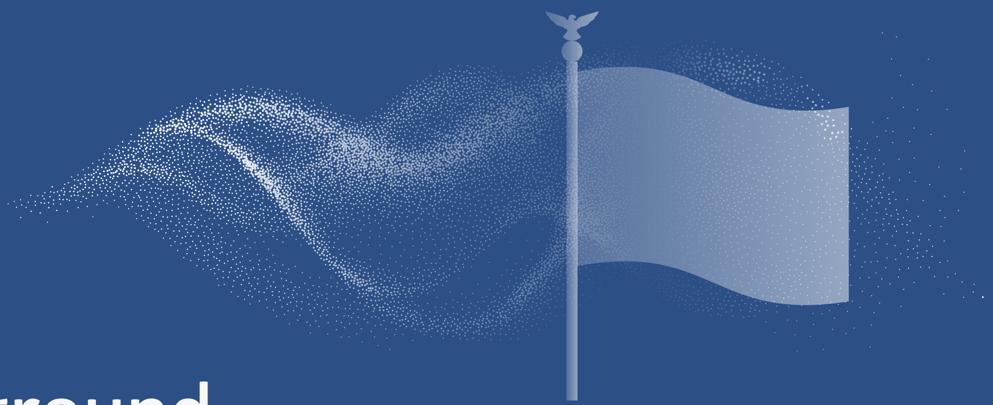
cloudcover®

# No More Hacking: Proactive Cybersecurity Solution for Midwest Local Government

With the help of the CC/B1 Platform™, a large Midwest County government upleveled its cyber defense and protected itself against more than 730,000 priority level-one threats.



# The Background

Cyberattacks can have catastrophic consequences for Local and County governments, including putting residents' lives at risk.

Cyberattacks for Local and County governments are on the rise. A recent survey of the Coalition of City Chief Information Security Officers – a group of municipal leaders and cybersecurity professionals – revealed that 50% of the group said they had experienced three or more cybersecurity incidents over the past month. In contrast, only 7.1% of those surveyed reported zero cybersecurity incidents in the past year.

**50%**
**REPORTED CYBERSECURITY INCIDENTS**

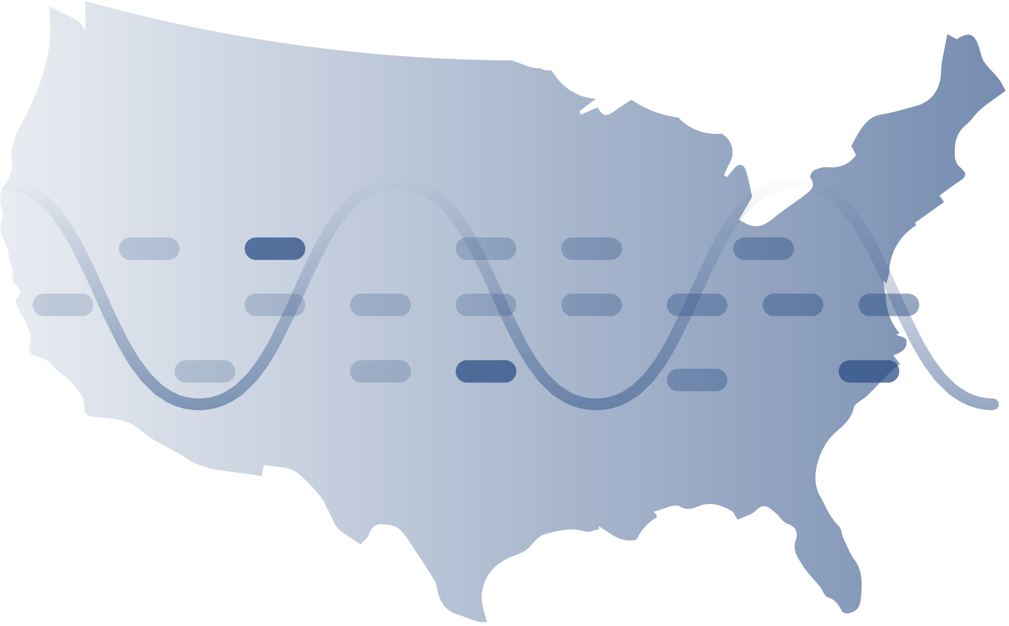
Those attacks are also making headlines. Here are just a few news stories that point to how much Local and County governments are being affected by data breaches.

**"Hackers post hundreds of pages of purported internal D.C. police documents."**
(The Washington Post)
In April 2021, a group calling themselves Babuk infiltrated the D.C. Police's computer network, threatening to make hundreds of pages of internal files public unless they were paid a specific amount as a ransom.

