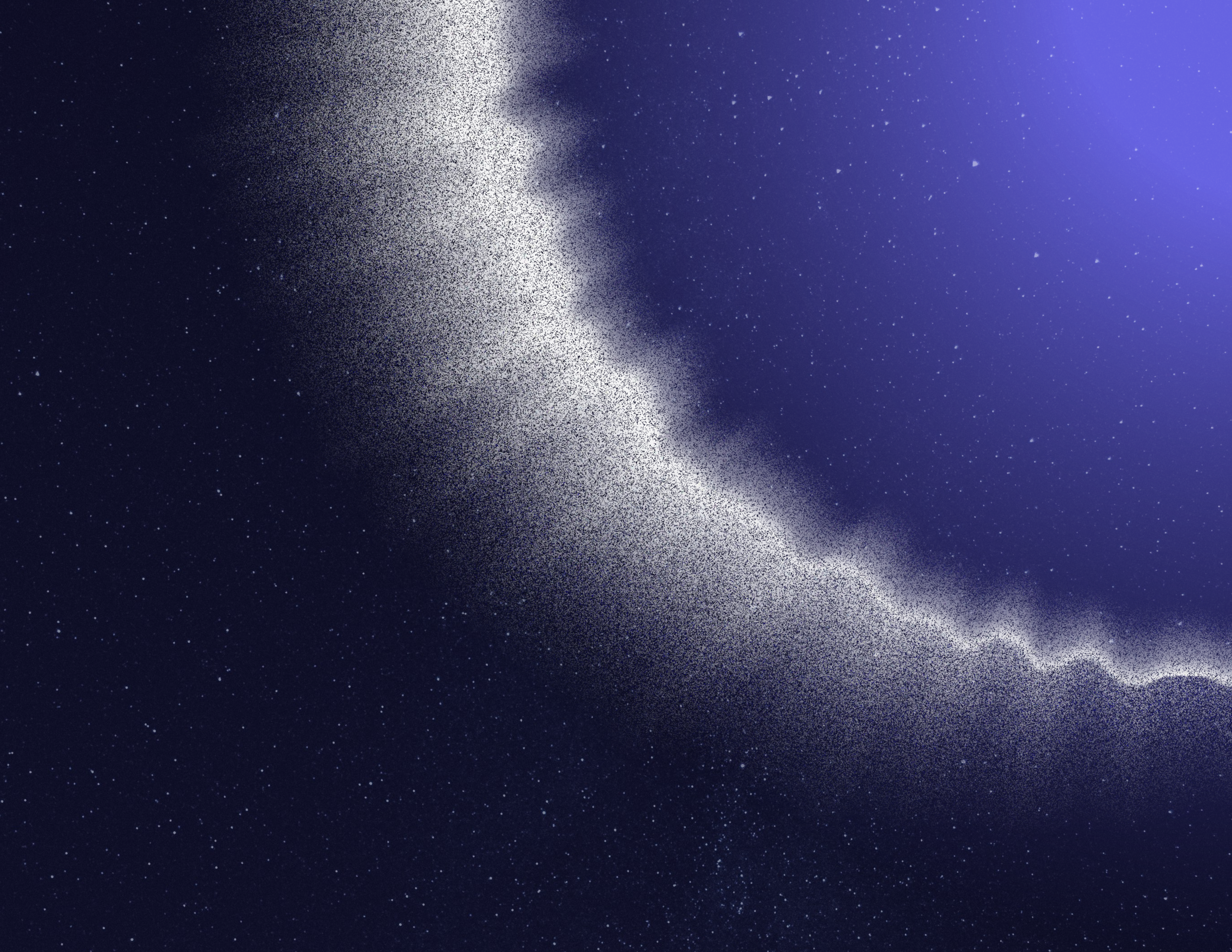
CYBER PROTECTION FOR LOCAL GOVERNMENT

Proactively Protect your Critical Assets



Local governments are on the front lines of an escalating cyber war, facing increasingly sophisticated and relentless attacks.

