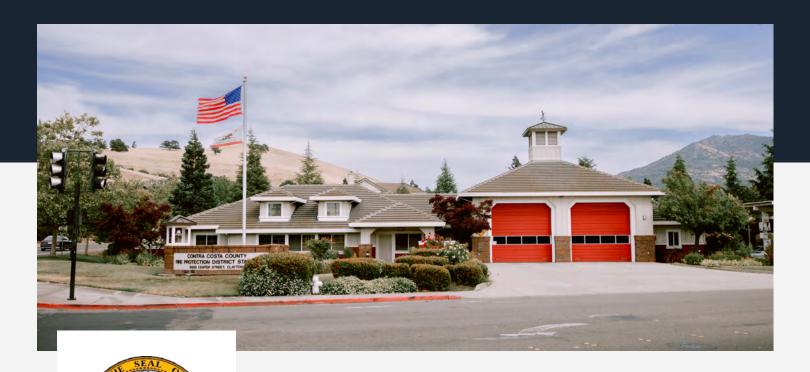TANIUM™

Contra Costa County protects endpoints, unites operations and security with Tanium

The California county government agency struggled to support their departments, secure remote devices, and even suffered a ransomware attack. That is, until it discovered Tanium.

ORGANIZATION

Contra Costa County

LOCATION

California, USA

The school of hard knocks is harsh. But its lessons can be valuable and lasting.

Just ask Contra Costa County. The California county – the name is Spanish for "opposite coast," reflecting its location across the bay from San Francisco – is home to 1.16 million residents living in 55 communities. Founded in 1850, Contra Costa is also one of California's original 27 counties.

Maintaining Contra Costa's more than 10,000 county-owned endpoint devices is far from simple. The county's responsibilities are diverse, with departments and offices ranging from agriculture and fire protection to veterans' services.

Some departments have required sophisticated work from the county's full-service IT department. That's included the creation of a geospatial mapping system, requested by the office of emergency services, to power dashboards that warn the public about local wildfires.

In addition, many of the county's nearly 10,000 employees still work remotely at least part-time, a trend that began during the pandemic. Remote work has made it harder for the county's IT department to identify, monitor, and manage all its endpoint devices. "We had to enable thousands of workers to work remotely on very short notice," says Marc Shorr, the county's CIO.

Most challenging of all, two years ago Contra Costa County's library system was breached by a ransomware attack. At the time, securing the library wasn't the IT department's responsibility (it is now). Nonetheless, the attack led CIO Shorr to realize that the county's then-current malware and antivirus software wasn't up to the task.

"Now Tanium is part of our core package. Every deployment we do, Tanium is part of that rollout. It's allowed our organization to transition from being reactive to proactive. And it's been a huge success story for us."

Marc Shorr
CIO, Contra Costa County

Clearing the deck

All that led Shorr to replace the county's older defenses with Tanium. After the attack, IT was asked to assume responsibility for the library's technology and shore up its defenses.

One surprising aspect of the project was just how difficult it was to remove the older antivirus and malware-blocking software. "We had a very difficult time," Shorr remembers. "Tanium stepped up with resources to address the problem. Now Tanium is part of our core package. Every deployment we do, Tanium is part of that rollout. It's allowed our organization to transition from being reactive to proactive. And it's been a huge success story for us."

It was a bit later when the county's CISO, Nathan Wiebe, says he really discovered Tanium. It was at the company's 2022 Converge conference. There, he heard Tanium staffers discuss the importance of having both the security and operations teams leveraging the same interface, ecosystem, metrics, and dashboards.

"That really has resonated with me and our executive team," Wiebe says. "We want to drive strategy and decision-making through a centralized platform where we have shared KPIs and an understanding of our organizational health."

Consistently secure

Tanium has helped the Contra Costa IT department unify the county's various departments on a consistent approach to endpoint visibility, security, and management. "As our departments see the success that central IT has had with Tanium, they become advocates for the approach," Wiebe says. "They're actually asking us to enable Tanium's capabilities in their own departments." All that, he adds, has led to greater consistency and more robust security.

Tanium is also helping Contra Costa County follow a security framework known as the Center for Internet Security (CIS) Critical Controls. This is a prioritized set of actions that organizations can take to protect themselves from cyberattack vectors.

"Tanium actually aligns with a number of these controls," says CISO Wiebe. "When we get an indicator of a compromise or information about an adversarial operation, Tanium helps us look at the CIS-ranked risks based on these controls. It's really quite amazing."

Monitoring potential risks is even easier with Tanium's dashboards, Wiebe says. Before the county used Tanium, when an alert was received, there was what Wiebe describes as "a lot of piecemealing," leading to extra work and dangerously slower responses.

But now, the county's security and operations teams can easily look up the vulnerability on their Tanium dashboard. They can then determine whether the threat poses a risk to the county. And if it does, they can determine which assets are potentially exposed and then remediate the risk. This all helps contribute to a safer, more secure environment for the community to live, and conduct business within. That's a lesson worth learning.

> "When we get an indicator of a compromise or information about an adversarial operation, Tanium helps us look at the CIS-ranked risks based on these controls. It's really quite amazing."

Nathan Wiebe
CISO, Contra Costa County

Results overview

Modernization

Tanium helped Contra Costa County remove older, ineffectual antivirus and malware-blocking applications.

County-wide visibility

County departments, seeing the success IT has had with Tanium, now ask for it to be deployed in their offices, too.

Following the framework

Contra Costa County uses Tanium to follow the CIS Critical Controls, prioritized actions that help organizations protect themselves from cyberattacks.

Protecting the community

Tanium has helped the IT department better secure and manage the county's endpoints, protecting the community's ability to access county services when they need it.

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

TANIUM