account: 123–4567". Because these attacks don't contain explicit payloads, they are not detected by Secure Email Gateways.



Understanding the spectrum of impersonation

Phishing attacks vary in sophistication and they employ different email tactics, but one thing they all have in common is impersonation. In every case, an attacker is impersonating someone who is known or trusted by their target in order to get the target to do something.



There is a broad spectrum of impersonation tactics ranging from basic to advanced. Basic impersonations involve targets being tricked into clicking on payloads (like URLs and attachments) that appear legitimate, but are in fact malicious.

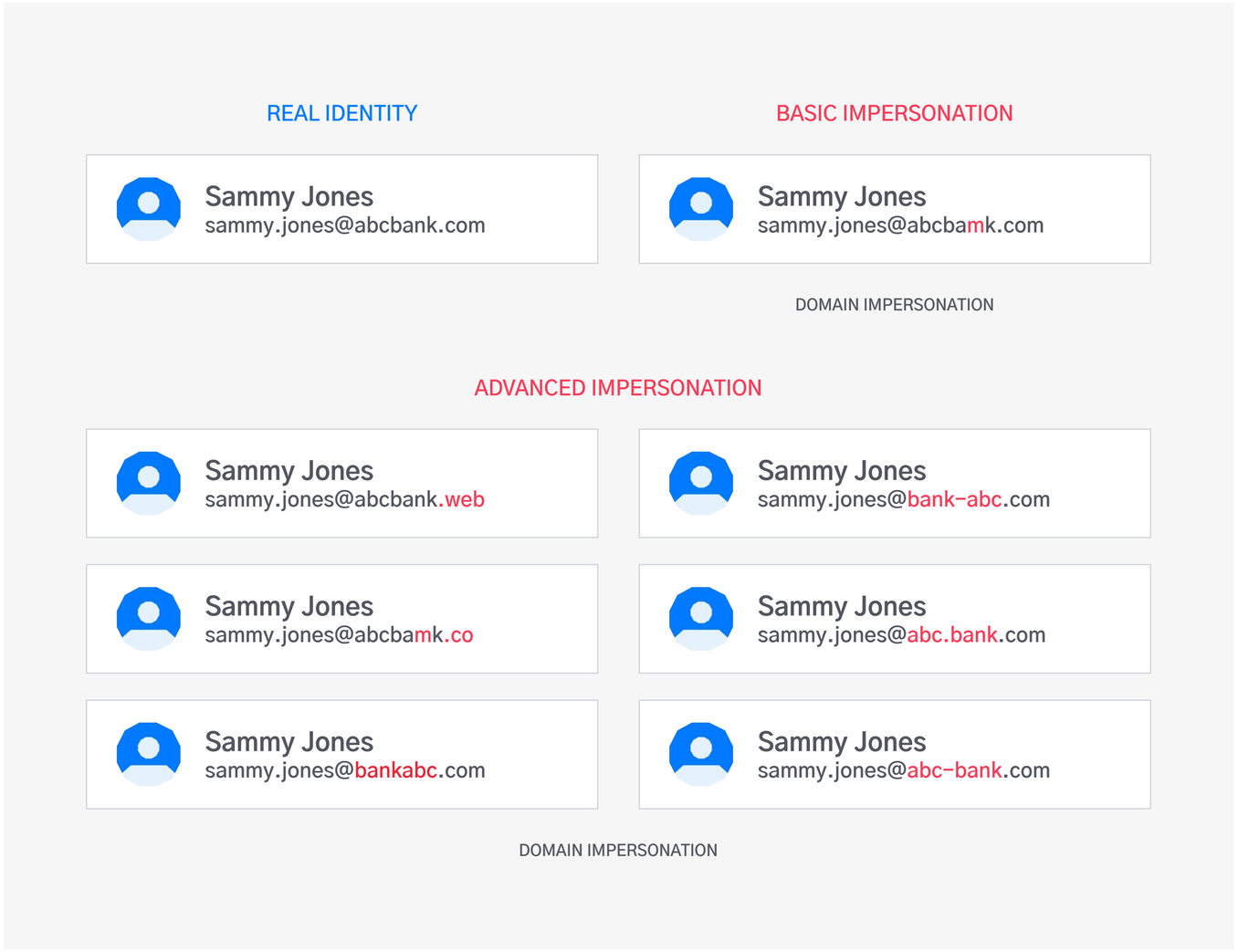
Advanced impersonation attacks deceive targets in less obvious ways, making them harder to detect. In an advanced attack, attackers typically initiate normal conversations over email and do not immediately send emails containing any requests.

Rather, they take the time to develop a legitimate dialogue with the target over multiple emails. Because trust is established between the attacker and target, any subsequent requests like wire transfers will appear genuine and likely compel the target to act.

