MENLO SECURITY

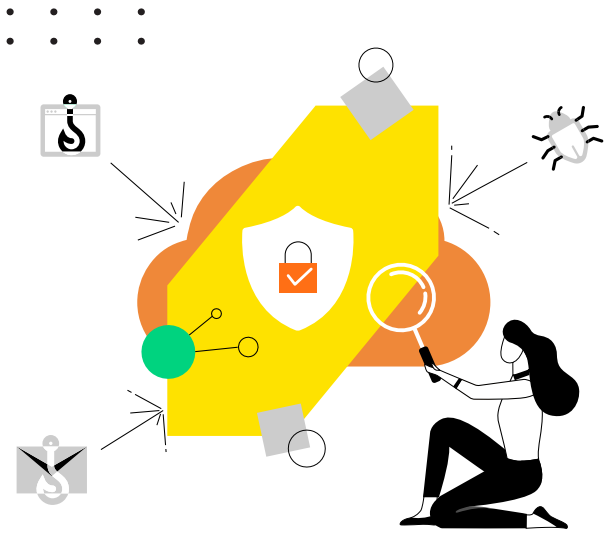
Ransomware: State & local governments fight back.

Federal money is on its way. Now state and local governments need to get results.

Use Case

Modern security for state and local goverments

The recent allocation of $1 billion in cybersecurity funding[1] for state and local governments shores up a critical weak point that has left them open to devastating ransomware attacks: limited budgets that are already stretched thin. The federal funds are included in the State and Local Cybersecurity Grant Program of the bipartisan Infrastructure Investment and Jobs Act, which President Biden recently signed into law. With a cash infusion in the pipeline, states, counties, cities, and towns will soon have the means to protect themselves. But money alone won't be enough. To keep ransomware at bay, effective strategies and proven technologies will need to be implemented and then supported for the long haul.



Attacks are legion—and costly

Although an exact tally is elusive, it is estimated that hundreds of municipalities suffer ransomware attacks annually, leading to painful decisions whether to pay up. Atlanta refused to pay $51,000 in ransom but ended up paying some $17 million in recovery costs[2] according to one estimate. Similarly, Baltimore faced estimated costs of $18.2 million[3] to recover its data, refusing to meet ransom demands of $76,000. Newark, NJ, meanwhile, paid $30,000 in bitcoin ransom[4] to recover its data.

1. The Hill. "State and local officials celebrate passage of infrastructure bill with $1 billion in cyber funds"

2. The Atlanta Journal-Constitution. "Atlanta's cyber attack could cost taxpayers $17 million Report"

3. SHRM. "Ransomware Attack Will Cost Baltimore Over $18 Million"

4. NJ.com. "Iranian hackers hijacked Newark's computers, extorted $30K ransom"

For the bad actors, state and local governments are a logical target. With annual budgets under pressure, ransomware prevention and recovery have often taken a back seat to other seemingly more important priorities. Not only are cybersecurity technology line items often missing, but cybersecurity specialists often are not hired. In another cost-driven practice, government bodies often maintain legacy infrastructure far longer than private-sector organizations. As a result, many of their systems lack up-to-date security protections. The pandemic also applied stress to state and local cyber-defenses, as it did to all organizations, when suddenly many workers were accessing systems remotely, often from personal devices on unsecured home networks.

Government demands are unique

While a privately held business might quietly pay ransom to recover its data with the public none the wiser, a ransomware attack on a governmental entity quickly becomes public knowledge. For example, when data is locked up, agencies cannot perform routine tasks such as issuing driver's licenses and permits, and police forces cannot provide evidence for prosecutions. And when critical services are stuck in limbo, there is likely to be outcry in the form of adverse public opinion—and ultimately, rejection at the ballot box for top officials.

Currently, public pressure is being applied through proposed legislation, as several states are mulling laws[5] to ban ransom payments.

Follow the federal leader

With funding waiting in the wings, it is time for state and local IT leaders to re-think their cybersecurity and anti-ransomware strategies. Their to-do lists should start with everything that thin budgets have been thwarting: up-to-date infrastructure, reliable and complete backups, and highly effective cybersecurity software and services.

To help federal civilian agencies tighten up their defenses, the United States Cybersecurity & Infrastructure Security Agency (CISA) released two playbooks.[6] Although intended for a federal audience, CISA recommends

5. Government Technology. "States Consider Legislation to Ban Ransomware Payments"

6. Cybersecurity & Infrastructure security agency. "New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks"

that critical infrastructure entities, state, local, territorial, and tribal government organizations, as well as private sector firms review the playbooks to benchmark their own vulnerability and incident response practices. CISA also released in November 2021 a Capacity Enhancement Guide[7] that explains how to secure web browsers against malvertising, which uses web ads to spread malware.