With limited resources and often outdated defenses, they are prime targets for cybercriminals seeking to exploit vulnerabilities.
The following provides a comprehensive guide to fortifying local government cybersecurity, offering strategic solutions and best practices to combat and prevent cyber crime. By adopting these intelligence-driven approaches, local governments can enhance their defenses, protect sensitive data, and ensure the uninterrupted delivery of essential public services.

The Growing Threat

According to a Center for Internet Security report, these entities experienced

148% **more** malware attacks

and 51% more ransomware incidents during the first eight months of 2023 compared with the same period in 2022.

Moreover, data breaches and other endpoint security service compromises rose by

313%

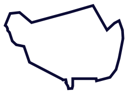
while non-malware intrusions grew by 37% during the same timeframe.

The escalating cybersecurity threats against state and local government entities can be attributed to a lack of established cybersecurity programs, inadequate funding, emerging technologies, and increasingly advanced threats. These challenges hinder the development of robust cybersecurity defenses, leaving these entities vulnerable to a range of cyber threats.

The Impact of Cyber Attacks on Government Agencies

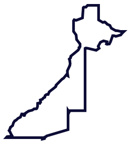
The escalating cybersecurity threats against state and local government entities can be attributed to a lack of established cybersecurity programs, inadequate funding, emerging technologies, and increasingly advanced threats. These challenges hinder the development of robust cybersecurity defenses, leaving these entities vulnerable to a range of cyber threats.

Lowell, MA



The city experienced a significant cyber attack, which impacted the municipality's computer systems. Servers, networks, phones, and other systems throughout the City became inaccessible.

Lowell, MA



Allocated $10.2 million to replace outdated software and an additional $1.2 million for verification and validation services following a cyber attack that shut down many of the county's operations including the Fulton County jail.

Coeur d'Alene, ID

Detected malware in its computer network that took the system offline, taking the city's website completely offline as well as the phone system for three business days.

Pennsylvania Court System

Encountered a major cyber breach affecting operations including downing several of the courts' computer systems, including online docket sheets and an electronic case document filing portal. While officials said the attack didn't compromise any data or interrupt the courts' regularly scheduled operations, court officials were forced to log court filings by paper and by mail.

Office of the Colorado State Public Defender

Suffered from a cyber attack impacting services including court schedules for those who cannot afford private counsel, trial judgements and access to case information, which resulted in hearings getting postponed for weeks.

The FBI reports that cyberattacks against government offices rose by nearly 36% from 2022 to 2023. These attacks impact community services that we all depend on, and any breach of private data can have a significant impact at an emotional, physical, and personal level for all service users.

Rethinking Cybersecurity: The Need for Intelligence Powered Cybersecurity

Proactive Defense

Traditional cybersecurity measures are often reactive, addressing threats only after they have infiltrated the network. Intelligence powered solutions, however, shift the paradigm to proactive defense. By leveraging real-time threat intelligence from a global network, these solutions identify and neutralize potential threats before they can cause harm, providing local governments with a robust security posture.

Enhanced Visibility and Efficiency

Intelligence powered cybersecurity offers enhanced visibility into potential threats, enabling intelligence operations analysts to monitor and analyze vast amounts of data in real-time. This visibility is crucial for anticipating and mitigating risks. Organizations using intelligence powered solutions have reported a 50% reduction in time to detect threats and improved incident response times. For local governments, this means quicker responses to potential threats and a more secure environment for sensitive municipal data.

Efficiency and Cost-Effectiveness

Deploying an intelligence powered cybersecurity solution can significantly reduce the operational burden on IT teams. Automated threat detection and response capabilities minimize the need for manual intervention, allowing IT professionals to focus on more strategic tasks. Additionally, these solutions offer a cost-effective alternative to building an extensive in-house security infrastructure – a challenge that local government agencies often face.

