bugcrowd

PLATFORM-POWERED BUG BOUNTY HELPS TRANSFERWISE INNOVATE PAYMENT SECURITY

Hackers from around the world are trusted to protect payments made through TransferWise. TransferWise, a global technology company building the best ways to move money worldwide, has adapted its security processes from a once traditional compliance-oriented penetration test to an innovative crowdsourced model. As **SecPoint reports**, some of the major limitations that penetration tests have are the restricted access and line of sight to the application testing environment, making this testing method fallible.

TransferWise's use of traditional penetration testing solutions were not providing sufficient depth and breadth for their testing use cases. As Chief Information Security Officer Shan Lee explained, "We wanted to do something more focused around genuine security than just about checking a box for some audit. We needed a process that offers a more real-world approach."

As a result, TransferWise's journey to crowdsourced security began. Lee understood the power and value of the crowdsource model, stating, "I've always been a long-time fan of the crowdsource security model. I've had experience using this methodology in past roles and have seen the value and the operational impact it can have on a security organization."

Having analyzed various crowdsource security vendors, TransferWise turned to Bugcrowd to help launch its first bug bounty program. Bugcrowd's program provided them with continual testing, greatly reducing risk and better mitigating threats. With its bug bounty program, TransferWise gained more insight into potential threats and vulnerabilities across its applications.

TransferWise

Industry: Technology
Bugcrowd Product: Bug Bounty

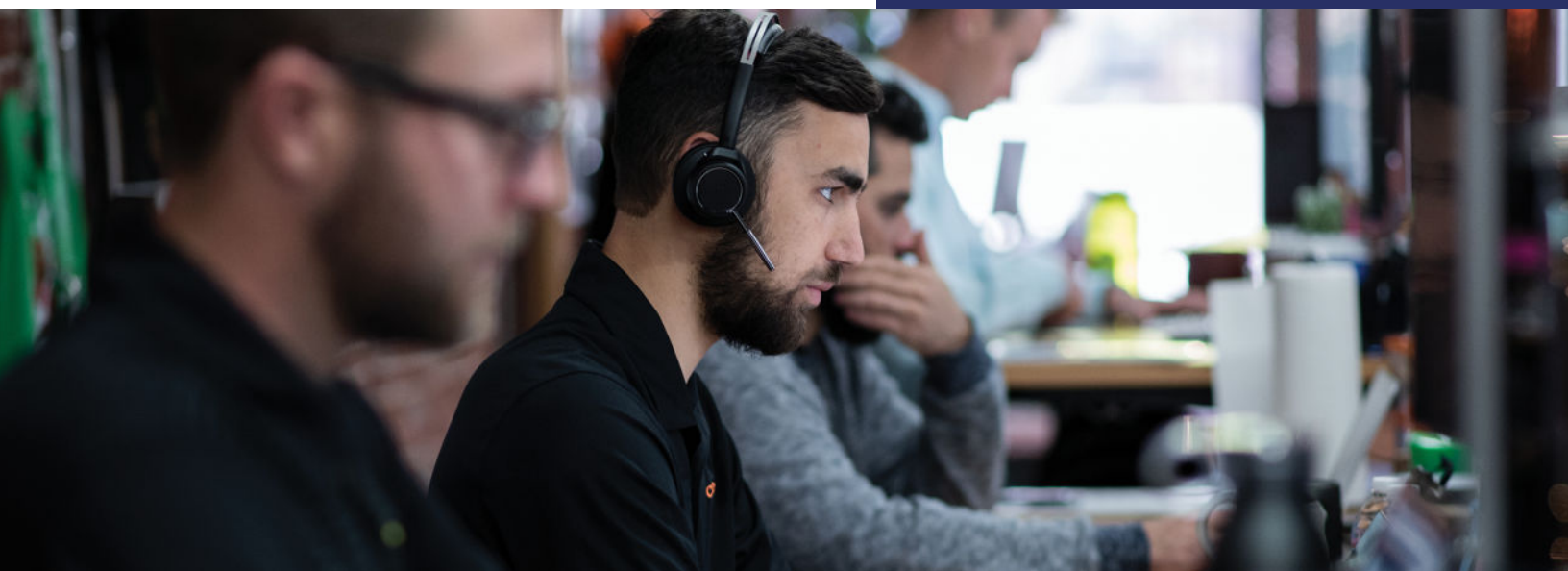
SUMMARY

Challenge —
Traditional compliance-oriented testing solutions were not providing sufficient depth and breadth in testing scenarios.

Solution —
Bugcrowd Bug Bounty

Outcomes —

- Improved Risk Reduction
- Expedited Threat Mitigation
- More Secure Applications



TransferWise started with Bugcrowd's private bug bounty program, which introduced bug hunting to the company with a scope that would expand alongside their increasing operational bandwidth. The private program helped to streamline the vulnerability management lifecycle and its associated remediation workflows before going public, ensuring scalability of these newly found security efficiencies. And within just 24 hours of launching the private program, TransferWise received its first valid 'P1 Business Critical' vulnerability (**learn more about this rating**). These rapid results highlight the risk reduction provided by the program, helping to keep threats like fraud, and e-skimming at bay. Discovering a considerable threat so quickly proved the concept that crowdsourced security works. As CISO Lee explained, "the finding we received would not have been discovered in a traditional penetration test, so by having a more expansive scope and the support from the **crowd**, we were able to focus on areas we didn't realize needed the attention".

Over time, TransferWise scaled its vulnerability management processes allowing them to broaden the scope of its private program. As the scope continued to expand, the program was at a point where it made sense to convert to a public program. With a public program, TransferWise opened the scope in a way that anyone from the crowd could be activated. This allowed the security team to accept bug bounty submissions at a higher volume and velocity and has helped to standardize submissions for repeatability while accelerating the vulnerability management lifecycle. As Security Engineer Ando Roots described, "over time we were able to effectively address and manage the number of submissions we were receiving and now have developed a workflow that is scalable and efficient. It exemplifies our security maturity as a team and an organization."

Adopting crowdsourced security has transformed vulnerability management at TransferWise and helped to create a security-focused culture. With Bugcrowd, TransferWise can test and defend real-world scenarios using a crowd of ethical hackers to safeguard their customer experience.

If you are interested in learning more about TransferWise or would like to join their security team, check them out **here**.

More about the Interviewees/Authors:

Shan Lee leads the Information Security and Privacy teams at TransferWise. As an established information security leader, he is passionate about promoting a "Security Culture" in what is a fast-moving and rapidly expanding environment. Check out his LinkedIn **here**.

Ando Roots is a security engineer at TransferWise. As a developer and a trainer, he works with engineers and the crowd on keeping TransferWise's systems secure.

> "The number of Bugcrowd findings is a true measure of our maturity as a company. I want to get to a point in the not too distant future where I am showing a graph at every board meeting that shows a meager number of Bugcrowd findings and not for lack of attention but due to our focus on enhancing our application security."
>
> **Lee, CISO, TransferWise**