While basic and advanced impersonation attacks aim to imitate a trusted contact through the language in the body of the email, more importantly, they do so via the sender display name and domain.

Legacy systems, like Secure Email Gateways, only prevent basic email manipulations by detecting single character deviations from the norm.

Furthermore, these basic systems only detect simple tactics used to impersonate internal contacts—for example, between employees within the same organization. Attackers have learned how to circumvent this basic protection and have evolved to use advanced impersonation tactics that are difficult to detect. Impersonation attacks prevail, but we believe if you solve impersonation detection, you solve the problem of phishing.



How do attackers bypass legacy systems?

There are thousands of ways to impersonate an internal contact that don't fall within the one-character deviation rule. All of these potential variations are dangerous. They cannot be prevented by legacy protection, and attackers are successfully leveraging them to deceive their targets.

Even worse, legacy systems can give employees and businesses a false sense of protection as they believe they are secure from inbound phishing attacks. As a result, employees may be less vigilant on email, assuming they are safe.

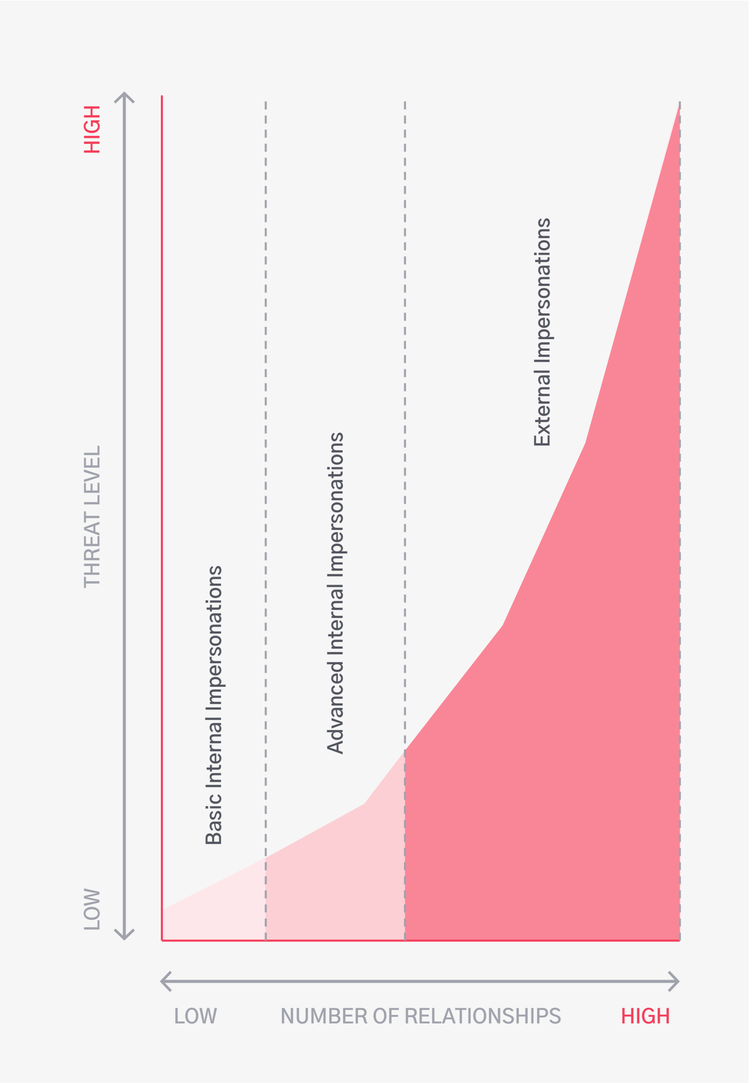
The risk of impersonation is far greater than you think

Advanced internal impersonation is only a small fraction of the risk. Most enterprises completely neglect the risk of external impersonation. Think about how many suppliers, clients and other trusted external parties your business has. Likely thousands, or even more.

Using publicly available information from things like news articles, LinkedIn and – importantly – DKIM records, attackers can choose from millions of possible domain manipulations to impersonate any one of the large numbers of suppliers, partners or clients associated with a business. They do this to target employees, exploiting existing relationships; in this case, with trusted external contacts.

With so many options across these variables when external contacts are considered, what results is combinatorial explosion.