- **Cost Savings:** Local governments can save up to 25% on overall cybersecurity costs by using intelligence-powered solutions.
- **Resource Allocation:** IT teams can reduce time spent on threat analysis by 80%, reallocating resources to more critical areas.

By adopting intelligence powered cybersecurity solutions, local governments can enhance their defense capabilities, improve efficiency, and achieve significant cost savings.

Maximize the Potential of Intelligence Powered Cybersecurity for Local Governments with These Three Strategic Steps

01

Utilize the Latest Threat Intelligence for Real-Time Protection:

Leverage the latest threat intelligence from the cybersecurity community and industry to enhance your defensive posture. By applying this intelligence in real-time, local governments can gain a distinct advantage. Blocking malicious and reconnaissance traffic before it enters the network eliminates threats before they can cause harm, ensuring the protection of sensitive municipal data.

02

Collaborate with Cybersecurity Experts Using AI and Human Intelligence:

The scale of cyber protection is now so vast that leveraging industry-wide expertise is essential. Partnering with cybersecurity experts who utilize powerful AI-enabled tools and deep industry knowledge can significantly bolster your defenses against a wide array of threats. Local governments can benefit immensely from these collaborations, enhancing their security measures without overextending their resources.

03

Collaborate with Cybersecurity Experts Using AI and Human Intelligence:

Security incidents at one local government often occur at others as well. By sharing threat data, municipalities can collectively improve their defenses. Geographic and sector-specific communities can exchange experiences, indicators of compromise (IOCs), techniques, and resolutions. Sharing threat data is increasingly becoming a regulatory requirement. Immediate strategic gains can be achieved by working with experts who can interpret and rapidly deploy community learnings, strengthening the overall cybersecurity posture of local governments.

THE SOLUTION: PROACTIVE PROTECTION WITH CLEANINTERNET®

Centripetal's CleanINTERNET® solution presents a tailored approach to the unique needs of local government agencies. In an environment where time-sensitive operations and classified documents are under continuous attack. CleanINTERNET® harnesses real-time threat intelligence from a global network, providing visibility into potential threats before they can affect your systems. This technology serves as a protective barrier, ensuring the security of sensitive information.

> "I did some spot checking on the firewall logs before Centripetal - 60 million before the appliance was implemented down to 500,000 the other day."
>
> - CENTRIPETAL CUSTOMER

CleanINTERNET® is an intelligence powered security solution that utilizes high-performance computing technology, patented software algorithms, and highly skilled security analysts to offer a cost-effective alternative protection strategy.

Local governments that have adopted CleanINTERNET® are impressed by its comprehensive capabilities, which far exceed basic intelligence feeds. Achieving a similar security posture independently would be financially unfeasible.

CleanINTERNET® revolutionizes cybersecurity by prioritizing threat intelligence and shifting from reactive to proactive defense. This enhances the efficiency and effectiveness of security teams. With advanced shielding technology, CleanINTERNET® eliminates the majority of threats and mitigates the impact of any malicious code that breaches defenses. The technology blocks malicious network attempts from known sources, prevents outbound activity to malicious domains, and eliminates unnecessary reconnaissance traffic from your network.

By implementing CleanINTERNET®, local governments can quickly bolster their cyber defenses without significant financial investment or the need to expand their cyber analyst teams. This solution greatly reduces the number of security events, allowing IT teams to focus on delivering essential services with greater confidence.

For Local Government The Stakes Have Never Been Higher

For local governments, embracing intelligence powered cybersecurity solutions is not just an option; it's a necessity. By being proactive, you can transform your defenses and ensure robust protection for your sensitive data and municipal operations. Take the lead in cybersecurity innovation and safeguard your community against the threats of today and tomorrow.

The tools and strategies are within your reach, and won't blow your budget. Seize them to protect your community and uphold your reputation in an increasingly digital world.

CENTRIPETAL

centripetal.ai