**"Baltimore County Schools suffered a ransomware attack. Here's what you need to know."**
(The Baltimore Sun)
A ransomware attack shut down the school's entire system in October 2020, halting classes for the 115,000 students that were attending virtually due to COVID-19. Nearby Fairfax County Public Schools – the largest public school system in the Baltimore-Washington metropolitan area – had been targeted just a few weeks prior.

**"Ransomware attack on Hampton Roads Sanitation District knocks out billing system."**
(The Virginian-Pilot)
The Hampton Roads Sanitation District, a government sanitation entity that serves the nine-County Hampton Roads region in Virginia and North Carolina, suffered a ransomware attack that took down its entire network and suspended the billing system.

Local government entities have become prime targets for cyberattacks. In 2020, more than 2,300 governments, healthcare facilities, and schools in the United States were impacted – and the threat stayed consistent in 2021 (Elwood, 2021). Public utilities, such as power and water systems, are also a particular focus for cybercriminals, as recently evidenced by the attack on a water treatment plant in Oldsmar, Florida.



Those government bodies that find themselves on the receiving end of a data breach or cyberattack can expect the "usual" impacts, such as:

- Logistical headaches
- Financial loss
- Disruption of legal and court business
- Loss of public trust
- Potential insurance loopholes, resulting in declined coverage

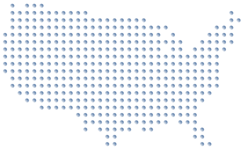
However, there are also repercussions that are specific to Local government:

- In the case of the Oldsmar water plant, hackers upped the sodium hydroxide settings to extremely dangerous levels. Other attacks can halt a community's emergency response capabilities, especially if 911, police department, or highway department systems go dark because of a data breach or ransomware attack. The absence of these services, no matter how short, could be devastating for a community by putting residents' lives at risk.
- Local governments are linked to their state and federal counterparts. If a County government becomes compromised, they're only one step away from a potential infiltration on a much larger level.

# The Challenge

Under consistent attack by malware that was costing hundreds of thousands of dollars in cleanup costs, a large Midwest County government looks to increase its level of cyber defense.

Cybersecurity for governments at the Local or County level is challenging, and they're susceptible to ransomware attacks and other cybercrimes for numerous reasons.



- **Sheer volume**
  According to the International City/County Management Association (ICMA), there are 90,075 units of Local government in the U.S. Of those, 3,031 are County-specific, 19,475 are municipal entities, and 16,253 are Town or Township governments (Norris, 2021).

- **Critical IT systems**
  While there's a substantial difference in tech sophistication between large metropolitan County governments and their smaller counterparts, most Local governments have some type of technology they depend on to efficiently provide services and utilities to their residents.

- **Lean budgets and minimal staff**
  Local governments often have constraints on spending, and many are not able to purchase expensive, state-of-the-art cybersecurity for government technologies. They're also not able to attract qualified cybersecurity staff – depending on the size of the entity, there may only be one IT staff member to handle a myriad of priorities.

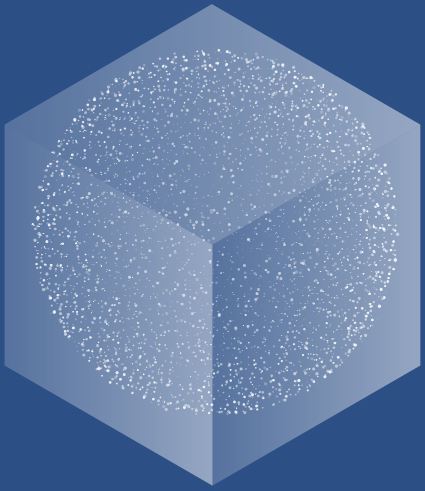
- **Valuable information**
  Local government data is a treasure trove of personally identifiable information, including names, addresses, social security numbers, dates of birth, credit card numbers used for billing and payments, medical information, and tax records – not to mention the financial information of the government body itself. Cybercriminals can extort this data and either sell it or hold it for ransom.

- **The Internet of Things**
  Technology continues to evolve faster than the organizations utilizing it, and the IoT has introduced new risks and vulnerabilities when it comes to cybersecurity for governments. As the IoT includes hardware, software, and data, it increases an organization's attack surface exponentially, opening governments up to increased cybercrime.

Knowing these factors, our client – a large Midwest County government – knew they needed a higher level of protection. When they reached out to us, they were being attacked by malware, even though they were using well-known, name-brand security technologies – CheckPoint, Surf Control and Barracuda. They thought they were well protected, but the malware attacks kept coming.