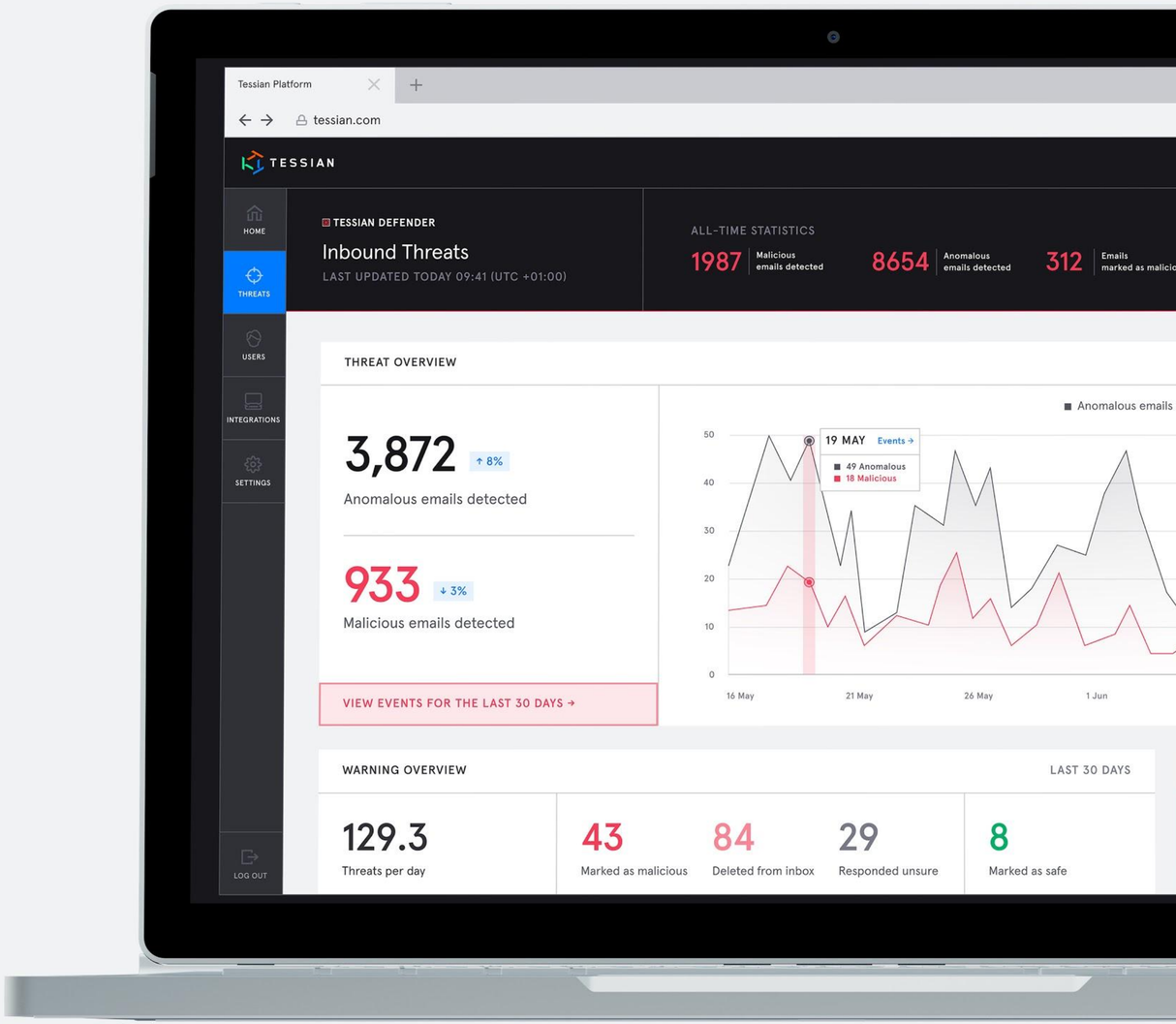
In other words, the size of the risk increases faster than exponentially. As demonstrated on the graph, legacy systems only protect against basic internal impersonation. This risk area is dwarfed by the threat of advanced external impersonation, which remains unprotected. When external impersonation is taken into account, the scale of risk becomes near limitless in size.



Machine learning provides complete protection against impersonation

Tessian Defender detects all possible impersonation types, including the manipulation of internal and external contacts. Defender stops all advanced threats that legacy systems miss.

By analyzing historic and live email metadata, machine learning algorithms intimately understand relationships with internal and external contacts across enterprise networks. By learning what normal communications look like, **our models can immediately identify anomalies, enabling highly sophisticated impersonation to be automatically detected and prevented.**



TESSIAN

Tessian protects every business's mission by securing the human layer. Using machine learning technology, Tessian automatically predicts and eliminates advanced threats on email 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.

TESSIAN.COM

大成 DENTONS · GRAPHCORE · rightmove · Investec · Schroders

arm · gubra · JTC · ITHACA ENERGY · EVERCORE

CHOATE · fieldfisher · Greenhill · HILL DICKINSON · CLYDE&CO