# Municipality Protects Critical Windows Operating System Workloads

Located 15 miles south of downtown Tucson, The Town of Sahuarita was incorporated in 1994 and has over 34,000 citizens. It has a $95.7 million annual budget and is one of Arizona's fastest-growing communities. Sahuarita residents have convenient access to the Tucson International Airport and the University of Arizona, one of the world's top 100 research institutions.

Facing an increased risk of ransomware attacks targeting state and local government, the organization wanted to deploy a defense-in-depth security model but faced several key challenges, including limited resources of the small IT team, an outdated first-generation security posture, and legacy security tools that generated a large volume of false positives to manage.

The organization knew they wanted to invest in additional server protection to diversify and have multiple layers of defense. They chose the Virsec Security Platform (VSP) because it was proven successful in stopping malware exploits targeting Microsoft vulnerabilities, even vulnerabilities that aren't patched.

**The Virsec Security Platform (VSP) provides Zero Trust Runtime Defense with a 'default-deny, allow-trusted' approach. Throughout the deployment, the organization proved that application control and allowlisting can be easily implemented with automation, tuning, and an excellent customer success team.**

> *It's always been my business philosophy that we need different layers of protection, and I wanted a defense-in-depth strategy to strengthen our security posture. We deployed the Virsec Security Platform to help my small team be more effective and lower the number of false positives, and it has proven successful in stopping malware exploits targeting Microsoft vulnerabilities.*

~ Ronald Bishop, Director of Information Technology
Town of Sahuarita

virsec™ Autonomous Application Control You Can Trust

To learn more about the Virsec Security Platform and to find out how to start protecting your mission-critical server workloads, visit us at **www.virsec.com**

## *Virsec Customer Success Profile*


**Industry**
State and Local Government

## Key Challenges

- Small IT team with limited resources to manage constant vulnerability patching
- Outdated first-generation security posture left the team unable to respond to the growing system intrusions targeting Microsoft Operating Systems.
- Legacy security tools generated a large volume of false positives that exceeded the capacity of their team.
- Existing security tools on the servers didn't catch critical vulnerabilities, leaving them vulnerable to exploits
- Increased risk of ransomware, with more than three-quarters of attacks targeting state and local government, and most of those stemming from exploited vulnerabilities

## Business Outcomes

- Investment recovered in less than 1 year through other security tool displacement and improvements in resource utilization
- Strengthened security posture by implementing a defense-in-depth strategy
- Team morale improved, knowing they can sleep at night, worry less about their server security, and allows them to deploy necessary patches on a routine basis, rather than panic patching
- Drastically reduced the number of false positives the small team had to manage, allowing them to prioritize other IT initiatives
- Full compliance with the Arizona Municipal Risk Retention Pool (AMRRP) by providing compensating security controls