MANAGED SOLUTIONS

Case Study

CROWN CASTLE | CYFLARE

CYBER DEFENSE powered by CyFlare

Providing a city government with greater visibility with Cyber Defense XDR.

City governments of all sizes are becoming increasingly vulnerable to ransomware attacks with the prevalence of distributed workforces. The government of a city in the US knew they were vulnerable to complex, multi-vector attacks. They needed a way to combat this growing ransomware threat while maintaining their lean IT team.

The Need

With a small team that included a Deputy CIO and four security analysts, the City government knew they had to either hire more analysts or find a way to reduce the many burdens their current security stack had placed on the team. To improve their cyber security while simplifying threat detection, they needed to:

- Decrease vulnerabilities that came with only using firewalls and a security information and event management (SIEM) system to protect its network.
- Address the wasted time analysts spent operating different sets of tools and the lack of transparency that resulted from not having full visibility into their environment.
- Reduce complications from their current threat detection and blocking processes.
- Increase productivity without expanding their internal security team.

> “The visibility we get into our environment is outstanding, whether it’s east/west traffic or north/south traffic, and we can triage from a generated incident to the source of what caused that incident. The Open XDR platform proved to be the solution needed to strengthen cyber security capabilities while holding the line on [our] IT budget.
>
> **DEPUTY CIO**
> City Government

Industry
State and local government

Solution
Cyber Defense

Population
>650K residents

The Solution

- Cyber Defense XDR technology integrates data from the City's existing security tools and its proprietary sensors to deliver a comprehensive picture of the entire environment.
- The city's new solution is more streamlined, combining NG-SIEM, NDR, IDS, UEBA, SOAR, malware/phishing and several other key security tools—all under a single interface.
- Cyber Defense XDR simplifies detection and response by leveraging AI and machine learning, ultimately producing a prioritized list of contextual incidents in our Cyber Defense portal.
- Their new solution provides greater visibility, allowing users to triage from a generated incident to the source of the incident.

The Impact

- According to the Deputy CIO, the City can now get to the bottom of an incident within five to ten minutes versus before, which would take days or even weeks to thoroughly investigate and resolve.
- The City is now able to provide meaningful reports to keep their CIO updated, and their analysts are more productive while quickly detecting and responding to threats.
- More efficient use of internal resources has allowed the City to stay within their budget.

Why Crown Castle?

Our unique, nationwide portfolio
With approximately 90,000 route miles of fiber, we own and operate one of the largest and densest fiber networks in the country with a presence in 23 of the top 25 US markets.

Our proven track record
In our 30 years of experience owning and operating network assets we've seen it all and we're always ready to adapt to changing network trends.

Our deep expertise
We've worked with nearly every industry so we understand your unique opportunities and challenges and can tailor solutions to meet your goals.

CROWN CASTLE

Crown Castle owns, operates and leases more than 40,000 cell towers and approximately 90,000 route miles of fiber supporting small cells and fiber solutions across every major US market. This nationwide portfolio of communications infrastructure connects cities and communities to essential data, technology and wireless service—bringing information, ideas and innovations to the people and businesses that need them.

For more information, please contact 888-906-9061 or visit CrownCastle.com