







How Tessian Is Preventing Breaches and Influencing Safer Behavior in Healthcare

ABOUT CORDAAN

Cordaan – one of the largest healthcare providers in Amsterdam – provides care to over 20,000 people from 120 locations across Amsterdam. They do this with the help of 6,000 employees and more than 2,500 volunteers. Cordaan also works in association with research institutes and social organizations.

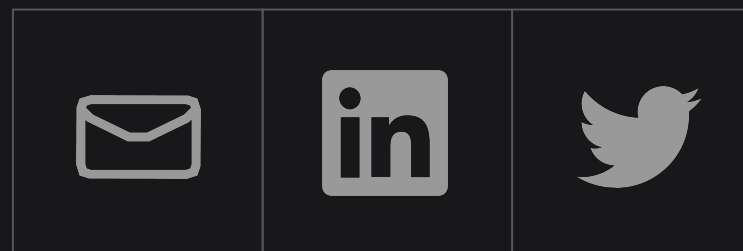
KEY FACTS

-  6,300 User Deployment
-  Tessian Defender Deployed
-  Tessian Guardian Deployed
-  Tessian Enforcer Deployed



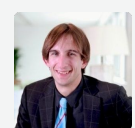
 [TESSIAN.COM/CUSTOMERS](https://tessian.com/customers) →

Share this story



Healthcare employees are especially vulnerable to inbound attacks

“The difficulty in healthcare is that we train our employees to be helpful. We train them to answer people’s’ questions. But that isn’t always the most secure thing to do, especially when you’re being targeted by hackers. So, how do you do both? How do you serve your clients and patients while also ensuring cybersecurity?”




CAS DE BIE,
Chief Information Officer, Cordaan

When it comes to inbound attacks like [spear phishing](#) and [business email compromise](#), the healthcare industry is [among the most targeted](#). It also has the highest costs associated with data breaches.

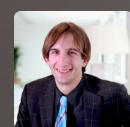
Why? According to [Cas de Bie](#), the Dutch healthcare provider’s Chief Information Officer, it’s not just because organizations operating in this industry handle highly sensitive data. It also has a lot to do with the very *nature* of the work: helping people.

Combine this empathetic approach with the stress of a global pandemic, and you’re left with an incredibly vulnerable workforce. With Tessian, Cas is now confident his email security will identify spear phishing emails before his employees respond to them and that employees’ workflow won’t be disrupted in the process.

When talking about inbound attacks, Cas said “It’s all about awareness. While people probably do know what they’re supposed to do when it comes to email security, it’s different in real life. It’s hard to decide in the moment. Of course, they don’t do it on purpose. They want to make the right decision. Tessian helps them do that.”



What we did until we did business with Tessian was all the “standard stuff”—standard email security, standard spam filtering. And while we have a good incident management process, it was all quite reactive. These measures weren’t effective enough on their own. They didn’t operate in real-time. We needed to do more proactively.



CAS DE BIE,
Chief Information Officer, Cordaan

THE PROBLEM

Reactive and rule-based solutions weren’t preventing human error on email in the short *or* long-term

To ensure [GDPR-compliance](#), Cordaan prioritized investment in privacy and security solutions. But, according to Cas, “standard” email security, spam filtering solutions, and encryption alone just weren’t enough. They weren’t keeping malicious emails out of inboxes, and they weren’t preventing data loss from insiders. They also weren’t doing anything to improve employee security reflexes in the long-term.



How Tessian Is Preventing Breaches and Influencing Safer Behavior in Healthcare



[TESSIAN.COM/CUSTOMERS](https://tessian.com/customers) →

So, to level-up Cordaan's email security, Cas was looking for a solution that was:

