DELLTechnologies

Improving security safeguards without adding to costly headcount

To significantly strengthen its cybersecurity, a large Southwestern U.S. county turned to Dell Managed Detection and Response.

> ❝
>
> "We knew we needed to improve our security posture. Dell Managed Detection and Response gets the job done without additional headcount."
>
> **Director of Information Systems**
> Large Southwestern U.S. County

Business needs

With the rapid rise in ransomware and other cyberthreats targeted against state and local governments, a large, growing county located in the Southwestern U.S. sought to strengthen its security posture and enhance its ability to detect and respond to threats without the cost and effort required to hire and train additional security specialists.

Business results

- Improves the county's security posture without increased headcount.
- Supplements the IT team's knowledge, skills and ability to scale.
- Frees the staff from the burden of 24x7 threat monitoring and response.
- Streamlined the detection and quick remediation of a server breach.
- Offers the comfort of experienced specialists the county can depend on.

Solutions at a glance

- Managed Detection and Response

A large, rapidly growing county located in the Southwestern U.S. serves several hundred thousand residents and is known for its diverse base of businesses ranging from vibrant medical, biotech and manufacturing firms to vital agricultural and farming operations.

In recent years, cybersecurity threats against state and local governments have increased dramatically. In the U.S. in 2020, 79 ransomware attacks resulting in nearly $19 billion in downtime and recovery costs were launched against government entities at all levels nationwide.[1]

After a disappointing experience with another vendor's offering, the Southwestern U.S. county chose Dell Managed Detection and Response, powered by Secureworks® Taegis™ XDR security analytics software. The solution is a managed, end-to-end, 24x7 service that monitors, detects, investigates and responds to threats across the county's entire IT environment.

"We knew we needed to improve our security posture," says the county's director of information systems. "Dell Managed Detection and Response gets the job done without additional headcount."

Combining two key capabilities

The solution brings together the two most critical components of a formidable security posture:

- The expertise of Dell Technologies security analysts to complement the county's lean team consisting of a single security analyst, plus a system administrator and engineer

- The wide-ranging capabilities of Secureworks Taegis XDR — a cloud-native security analytics platform designed to detect the most advanced threats — allowing MDR analysts to streamline and collaborate with the county on investigations, and ultimately help them take the right actions to mitigate any impacts

> "
>
> "When we required the help of Dell Technologies specialists, they virtually parachuted in for a week or ten days and we knew we were in good hands."
>
> **Director of Information Systems**
> Large Southwestern U.S. County

[1] Bischoff, Paul, "Ransomware attacks on US government organizations cost $18.9bn in 2020," Comparitech, March 17, 2021. https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

D∢LL Technologies

"They helped us install software agents on every server and workstation, with selected triggers to stop services or shut down a machine or account and notify us should a threat be detected," the director of information systems explains. "Dell Technologies specialists provided us valuable advice and prioritized what steps we needed to take over the 90 days we implemented everything."

Quickly mitigating a breach attempt

The solution also includes up to 40 hours quarterly of clearly spelled out guidance to respond to and remediate threats in even the most complex situations, as well as another 40 hours annually to investigate activities and initiate recovery from severe security incidents, if necessary.

"What really sold us on the solution was when we had an actual breach attempt," recalls the county's director of information systems. "A hacking group discovered an exploit in the Microsoft Exchange email server. After being notified by Microsoft and our state's cybersecurity agency, we discovered that one of our three servers had been compromised. The Dell Technologies team was very thorough in investigating the breach and helping us restore our server."

He continues, "My recommendation for any county CIO would be to go with an enterprise-class security solution such as Dell Managed Detection and Response, rather than an offering from a virus protection software vendor. When we required the help of Dell Technologies specialists, they virtually parachuted in for a week or ten days and we knew we were in good hands. We worked smarter together, and there was a lot of synergy between our teams."

3

Learn More about Dell Managed Detection and Response

Contact a Dell Technologies Solutions Expert

DELLTechnologies

Connect on social