Despite the County's sizeable investment in these cybersecurity technologies, they learned they were the victim of an attack by a rootkit virus. A rootkit is a malicious software bundle designed to give unauthorized access to a computer or software. Hard to detect, rootkits conceal their presence within an infected system, but actively listen for open ports and steal command line code.

In our client's case, the rootkit virus had cost the County hundreds of thousands of dollars in cleanup before they reached out to us. As the vulnerability grew with size and complexity, they wanted technology that could not only help them be aware of the threats to their network security landscape but stop them completely.

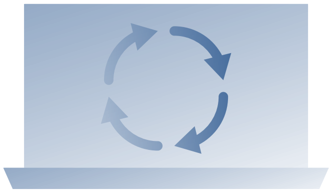


# The Solution

Proactive risk aware, risk control, and risk transfer with the CloudCover CC/B1 Platform™.

Encompassing three core elements – risk aware, risk control, and risk transfer – the CC/B1 is an Intelligent Threat Management™ platform that can identify and stop all incoming cyber threats or ransomware attacks – in microsecond speed, with near zero-positive threat accuracy – at the TLS handshake before they can enter an organization's network. After speaking to several government entities that had also worked with CloudCover, the County's IT department brought in the CC/B1 Platform.

The platform relies on patented AI/ML (automated intelligence/math-based learning) X/NDR (extended network detection and response) SOAR (security orchestration, automation, and response) technology that collects data from all corners of an organization's network (devices, software, data at rest, and data in motion) and streamlines it into a single view of IT events and suspicious traffic.



Because of its deep learning capabilities, the CC/B1 performs as a Firewall Everywhere™ – while most firewalls only look at ingress traffic, our platform looks at egress traffic as well as laterally, in all directions. This coverage makes it possible to generate algorithms that analyze and learn from a network's behavior, allowing the network to be monitored without human intervention.

**Outcome:** We deployed the CC/B1 within minutes and it began to demonstrate its value in 72 hours.

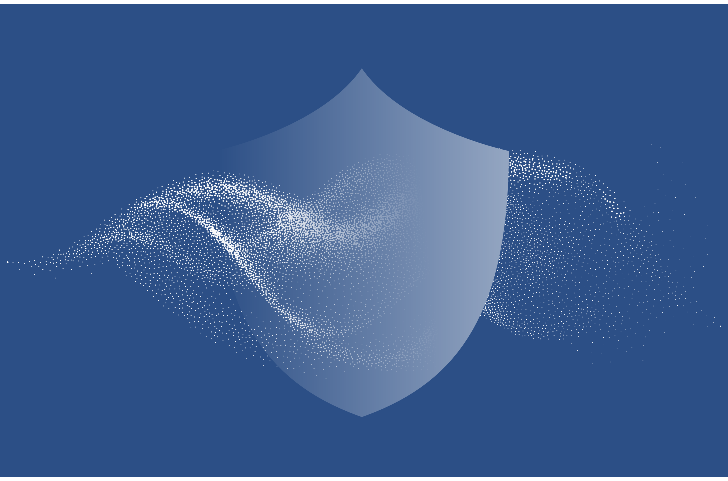
# The Results

## After showing immediate benefit, the CC/B1 goes on to detect and stop over 730,000 unique cyber attacks.

After 45 days of testing, the CC/B1 had defeated several sophisticated attacks that previously compromised the government's IT network. After a review of the results, the County went ahead and purchased the CC/B1, replacing all other security technologies and increasing the effectiveness of their network.

As of September 2020, the CC/B1 had logged 732,762 priority level-one attacks – an incredible feat, as just three of these attacks would have defeated their previous security technologies.

In addition to the hard numbers, there are qualitative data points as well. The County's "small but mighty" IT department sleeps better at night, knowing that there's ongoing monitoring of the organization's security posture in real time. This allows them to focus on other efforts and use their time more efficiently.



**732,762**
**Attacks Prevented**

## Cybersecurity for governments is too important for a reactive approach. Shift to a proactive CyberSafety posture, take a look at the CC/B1 Platform™ by requesting a demo.

References
Elwood, Karina (August 21, 2021). "Ransomware poses threat to vulnerable Local governments." The Washington Post.
https://www.washingtonpost.com/local/local-government-ransomware-dc/2021/08/05/048051cc-efc6-11eb-81d2-ffae0f931b8f_story.html

Norris, Donald F. (July 14, 2021). "A Look at Local Government Cybersecurity in 2020." International City/County Management Association (ICMA).
https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020