CASE STUDY

SaaS Startup

Small SaaS Startup hit with **$2M ransomware** before they even onboard their first client.

INTRODUCTION

Ransomware is growing exponentially, and small companies are no longer immune. Trustvio (real name kept private for security reasons) is an innovative startup that was trying to get their start with their first customers when they were attacked with a $2 million ransomware.

CHALLENGE

SaaS companies will always be a large target for hackers, because of the numerous attack vectors. But Trustvio certainly didn't expect to be a target before they onboarded their first customer. Not only did they suffer a ransomware attack that they couldn't possibly afford as a startup, but their first prospects now worried about the integrity of the company. After reporting the attack to the FBI and putting numerous security measures in place, Trustvio searched for a penetration testing company that could produce fast results to give their prospects assurance that they had remediated any weaknesses in their environment.

SOLUTION

Trustvio searched for a fast and affordable partner they could trust, and finally found Red Sentry. Red Sentry provided a full penetration test for their external, internal, and web app environments, and found 37 vulnerabilities. These findings were remediated and Red Sentry provided a letter of attestation that Trustvio could provide to their clients.

Because time was so sensitive to this startup, Red Sentry scheduled the test in 2 business days and had the final report delivered to the company 5 business days later. Other quotes they received required over 3 weeks to schedule and cost over 30% more.

BENEFIT

Trustvio was able to regain their prospects' trust and close their first contracts.

RESULT

Although they will always have a healthy fear of ransomware, the team at Trustvio can move forward more confidently now that they have Red Sentry behind them and a strong security program in place.

High-Severity Findings:

- MongoDB Backup Exposed
- Insecure Direct Object Reference (IDOR)
- Default Login Credentials
- SQL Injection