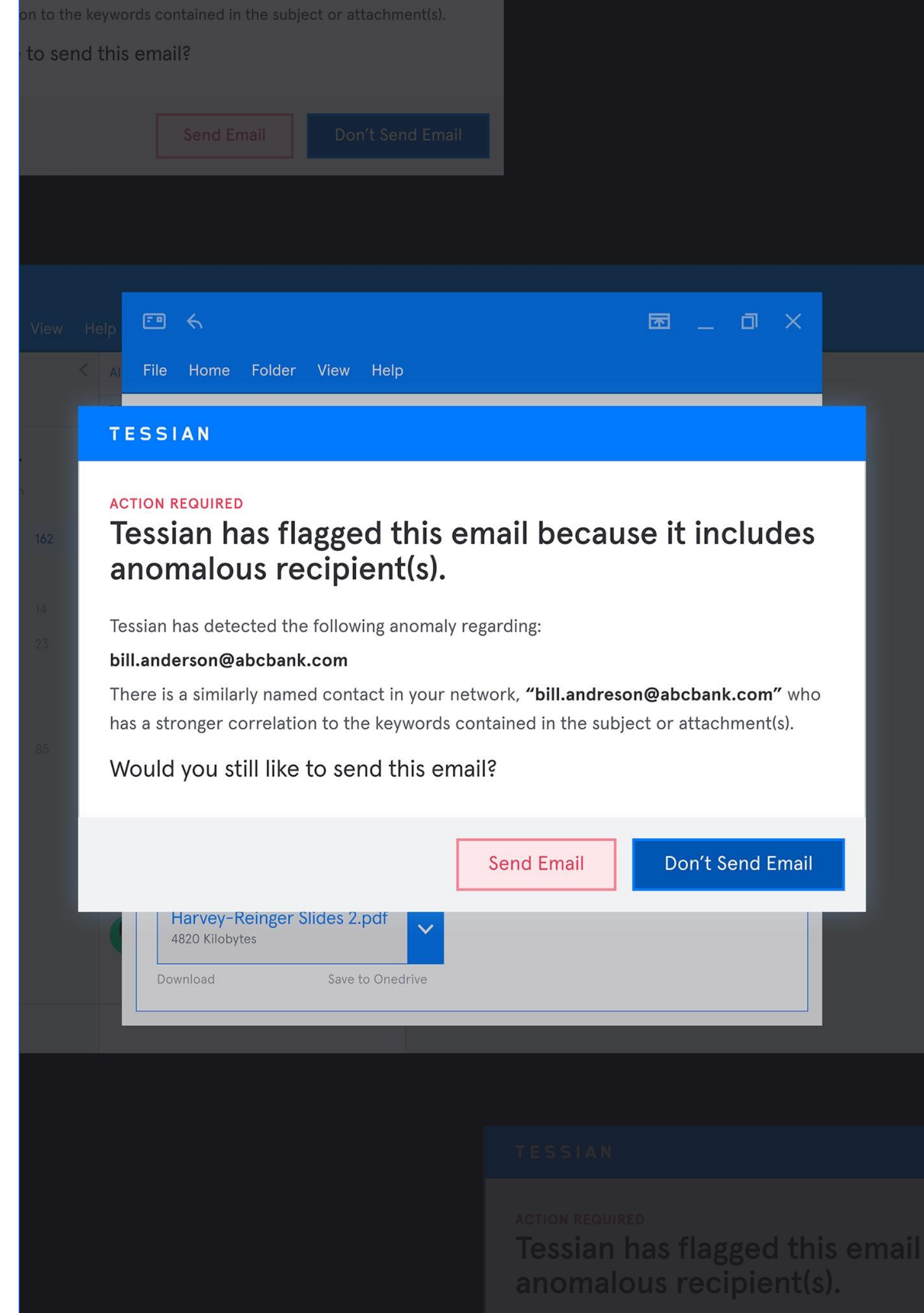
- ✓ Technologically advanced
- ✓ User-friendly
- ✓ Proactive

With Tessian, he found all three.

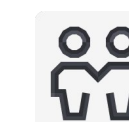
Powered by [contextual machine learning and artificial intelligence](#), our solutions can detect and prevent threats and risky behavior before they become incidents or breaches. How? With the in-the-moment warnings – triggered by anomalous email activity – that look something like this.

These warnings help nudge well-intentioned employees towards safer behavior and ensure data stays within Cordaan's perimeter. And, because Tessian works silently in the background and analyzes inbound and outbound emails in milliseconds, it's invisible to employees until they see a warning.

This was incredibly important to Cas, who said that **“The added value of Tessian is that it influences behavior. That really resonated with the board and helped me make a strong business case.** While I can't show how cybersecurity creates revenue, I can show – via a risk management calculation – **the potential fines we could avoid because of our investment in Tessian”.**



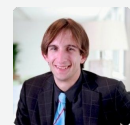
How Tessian Is Preventing Breaches and Influencing Safer Behavior in Healthcare



[TESSIAN.COM/CUSTOMERS](https://tessian.com/customers) →

Cordaan's security team had limited visibility into – and control over – data loss incidents on email

“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,
Chief Information Officer, Cordaan

While Cordaan had invested in other email security solutions, Cas and his team still lacked visibility into the frequency of data loss incidents on email. But, **after deploying Tessian for a Proof of Value, the scope of the problem became crystal clear.**

The reality is that employees do actually send unauthorized and misdirected emails more frequently than expected. (We explore this in detail in our report, [The State of Data Loss Prevention 2020](#).)


But, the *good news* is that this behavior can be influenced and corrected—all without access restrictions that make it harder (or impossible) for employees to do their jobs.


Cas explained it well, saying that “Of course there are things that we have to police and prohibit. But, most of the time, people aren't doing things maliciously. So it's nice that – with Tessian – we can take a more nuanced approach. We can influence behavior and help our employees do the right thing.”




Learn more about how Tessian prevents human error on email.

Powered by machine learning, [Tessian's Human Layer Security technology](#) understands human behavior and relationships.

 **GUARDIAN**
Automatically detects and prevents misdirected emails

 **ENFORCER**
Automatically detects and prevents data exfiltration attempts

 **DEFENDER**
Automatically detects and prevents spear phishing attacks

Importantly, [Tessian's technology](#) automatically updates its understanding of human behavior and evolving relationships through continuous analysis and learning of an organization's email network. That means it gets smarter over time to keep you protected, wherever and however your work.

Interested in learning more about how Tessian can help prevent email mistakes in your organization?

[CUSTOMER STORIES →](#) [BOOK A DEMO →](#)



 [TESSIAN.COM/CUSTOMERS →](https://tessian.com/customers)

Share this story

