TESSIAN

CAESARS ENTERTAINMENT®

Why Caesars Entertainment Chose Tessian as Their Complete Outbound Email Security Solution

ABOUT CAESARS ENTERTAINMENT UK

In 2006, Caesars Entertainment — the world's largest casino entertainment company, best known for properties such as Caesars Palace, Planet Hollywood, and Harrahs — acquired London Clubs International. The current seven casinos in the UK form Caesars Entertainment UK.

KEY FACTS

- **250** User Deployment
- **Tessian Guardian** Deployed
- **Tessian Enforcer** Deployed

While the organization is passionate about delivering exceptional gaming entertainment and proud to offer customers unrivaled networks and benefits, they're also active in the community, sponsoring and supporting a number of charities, including YGAM, GamCare, and The Gordon Moody Association.

To help prevent both **accidental data loss and malicious data exfiltration**, Caesars has deployed Tessian Guardian and Enforcer as a **complete outbound email security solution** to protect 250 employees.

Tessian solves three key problems for Caesars.

PROBLEM

An honest mistake on email almost caused a data breach

> "Before this incident, we viewed misdirected emails as a minor incident. And when it came to budget, we wanted to focus on the major things. But this incident with the spreadsheet woke everybody up. It was no longer a case of "How much?" but instead "Which one?" and we decided on Tessian pretty quickly."

CHARLES RAYER
Group IT Director at Caesars Entertainment UK

Oftentimes, cybersecurity solutions are purchased retroactively, meaning **after** a breach has occurred. But, for Charles Rayer, Group IT Director at Caesars Entertainment UK, Tessian was a *proactive* investment, elicited by a near-miss.

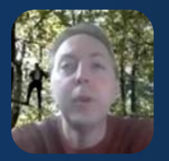
Here's what happened: A customer relations advisor was sending emails to the casino's VIPs. But, in one email, **the employee accidentally attached the wrong document, which was a spreadsheet** containing personal information related to some of their top 100 customers.

Luckily, they *also* spelled the email address incorrectly, so it was never actually sent. Nonetheless, it was a wake-up call for Charles and his team.

So, what would the consequences have been if the email *had* actually gone through?

Charles explained, saying, "We're covered by the GDPR and the Sarbanes-Oxley Act because we're a public listing with US parent companies which means, had the email been sent, we would have had to report it which is a long process. And, even though we had security solutions in place, we would have most likely received a fine."

"It's an issue of human error. **We truly believe people are 100x more likely to accidentally mishandle data than to do it deliberately. So how do you solve it?** There are thousands of solutions that categorize emails, look for strings of numbers, and identify keywords based on rules. But they don't help in this situation. **Tessian does.** It knows – and continues learning – what conversations you normally have with people and can pick-up when something's off. That's the feature that really stood out to us."



CHARLES RAYER
Group IT Director at Caesars Entertainment UK

"But for us, the biggest issue would have been the reputational damage. If that personal information did fall into the wrong hands, what would they do with it? Would they use it for their own personal benefit? Would they use it against us?"

With Tessian Human Layer Security Intelligence, Charles now has clear visibility of misdirected emails – what he previously considered an "iceberg threat" – and, because Tessian Guardian automatically prevents emails from being sent to the wrong person, Charles feels confident that a simple mistake won't cost Caesars its reputation.

To learn more about how Tessian Guardian uses historical email analysis, real-time analysis, natural language processing, and employee relationship graphs to detect and prevent misdirected emails, download the data sheet.

PROBLEM

Other solutions triggered 10x as many false positives as real events

While – prior to deploying Tessian – Charles didn't have any technology in place to prevent misdirected emails, he *did* have a solution in place to prevent unauthorized emails.

But, because it triggered so many false positives, he and his security team were drowning in alerts, making it impossible to investigate even a fraction of the alleged incidents in real time.

It was also disruptive for employees to interact with day-to-day.

