government technology

# Securing the Distributed Workforce: San Joaquin County

San Joaquin County, Calif., is one of the first counties in the country to have a three-year cybersecurity plan. In this Q&A, **Chris Cruz**, director/CIO of the county's Information Systems Division, shares insights with Teri Takai, co-executive director of the Center for Digital Government, on how the plan and its enterprise-wide endpoint protection initiative paved the way for moving thousands of employees to remote work when COVID-19 struck.

**Can you talk about San Joaquin's cybersecurity strategy and how it prepared the county for remote work?** In 2019, we developed a three-year cybersecurity strategy. We are now in year two and have implemented multiple strategic initiatives, including yearly performance metrics milestones for people, process and technology buckets in cyber strategy. In terms of policy, we're using Tanium for asset visibility, endpoint remediation and vulnerability remediation. These tools integrate with our security incident and event management (SIEM) solution, which we use to monitor and manage security events across the county. Multiple initiatives within our plan addressed key requirements for remote work, which helped us move quickly to a secure virtual working experience when the pandemic hit.

**Did you have to modify any plan elements to accommodate remote work?** To our benefit, weeks before the pandemic hit, we started upgrading network bandwidth and utilization to accommodate a hybrid working model and virtual private network (VPN). This helped with the onslaught of 5,000 plus workers suddenly in full-on telework mode. In addition, because we had Tanium endpoint protection, we could allow people who didn't have laptops to bring home their county-provided desktops. We updated our telework plan to allow two to three days of remote work per week, with the modification that performance metrics would be tied into the employee's job performance. The VPN metrics show that people are giving the county eight to nine hours of work a day. That has changed the whole mindset of the board of supervisors, the county executive officer and the department heads about telework and its potential.

**How has your unified endpoint management and security platform helped you manage risk?** It's all about visibility. A single pane of glass is key to avoiding blind spots and managing risk. Unified endpoint management tools such as Tanium's help us detect, remediate or reduce risk in a matter of minutes. They also help us enhance network hygiene and monitoring, as well as continuously improve our security posture. Besides enabling a secure virtual working platform, these tools will allow us to create secure environments for our sheriff's department and its patrol cars, our district attorney's office, our county hospital with all its HIPAA compliance requirements, our registrar of voters and 27 other departments once they are fully deployed.

**Beyond cybersecurity, what other benefits have you found?** The diversity of modules across the unified endpoint protection platform enables a range of capabilities. For example, with asset management, we were able to look across the entire network and identify software that we were not using but paying costly maintenance fees for. Eliminating that technology helped us create ROI and a tangible business case. The tool is also our major point of reference for performance metrics and risk management. We can look at endpoints and protection across the entire network, and then make decisions to manage risk appropriately. That enables the CIO and the CISO to work together to create the right policy in the county, provide the necessary direction and ensure we have the technology to do the job.

**What's next for the county?** COVID-19 and the onset of the November election have given the county the opportunity to get on a faster track for innovation and transformation. Leaders and department heads now have more confidence in telework. We're now looking at a permanent remote/virtual work plan for the entire county. Part of our strategy is to set up a virtualized work environment long term, not just within San Joaquin County, but also for other cities and educational institutions in our ecosystem. The virtual work environment is here to stay. It makes sense to protect everybody's data. By setting up the technology and having it appropriately managed and secure, we'll be better off now and into the future.