

**CASE STUDY**  
State Government

# The State of New Mexico

## Treasurer's Office Secured Classified Information

### CUSTOMER PROFILE

The State of New Mexico Treasurer's Office is a department of the state's government that oversees providing banking assistance and services to state agencies, validating bank activity, and managing and investing the state's operating cash, among other responsibilities. Simply put, the department is responsible for a large amount of private information.



*"The greatest benefits we receive from the RiskSense Platform is the quickness in turnaround and visibility to information that you receive within the Platform, which is important for our small team."*

– Brent Johnson,  
CIO / IT Bureau Chief,  
State of New Mexico



### THE CHALLENGE

A few weeks after new Chief Information Officer Brent Johnson started at the State of New Mexico Treasurer's Office, the department experienced a data breach. All of their sensitive information had been compromised. Both Johnson and the board realized there was a clear need for better management of their cyber risk. They needed more transparency into their information and a more precise look at their security posture. At the end of the day, they needed to make sure a breach never happened again.

With a small team of just three other people, Johnson knew that they needed to bring in a solution that would help them manage all of their data. There was too much information for the team to accurately handle by themselves. The board and upper management agreed and created a budget to bring in a cyber risk management solution.

From working at another agency, Johnson had prior experience with RiskSense and their attack surface validation services. He decided to call RiskSense and brought them in to see if their services could help the Treasurer's Office prevent another damaging breach.

### THE SOLUTION

After meeting with the RiskSense team, the State of New Mexico Treasurer's Office's board and upper management decided that they would make room in the budget to bring in RiskSense Platform to prevent a data breach from occurring again. RiskSense would come in to help Johnson and his team manage their large amount of security data, arrange remediation when needed, and observe the results. With more visibility into their secure information, the Treasurer's Office had a greater chance of preventing another breach.

When the department first implemented RiskSense, they started off by conducting an attack surface validation assessment. There would be an annual scan that would report back any vulnerabilities found on their network that potential hackers could exploit. At this stage, Johnson was receiving everything by paper, which still made it slightly difficult for his team of four to manage all of their information.

## The RiskSense Platform drastically improved remediation prioritization and validation times.

Shortly after, the office started to use the RiskSense Platform, which has since made it simpler for the Treasurer's Office to manage their cyber risk and protect their sensitive information. The RiskSense Platform allows the department to have a better understanding of what is going on in their network as well as where information and data was found. This allows them to fix vulnerabilities in a more timely manner than ever before. The Platform provides a near-real-time view from when the scan happens to when the information is available for Johnson's team to review online. This allows for immediate remediation while penetration testing continues.

To enhance their RiskSense experience, the State of New Mexico Treasurer's Office just invested in a Nessus Scanner to do their own penetration tests. This allows them to scan quickly and at any frequency interval, providing even more visibility into their security posture.

### THE RESULTS

Since implementing the RiskSense Platform, Johnson and his team at the Treasurer's Office have been able to more effectively manage their cyber risk.

The Platform allows them to have more transparency into what is going on with their data, which lets not only the team, but the board and upper management, to have superior visibility into their metrics and their security posture.

The dashboard within the Platform clearly illustrates where their greatest vulnerabilities lie and provides easy steps for remediation. The RiskSense Security Score, or RS<sup>3</sup>, helps the team monitor and track their overall exposure to risk. The RS<sup>3</sup> score can be used as a great visual tool to provide to the board to show the department's security progress. The Treasurer's Office

has found a lot of value in being able to clearly see where their biggest risks lie within their network, and it has helped them prove that they need a continuous budget for the software.

Before the RiskSense Platform was brought in, when the team tried to fix a vulnerability, they often could not tell right away if it worked. They would have to wait for the audits to come back before they knew that everything looked good. Now with their own scanner and the Platform, Johnson is able to see almost immediately if the remediation was a success. They no longer have to sit and wait for the results.

Because of both the quickness in turnaround of information and the visibility that the RiskSense Platform provides, the State of New Mexico Treasurer's Office has been able to successfully secure their classified information and prevent another breach from occurring.

### NEXT STEPS

Now that the State of New Mexico Treasurer's Office has successfully used the RiskSense Platform for some time, they are looking towards what's next. Since they invested in their own Nessus scanner, Johnson's team will be able to scan the network more frequently. This will provide them with more real-time updates into their security posture.

As the team grows, they will need to extend their coverage to look at the Internet of Things, but at the moment, they are not in a place to do so. In the meantime, RiskSense will continue to work closely with the Treasurer's Office to make sure they are satisfied with the Platform, that they are able to protect their network, and when the time comes, help them to explore the other services RiskSense provides.

### WHY RISKSENSE

Determine whether any of your business critical assets are at risk.

Gain insight on how your cyber adversaries operate based on RiskSense Platform threat intelligence and Proof of Compromise.

Synchronous delivery of findings in near-real time.

Get comprehensive recommendations for remediation actions.

Minimize your attack surface and cyber risk exposure.



Contact Us Today to Learn More About RiskSense

RiskSense, Inc. | +1 844.234.RISK | +1 505.217.9422 | info@RiskSense.com

© 2018 RiskSense, Inc. All rights reserved. RiskSense and the RiskSense logo are registered trademarks of RiskSense, Inc.

CONTACT US

SCHEDULE A DEMO

READ OUR BLOG

CaseStudy\_StateofNewMexico\_822018