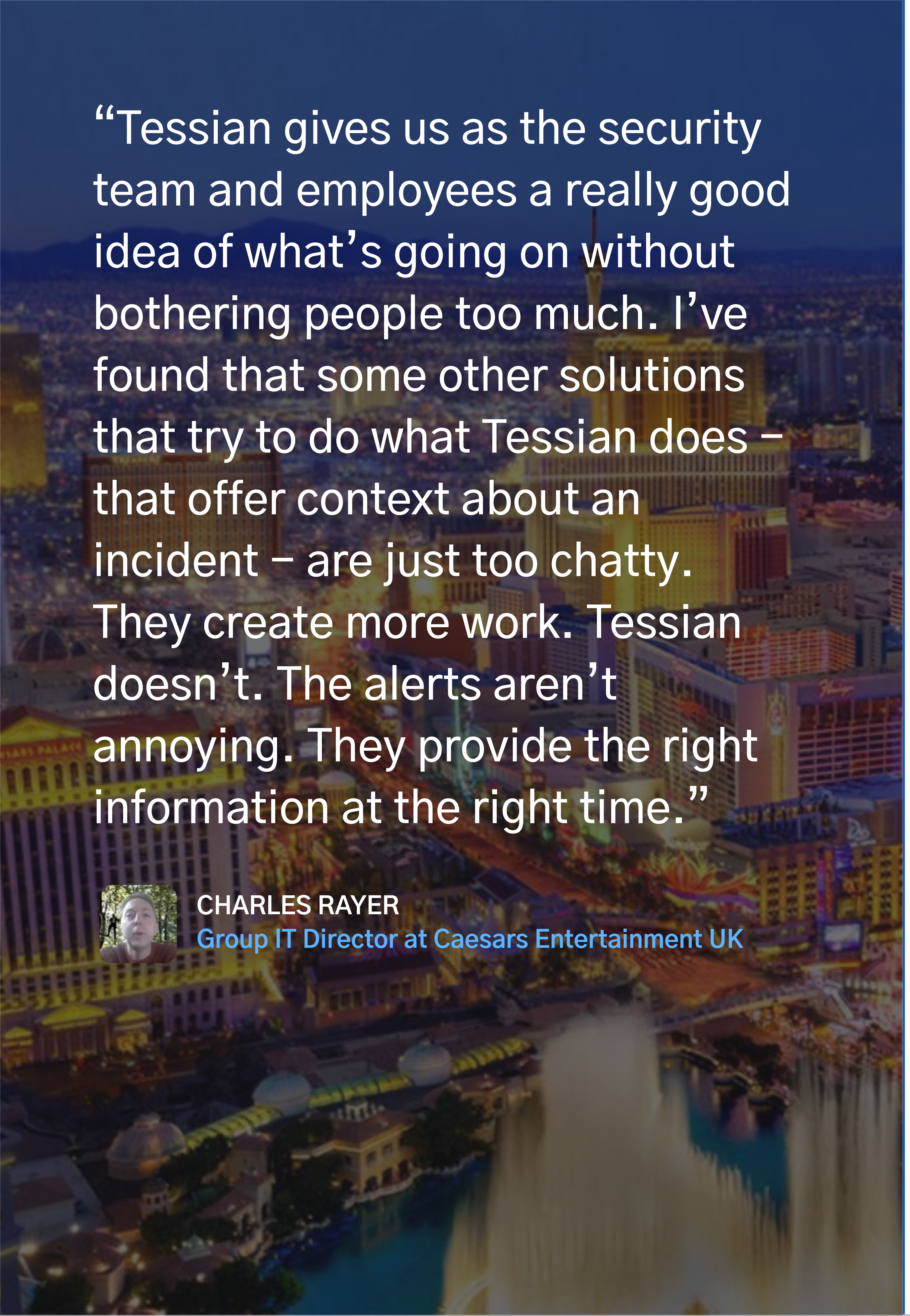
"I would say on average, **we saw 10x as many false positives as real incidents of data exfiltration. Some days you'd have 100 incidents logged**, and not one of them would be of merit. It was a deluge of junk, with the occasional useful bit of information," he explained.

Charlies pointed out that **Tessian, on the other hand, flags just 5-6 unauthorized emails a day company-wide with a false positive rate that's marginal** now, and will only get smaller as it continues to learn from employee behavior and relationships. Yes, that means it gets smarter over time.

How? Enforcer analyzes historical email data to understand what "normal" content, context, and communication patterns look like. The technology uses this understanding alongside real-time analysis to accurately predict whether or not outbound emails are data exfiltration attempts.

That means Charles and his team can actually investigate each and every incident and, when employees do see a warning, they interact with it instead of ignoring it.

Want to learn more about how Tessian Enforcer's machine learning algorithms get smarter over time? You can get more information here.



> “Tessian gives us as the security team and employees a really good idea of what’s going on without bothering people too much. I’ve found that some other solutions that try to do what Tessian does – that offer context about an incident – are just too chatty. They create more work. Tessian doesn’t. The alerts aren’t annoying. They provide the right information at the right time.”

CHARLES RAYER
Group IT Director at Caesars Entertainment UK

PROBLEM

Employees in the entertainment industry handle highly sensitive data – but not *all* of them

As Charles pointed out, employees working in the entertainment industry – especially those who work in customer service – handle a *lot* of sensitive information. That means that mistakes – like sending a misdirected email or emailing a contract to a personal email address to print at home – can have big consequences. It also means employees may be motivated to exfiltrate data for a competitive advantage or financial gain.

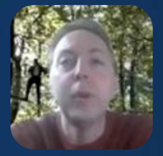
Charles has seen all of the above.

“Not just our sector, but *all* sectors in the entertainment industry are based around customer service and personal contact. That means we have to know a lot about our customers. And that information is valuable. It’s information people want which means we have to make sure we protect it,” he explained.

But, not all employees have access to the same type of information. Customization, therefore, was important to Charles, who said, “We have a number of employees who don’t actually have access to sensitive information and a number of employees who don’t email anyone external. So there’s no point deploying across the entire company. We wanted to focus on people who deal with customers.

While Tessian *does* offer 100% automated threat prevention, we know that for security strategies to be truly effective, technology and in-house policies have to work together. With Tessian Constructor, security leaders can create personalized rules and policies for individuals and groups.

> “We have a number of employees who don’t actually have access to sensitive information and a number of employees who don’t email anyone external. So there’s no point deploying across the entire company. We wanted to focus on people who deal with customers. Likewise, not everyone who has been onboarded is in the same internal email group, which means we have to apply different controls and rules to different people. We can do all of this easily with Tessian.”



CHARLES RAYER
Group IT Director at Caesars Entertainment UK

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?

REQUEST A DEMO →

CUSTOMER STORIES →

TESSIAN

TESSIAN.COM/CUSTOMERS →