halcyon

Customer Story

When Feeling Safe Isn't the Same as Being Safe: How this City Closed Its Ransomware Blind Spot

With a six-person IT team, 24 years of institutional knowledge, and one threat that no amount of layered defenses could fully address, the City of Williamsburg added Halcyon to an already-strong security stack to deliver the ransomware-specific protection the historic city's residents deserve.

The City of Williamsburg, Virginia carries responsibility well beyond its 15,500 residents. Home to Colonial Williamsburg, William and Mary, and a city government supporting 230 employees across public safety, human services, and finance, it's a small city with outsized stakes. CIO Mark Barham has led its IT organization for 24 years, and as Williamsburg prepares for the 250th anniversary of American independence this July 4th, keeping operations secure and residents' data protected has never felt more consequential.

Firewalls, EDR, a 24/7 SOC... and the One Threat That Still Kept Him Up at Night

The City of Williamsburg's security posture was, by any reasonable measure, strong. Firewalls blocked traffic originating outside the United States. A 24/7/365 SOC monitored the environment around the clock. Endpoint detection was in place. Years of consistent employee training produced a genuinely security-aware workforce, the kind where staff actually thank IT for catching them in phishing simulations.

"I always get responses from employees where they're like, 'You almost got me the other day,'" Barham says. "We have a really educated workforce as it relates to cybersecurity."

But one threat still kept him up at night: ransomware. Not because the city lacked defenses, but because ransomware operators are especially skilled at getting around them.

"That was the one thing we were not going to block," he explains. "They're pretty evasive in terms of getting around whatever defenses might be in place. And we had layer upon layer upon layer of defenses in place."

The headlines made it impossible to ignore. Atlanta. Columbus. Baltimore. Dallas. Cities with far greater resources than Williamsburg had been taken offline for months, and it wasn't lost on Barham that confidence in a strong security posture hadn't saved them. The damage, he knew, wasn't just operational.

CITY OF WILLIAMSBURG
VIRGINIA'S COLONIAL CAPITAL

Customer Snapshot

- Customer: City of Williamsburg, Virginia
- Sector: State and Local Government
- Employees: 230 IT
- Team: 6 people
- Headquarters: Williamsburg, Virginia

Key Results

- Deployed across all endpoints in under an hour
- Immediate visibility into unauthorized remote access tools that had bypassed existing defenses 24/7 ransomware-specific expert coverage for a six-person IT team, at no additional cost
- Clear, defensible ROI justification for city leadership
- Dramatically elevated confidence in ransomware readiness across the organization

> "It keeps me out of the newspaper. It also keeps the City of Williamsburg out of the newspaper."
>
> Mark Barham,
> CIO, City of Williamsburg, Virginia

"That hit to your reputation, it's kind of like once the bell's rung, you can't unring it," he says. "That was something I wasn't willing to sacrifice."

The instruction his first city manager gave him on day one had shaped his thinking ever since: keep us out of the newspaper. That simple mandate, offered long before ransomware was a household word, turned out to be the most clarifying frame for every security investment that followed. Feeling protected and actually being protected from ransomware, Barham had come to understand, are two very different things.

"You think you're safe, you think you're blocking so much, everything is just solid. Run a proof of concept. And then come back to me when you see that data start flowing in, and tell me again how protected you are."

Mark Barham, Chief Information Officer,
City of Williamsburg, Virginia

After an initial conversation with Halcyon's team, Barham agreed to a proof of concept. The deployment took less than an hour, and data began flowing into the tenant almost immediately. What that data revealed changed the conversation entirely.

In detect mode, before any blocking was active, the platform began surfacing activity that Williamsburg's existing tools had never flagged. The finding that hit hardest: a significant number of employees were connecting to the network using unauthorized remote desktop tools, none of which the IT team had approved and none of which had appeared in any prior monitoring.

"We had absolutely no idea that stuff was flowing into our network," Barham says. "What was still getting through our really locked-down environment was pretty amazing."

The proof of concept ran for two months, surfacing issue after issue that had been invisible to every other tool in the stack. For Barham, it reframed the entire question of ransomware readiness.

"Before Halcyon, you're like, we're pretty good, we're solid, everything is good," he says. "And then you launch it, and stuff starts popping into the tenant."

By the end, there was no debate about the decision.

Run the Proof of Concept. See What Your Stack Misses.

When asked what he would say to a fellow city IT leader who felt confident in their existing security posture, Barham's answer is direct: run a proof of concept first, then form an opinion.

"You think you're safe, you think you're blocking so much, and everything is just solid. Run a proof of concept. Have them stand up a tenant, and then come back to me when you see that data start flowing in, and tell me again how protected you are."

His prediction for what they'll find mirrors exactly what Williamsburg discovered, activity and exposure their existing tools weren't catching, and a new understanding of just how specifically dangerous ransomware is compared to threats their stack was actually built to stop.

"You're nowhere near as protected as you think you are from something as harmful and dangerous as ransomware," he says.

The Halcyon Team of 24/7 Experts Fill the Gap a Small Team Can't

One of the realities of local government IT is that small teams carry outsized responsibility. With six staff members supporting an entire city's technology infrastructure, Barham's team cannot dedicate focused resources solely to security, even though security is arguably the most critical thing they manage.

That's where the Halcyon Ransomware Operations Center (ROC) changes the equation. Staffed by ransomware-specific experts who investigate alerts, respond to threats, and lead recovery efforts if an attack does occur, the ROC functions as a force multiplier for Williamsburg's team at no additional cost.

"The resources made available to us through just being a subscriber to the platform, that gives me a lot of comfort," Barham says. "A lot of comfort."

Knowing that purpose-built ransomware experts at Halcyon are monitoring and ready to respond around the clock means Barham's team doesn't have to choose between security and everything else the city needs from them.

Confidence that Extends to City Leadership

Making the case to city leadership has never been difficult. Barham sits on the city's executive team, and 24 years of tenure have given him significant credibility with his leadership. But even without that context, the economics of the decision make it an easy one to defend.

"The costs for what we pay for Halcyon versus what could happen if something were bad, it's one of the easiest sells," he says. "Negligible is probably the term I would use."

His framing for leadership mirrors the guidance he received on his first day. Walking through what an incident would actually cost, the executive team pulled in, attorneys, communications staff, third-party incident responders, Virginia State Police, CISA, and weeks of recovery time for a six-person team, makes the alternative clear to anyone in the room.

Built for a City That Cannot Afford to Go Dark

For organizations like Williamsburg, highly visible, mission-critical, and operating with small IT teams, Halcyon isn't a replacement for the security stack already in place. It's the ransomware-specific layer that closes the gap everything else leaves open, backed by experts available around the clock and priced in a way that makes the decision easy to justify at any level of leadership.

"Great product," Barham says. "It's one I believe in, that my organization believes in, and it's shown its value to us many, many times over. It keeps me out of the newspaper. It also keeps the City of Williamsburg out of the newspaper."