Zero Trust and the Cyber EO

The CISA publications are a response to Executive Order (EO) 14028: Improving the Nation's Cybersecurity, issued in May 2021 by President Biden.[8] That order also mandated the implementation of Zero Trust by federal agencies. In a Zero Trust strategy, persons and devices that have been granted access to data and applications are assumed to have been compromised and are therefore continually examined for evidence of malware or suspect behavior.

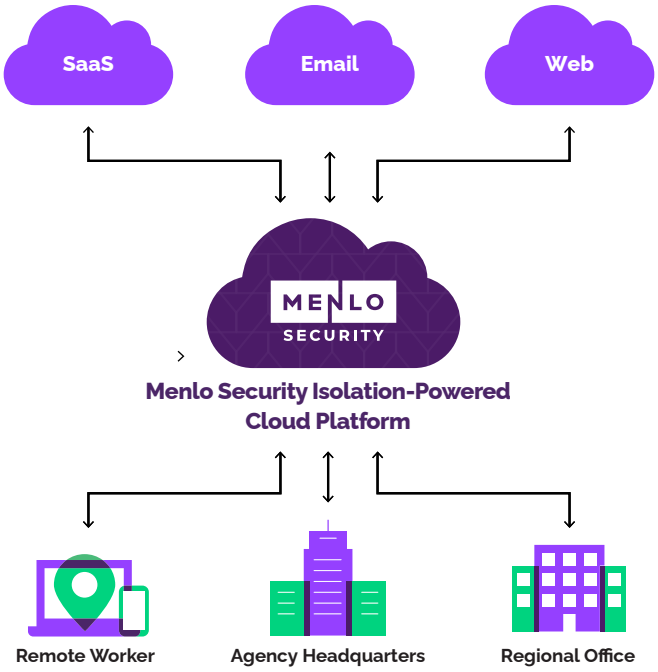
Just as state and local governments might well benefit from the CISA playbooks and Capacity Enhancement Guide, they could also stand to gain from implementing Zero Trust. In practice, Zero Trust strategies include multi-factor authentication, least-privilege access to applications and data, and micro-segmentation of network resources to prevent bad actors from moving from one application to another. The overriding goal is to sharply limit the damage of successful attacks.

7. Cybersecurity & Infrastructure security agency. "Capacity Enhancement Guides"

8. The White House. "Executive Order on Improving the Nation's Cybersecurity"

Remote Browser Isolation

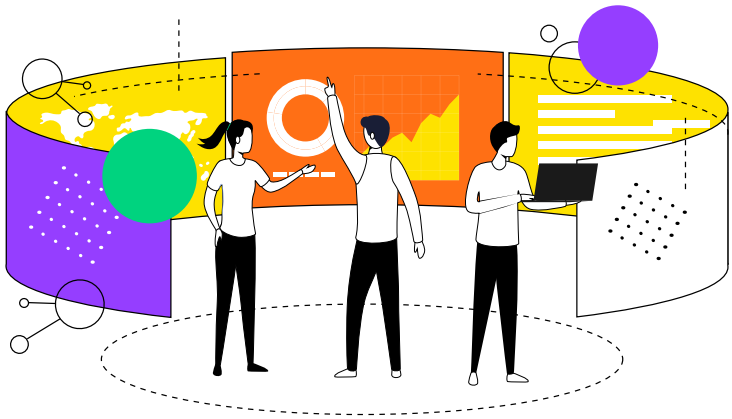
Although Zero Trust is a worthy goal, it's possible to go beyond conventional Zero Trust implementations by keeping malware entirely off end-user devices. The best way to achieve that is through Remote Browser Isolation (RBI), which is one of the CISA Enhancement Guide's recommended measures for malvertising prevention. "Embraced by the Department of Defense and major corporations, browser isolation is a strategic architectural decision," according to the guide.



RBI creates a virtual "air gap" between the user's system and online resources. Instead of opening a website in a browser, a cloud-based virtual machine fetches and executes the website content. A sanitized version of the website is sent to the end user, who receives a fully functional experience with malicious code removed. By assuming that no website can be trusted, RBI is a true implementation of Zero Trust.

The Menlo Security Cloud Platform implements RBI through its Isolation Core™. Not only does this solution keep your users' devices free of ransomware, its virtual-air-gap technology delivers the added benefit of reducing the number of alerts. That in turn lightens the burden on IT staff since person-hours are not required to chase down alerts to determine whether they are real or false.

Even with additional funding, spending money wisely will enable you to make the most of your staff, allowing them to focus their energy on the highest priority tasks.



As with any technology, it is best to start small to prove its effectiveness and grow incrementally. To that end, the Menlo Security Cloud Platform is scalable. A state could roll it out for the state police or department of health to begin, then make it available to other agencies, all under the same license.

The federal infrastructure bill will provide a much-needed infusion of funds, and a chance for state and local governments to do things right. That means implementing the most effective cybersecurity strategies and technologies – including RBI – through a proven, patented, proactive solution like the Menlo Security Cloud Platform.

We're ready to answer your questions at: ask@menlosecurity.com.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.