

Real Estate Leader Jellis Craig Safeguards Clients and Its Brand With Proofpoint

JellisCraig

The Challenge

- Protect client and company email communications from phishing and other cyber threats
- Protect brand from spoofing and abuse by bad actors
- Strengthen a company culture of security

The Solution

- Proofpoint Enterprise Protection
- Proofpoint Email Fraud Defense
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull
- Proofpoint Security Awareness Training

The Results

- Improved visibility provides insights into security posture
- Email security protects firm from malicious attacks
- Enhanced DMARC authentication protects brand

The Company

Jellis Craig is one of the premium property real estate firms in Australia. The organisation spans residential sales, property management and marketing. With 28 offices across the country and a staff of 800, the company runs its business based on ethics, integrity and personal service. But with such a wide range of locations and services, its cybersecurity is of the utmost importance.

The Challenge

Protecting customers in high-value transactions

Established in 1991, Jellis Craig has continually evolved and grown to become one of Melbourne's leading real estate groups. Its network of strategically located offices are positioned across Melbourne's most sought-after suburbs and reach into local, interstate and international markets.

Like most businesses, Jellis Craig places a high priority on security, so when its existing solutions began to fall behind emerging threats, its IT team knew it would have to move fast to put stronger protection in place.

"The security platform we were using for email was not functioning that well, and a lot of phishing email attempts were making their way through," said Christian Marotta, group IT manager at Jellis Craig. "At the same time, the real estate industry was increasingly becoming a high target for ransomware threats and business email compromise threats. Since we are quite a well-known brand, I could see us being targeted more and more."

Jellis Craig has earned a reputation as a highly customer-centric organisation, and robust security was especially critical to protecting its clients from fraud.

“We had two key priorities: to protect our brand, and our clients,” said Marotta. “If a client puts down a large deposit on an expensive home, and a bad actor pretending to be us reaches out to them and provides fraudulent banking details, the results could be disastrous.”

The Solution

Proactive brand protection and safer email

After considering a variety of options, Jellis Craig chose to migrate its email security to Proofpoint Enterprise Protection, which scans inbound and outbound email messages for malware, phishing and spam threats. If a questionable email does slip through, Proofpoint Threat Response Auto-Pull (TRAP) lets the security team analyse it and move malicious communication into quarantine after it's delivered.

“Getting our email domains to ‘reject’ policy was something that I’ve wanted to do for years, and having a solution in Proofpoint Email Fraud Defense that enabled us to do that in a relatively quick time was great. I was really happy with the process.”

Christian Marotta, group IT manager, Jellis Craig

“We did some research and found that Proofpoint offered some important advantages for us,” said Marotta. “They were very strong in blocking phishing emails, and if something were to get through, they could put a system in place that would let us call those emails back quite easily.”

A proof-of-concept exercise at the beginning of the migration process confirmed the need for stronger protection for the company’s brand. The audit uncovered multiple incidents where the Jellis Craig domain name had been spoofed, targeting employees and consumers. The process also highlighted more than 40 different shadow-IT systems sending emails on the company’s behalf.

The firm deployed Proofpoint Email Fraud Defense to improve visibility and gain access to the tools and services needed to authorise legitimate email. The firm was also seeking to enforce a DMARC “reject” policy on its trusted domains—the strongest level of protection available for protection from email spoofing attacks.

“The main aim for deploying Proofpoint Email Fraud Defense was to get our main sending domain to a DMARC ‘reject’ point,” said Marotta. “We wanted to ensure that bad actors couldn’t spoof our domain and trick our clients into paying money into the wrong account. We really wanted to make sure our clients were protected—and protect our brand from any misuse of our domain name.”

Proofpoint Professional Services provided assistance with deployment, and the migration process moved forward quickly and easily.

“The guidance provided by Proofpoint Professional Services was great,” said Marotta. “We managed to turn around quite quickly and discovered several shadow IT centres that we were able to shut down pretty quickly.”

The Results

Stopping phishing and email fraud in its tracks

After onboarding its Proofpoint solution, Jellis Craig has quickly strengthened its DMARC protection and stopped BEC incidents targeting employees and consumers—without blocking any of its legitimate email.

“Using the Proofpoint Email Fraud Defense module and the dashboard was so clear and enabled us to actually get to ‘reject’ within six months,” said Marotta. “It was quite a quick process.”

Phishing and other threats have been dramatically reduced as well, and Jellis Craig has gained improved insight into its security challenges to stay ahead of changing threats.

“Proofpoint has enabled us to block well over 90% of our phishing emails,” said Marotta. “Looking at the last three days alone, I’m seeing 80 to 100 threats blocked. I actually sleep quite well and I’m quite happy with how Proofpoint is performing. With our previous systems, we didn’t have clear visibility into what was going on, but now I can easily see suspicious logins, along with our ‘very attacked people’ and what type of email threats they’re getting. I can better understand the threat landscape and know what we need to make sure we’re on top of the most common threats and protecting ourselves from them.”

To build on its momentum, Jellis Craig is enrolling its staff in Proofpoint Security Awareness Training, to help ensure the strongest response from users when they encounter cybersecurity threats. As a result, Jellis Craig users reported more than 400 emails over several months, and over 50% of them were confirmed malicious, suspicious or spam email.

“We’re feeling really happy that we’re protecting ourselves and our clients,” said Marotta. “We’ve just signed up for Proofpoint Security Awareness Training. We knew we needed to educate our users, and we needed a system that could do that, measure it, report to us individuals who regularly click on suspicious messages, and make sure that we can give them appropriate training to protect them. And now we have that.”

LEARN MORE

For more information, visit [proofpoint.com](https://www.proofpoint.com).

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity company that protects organisations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.